Digital advertising guidance: Legitimate Interests Assessments under the UK GDPR

March 2021

Table of 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 UK GDPR (while recognising that individual companies remain accountable for deciding what approaches they should take in practice).

The purpose of this guidance is to provide a practical guide to carrying out legitimate interests assessments (LIAs) in the context of processing data in ad tech, for digital advertising generally, and for RTB, in order to help companies understand their obligations, and how to comply with them in practice.

Legitimate interests can be relied upon as a legal basis to process personal data but organisations need to balance these interests with the rights and interests of the individual. You should be aware of regulators' views on the use of legitimate interests in relation to digital advertising (see 'How to use the guidance' below). Legitimate interests cannot be used as a basis for setting cookies, and where processing of personal data is dependent on non-essential cookies, which require consent, that consent is a prerequisite to the subsequent processing. See our separate guidance on Cookies, consent and the GDPR.

In order to use this legal basis, organisations must carry out a balancing test, weighing their interests to process personal data against the interests, fundamental rights and freedoms of the individual. As part of this assessment, organisations have to consider whether individuals would reasonably expect their personal data to be processed based on the relationship they have with the organisation but also how their data is processed. Overall, key to using legitimate interests as a legal basis is that the interests, fundamental rights and freedoms of the individual are not overridden.

This guidance is intended 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 and IAB Europe have worked to develop this guidance jointly. This version is intended for the UK market, and assumes that your data processing is regulated by the ICO. For other companies, the equivalent version of this guidance is available from IAB Europe at https://iabeurope.eu/.

We recommend that, if you intend to process or are processing personal data on the basis of legitimate interests, you ensure that you have undertaken an LIA and that it meets all the relevant requirements, so that you can demonstrate that individuals' rights and freedoms do not override your interests.

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 UK 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.

Note that, following Brexit, the GDPR has been retained in UK law (with some minor amendments to reflect the UK's new status) and renamed 'UK GDPR'. For details see the ICO's guidance at https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/.

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

- UK-established data controllers and processors
  and
- entities outside the EU that process the data of individuals in the UK.

1.2 How to use the guidance

This is a guide to conducting a legitimate interests assessment (LIA) in the digital advertising industry. The aim is to provide a standardised approach to conducting an LIA that takes into account the particularities of processing and the associated risks in the industry, and further, takes into account specific questions and concerns raised by regulators.

This guidance does not cover legal bases in general, or how to select the most appropriate legal basis for your processing. It assumes that you have already identified that legitimate interests is your intended legal basis. However, you should be aware of the ICO's position on the use of the legitimate interests legal basis for digital advertising (particularly where consent is required for the use of cookies or other similar technologies), and for RTB specifically, as set out in section 3.3 of their 'Update report'[1] (pages 17-19). The report says (p.18):

> 'In our view, the only lawful basis for 'business as usual' RTB processing of personal data is consent (i.e. processing relating to the placing and reading of the cookie and the onward transfer of the bid request).'
>
> The rationale for this position is explained in the report, and is based on the consent requirements in PECR and 'the nature of the processing in RTB'.

We remain of the view the legitimate interests can be an entirely appropriate legal basis for processing personal data for many industry functions, both in principle and in practice, if properly established.

[1] ICO, *Update report into adtech and real time bidding* (June 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

There are also concerns that legitimate interest is considered by some in the industry to be the 'easy' alternative to consent,[2] and that LIAs are being done as a pro forma exercise, without the rigorous and honest reckoning of risks that is required. One key purpose for this guidance, therefore, is to help establish a common understanding of how a properly thorough LIA is done in our industry.

There is no guarantee that using this guide will result in a legally viable legitimate interests determination. However, whereas today we have very little guidance in the market, and no common understanding of where the bar is set, we hope for this to provide a roadmap that can get companies to where they need to be, if they do the work. In that spirit, note that this guidance does not provide legal advice or analysis. Still, a map is all that it is. Like a DPIA, an LIA is more than paperwork. Like a DPIA, conducting an LIA is an extensive process. Companies must give thoughtful, objective[3] consideration to the balancing test of the LIA, and all of the relevant factors that go into it. The process should be approached without a predetermined expectation of the outcome of the balancing test, and therefore whether or not legitimate interest can be used as the legal basis for the proposed processing. Regulators will expect to see that an LIA has thoroughly credited the data subject perspective, cited robust supporting evidence, and wrestled with the balancing of rights and interests. This guide aims to help companies do so.

Additionally, the IAB has produced other guidance that is referenced in appropriate places in this document, that you should consult as appropriate, and a resources section is included at the end.

1.3 Who is the guide for?

The guide is intended for use by digital advertising companies of varying natures and types, and the advertisers, agencies, and publishers who work with them. It is particularly fitting for use in conjunction with the Transparency & Consent Framework (TCF),[4] which requires companies declaring legitimate interests as their legal basis for particular processing purposes to attest that they have completed legitimate interest assessments for each purpose where they claim it as a basis. As with use of the TCF generally, vendors remain responsible for ensuring that they comply with all the legal requirements associated with processing personal data, including (if they are a data controller) the legal basis that the select for their processing. The fact that it is possible to declare that you are relying on the legitimate interests for a particular TCF purpose should not be taken as an indication or guarantee that it is possible, or would be lawful to do so, in any particular instance.

[2] ("There seems to be a perception by some participants that consent is 'challenging' and legitimate interests is the 'easy option'. Overall, we do not believe there is a full understanding of what legitimate interests requires." (ibid.))

[3] Objectivity means stepping back and taking a view from outside your company. Your personal, or your company's, views should not govern. You must adopt a broad perspective.

[4] https://iabeurope.eu/transparency-consent-framework/

1.4 What is an LIA?

Article 6 of the UK GDPR offers six possible legal bases under which personal data can be lawfully processed. In general, for our industry, only two are likely to be relevant[5]: consent[6] and legitimate interests.[7]

The term "legitimate interests" used to identify the legal basis of Art. 6(f) is shorthand for something more complex than it implies. This shorthand should not be misunderstood to mean that the focus is primarily on the controller's interests (or the interests of a third-party), because those interests must be measured (objectively) against the impact on data subjects' interests and rights.

In fact, the legitimate interest of the data controller is only the first of three steps required to establish the legal basis, as derived from the text of Art. 6(f):

1. Purpose: Determine that the purposes for processing reflect an identified legitimate interest of the controller or third-parties (which can include data subjects) or both;
2. Necessity: Show that the proposed processing is necessary and proportionate for the purposes of the legitimate interests pursued, or for achieving that purpose, and that there is no less-intrusive alternative; and
3. Balancing: Show that the legitimate interests pursued are not be overridden by the data subject's interests or fundamental rights and freedoms.[8]

These steps are explored in more detail below.

1.5 The scope of this guide

The guide is specifically designed to guide a LIA for processing of data in the digital advertising industry. There is no fixed recipe for arriving at a conclusion in favour of a legitimate interests legal basis. Each circumstance must be analysed objectively in its own terms, and on a case-by-case basis. However, this guide is intended as a roadmap to guide a properly done LIA for our industry, hoping to ensure that the analysis is directionally correct and hits the key points along the way.

By employing this guide, we can establish consistency across industry, and help establish the bar for what a robust LIA looks like. So, while using this guide does not guarantee a legally supportable outcome, it does help move companies in the industry toward a similar approach, which considers issues common to the industry, and which we hope will produce consistency across different companies.

[5] Without prejudice to circumstances where other legal bases may be appropriate.
[6] UK GDPR, Art. 6(a).
[7] UK GDPR, Art. 6(f).
[8] Art. 6(f) provides for a legal basis for processing if "[it] is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

1.6 The relationship between LIA and DPIA

You may notice a resemblance between a LIA and a DPIA. Both may be prerequisite to processing personal data. Both entail deep consideration of the potential impacts on a data subject's privacy. Both involve considering the trade-offs between the controller's aims for the processing and the data subject's interests, rights and freedoms.

While a DPIA is a process to be used to assess and mitigate the likelihood of high risks to data subjects, a LIA is legal analysis to determine whether the rights and interests of data subjects outweigh identified legitimate interests that the controller believes necessitate the processing of personal data.

Where a DPIA is required[9] to ensure lawful processing (which it is likely to be, in many digital advertising and RTB-related use cases) and legitimate interests is the intended legal basis for processing, that DPIA should be completed prior to, or at the very least, in parallel with your LIA. As the LIA is begun, the results from the DPIA, in particular, the residual risks, will be important inputs into the LIA. In fact, a completed DPIA should include most of the underlying work for the LIA. If you have not completed a DPIA process, you should consider whether one is necessary, particularly if your LIA identifies significant risks (see our separate guidance: 'Data Protection Impact Assessments under the GDPR'[10] for more details).

2. When and how to do an LIA

2.1 General approach overview

Obviously, the LIA should be completed before processing under the legitimate interests legal basis. In terms of product design and development, the intended legal basis for processing personal data should be determined very early in the product development process, and if legitimate interest is the intended legal basis, the LIA balancing test should be considered throughout the development. Moreover, legitimate interest may not be appropriate at all under many circumstances. LIAs should also be reviewed and updated if the processing activities change or develop over time, or if the circumstances relied on in the balancing test change.

Legitimate interest should not be approached as a foregone conclusion. The LIA is an opportunity to do, and show, the work of a thorough, objective balancing test and credible outcome. You should approach the process objectively and with an open mind and be prepared for the balancing test to weigh in favour of the data subjects' interests overriding your legitimate interests.

The LIA will take as inputs: the controller's (or a third-party's) interests in the data processing, the detailed facts about the processing, and the potential impacts on data subjects that could result from the processing.

---

[9] For guidance on when DPIAs are required see our guidance on Data Protection Assessments under the GDPR https://www.iabuk.com/news-article/digital-advertising-guidance-dpias-under-gdpr

[10] ibid.

Then, the three-part process begins, as outlined in the section 'What is an LIA?', above.

First, the controller must establish what legitimate interests of the controller and/or a third party are being pursued in connection with the proposed processing . The legitimate interests can be those of the controller, but also, possibly, the legitimate interests of or beneficial outcomes for data subjects or other third parties, and society as a whole (as appropriate). Next, the controller must show that the proposed processing is necessary and proportionate to achieving those interests, and that there is not a less intrusive alternative. Finally, the controller must examine the potential impact on the data subject and evaluates whether, given that impact, "the interests or fundamental rights and freedoms of the data subject"[11] override the legitimate interests being pursued by the proposed processing.

The work should be done with specificity as to all factors. It is not sufficient to say, for example, that your interest is in "showing ads" or "making money" or "improving ad performance." There are many alternative ways to show ads, or make money, or improve performance. You must explain a legitimate interest (e.g. a legitimate purpose or intended outcome) with some specificity. The ICO's guidance[12] says:

> 'Showing that you have a legitimate interest does mean however that you (or a third party) must have some clear and specific benefit or outcome in mind. It is not enough to rely on vague or generic business interests. You must think about specifically what you are trying to achieve with the particular processing operation.'

You should keep a written record of your LIA to help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. Your record of your LIA should be sufficiently detailed and descriptive so that your reasoning and decision-making is clear and comprehensible to others (for example the ICO, should they need to review it).

2.2 Who is involved?

Legal and/or compliance functions typically take the lead in carrying out LIAs within an organisation. They may be done by internal personnel, or sometimes are completed by an outside lawyer. Whereas a DPIA is in large part a technical exercise – identifying risks and applying mitigations – the LIA balancing test is very much a legal-style exercise (though one need not be a lawyer to do it) and the outcome represents a legal determination of the appropriate legal basis for processing of data. While the legal and/or compliance team, will likely be in the lead, ownership over the exercise should be shared with the business owner or the team leading the particular business activity to which the LIA relates so as to encourage, reinforce and effectively legitimise decisions involving data processing. Moreover,

[11] UK GDPR, Art. 6(f).
[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

the DPO has a role in ensuring the adequacy of an LIA. Whatever the case, it is important to ensure that persons with a high level of expertise and experience – sufficient to properly and objectively judge the balancing test – are engaged to complete the LIA. Others may need to be involved in providing the inputs to the assessment, including your DPIA team.[13]

3. The LIA

3.1 The three-part test

The LIA is a three-part test, all parts of which must be satisfied:

1. Purpose test: What is the purpose and objectives of the processing and are there legitimate interests in conducting the processing?
2. Necessity test: Is the specific processing necessary to achieve the legitimate interests described in step 1?
3. Balancing test: What are the impacts of the processing on data subjects, and how does this compare with the interests from step 1; are the interests overridden by the data subject's interests, fundamental rights and freedoms?

We will explore considerations for each in more detail.

Part 1: Purpose test

First, assess whether there is a legitimate interest behind the processing.

You should detail your specific plans for processing data – the data and the processing operations involved – including such things as retention period and sharing. If you have done a DPIA for the processing, you will have this information compiled.
Your purpose(s) for processing the data should be defined in detail to be able to identify the proposed legitimate interests. Highly generalised or vague objectives are not sufficient. Explain precisely why you want to do this particular data processing activity and what outcomes, benefits, etc.it is intended to achieve.

For example, "measure ad performance" is a TCF purpose. It is broad, in order to encompass a wide range of possible processing activities done by various companies. However, if you do an LIA for ad measurement to be done under this purpose, using legitimate interest as the legal basis, you should be more precise, for example: "using last click attribution to measure ad performance and attribute results to particular publishers." You might be even more precise than that, for example: "using a new model of analysing last click attribution data to attain 20% improvement in predictions of performant ad-publisher combinations."

You should also specify, again with precision, the benefits you seek to derive from the processing. These could be benefits to your company or to others. You can be

[13] Data Protection Assessments under the GDPR https://www.iabuk.com/news-article/digital-advertising-guidance-dpias-under-gdpr

thorough and expansive. Broad pronouncements, such as “targeted ads help support publishers,” even if supportable, might be relevant but not sufficient.

Here are some examples, as illustration (without any assertion that these are appropriate uses for legitimate interests.)

Frequency capping:

- Users benefit from seeing less repetition in ads
- Publishers benefit because users have a better experience if they do not see the same ads over and over
- Advertisers benefit from not over-saturating particular users with their ads, and can direct their ad spend more efficiently by not showing the same ad too many times to one user

Last-click attribution:

- We can learn which ads and which publishers work best for which advertisers, which leads to more efficient ad spending; without measuring ad performance, we would not know what works and what doesn’t so would cause advertisers to waste more money
- Enable performance-based rewards to be paid to publishers, which is an efficient mode of advertising, and which rewards publishers for having audiences that respond best to certain ads
- More efficient ad spend benefits all users and society because: it helps keep prices lower, makes ads more relevant, rewards publishers with more engaging content

Note that for illustration purposes, these benefits are included here without details of the processing and without additional support to back up the claimed benefits. It will depend on your particular circumstances, but you should be able to support the assertions that you make, ideally with quantitative or other objective analysis. Public research, industry papers, and other sources are also good places to look.

Note also, that if there is enough similarity in various interests, you can group them together into the LIA. But the similarity should be relatively consistent across all steps of the test and all of the factors considered, otherwise the results may not be applicable to all of the processing. You can determine what is appropriate for your circumstances.

Step a: context of processing

Compile a complete factual description of the processing involved. Our DPIA guidance gives more detail on how you can do this. See https://www.iabuk.com/sites/default/files/public_files/IAB-UK%20Digital-advertising-guidance-Data-Protection-Impact-Assessments-under-the-GDPR.pdf (page 12).

Some particular things to consider for the LIA include:

- How will data subjects receive notice of the processing and your legal basis?
- What diligence and other mechanisms or procedures do you have in place to ensure that data you receive was collected and transferred under appropriate legal bases?
- In particular, how are data subjects informed of, and able to exercise, their rights to restrict processing14 or object?[15]

Step b: purposes of processing

Define, in detail, the purposes for processing, and the interests for your company, and any third parties.

- What, precisely, is the processing intended to accomplish, and how will it do so?
- What are the benefits for your company?
- What are the benefits for your clients?
- What are the benefits for other commercial parties, such as publishers?
- What are the benefits for data subjects, any particular community, or society as a whole?
- What would be the impact if you did not do this processing?
- What support, including evidence, do you have for the above? Can you qualitatively and/or quantitatively show the value and likelihood of the benefits you are claiming;16 have you considered any case-law / precedent in identifying interests that would be considered as "legitimate"?

Part 2: Necessity test

Once you have detailed your intended purposes and legitimate interests, now you must demonstrate that the intended processing is necessary and proportionate for those purposes and interests. This bears some resemblance to a data minimisation exercise, and if you have done a proper DPIA, you may have produced as a by-product the necessity justification you need. As with data minimisation, there is an element of balancing within the necessity test. It is not that the processing must be absolutely essential or the only possible way of achieving your interests, but 'it must be a targeted and proportionate way of achieving your purpose.'[17] So, you must make and honest and objective assessment of:

- how the processing actually helps you achieve your legitimate interests
- whether the processing is proportionate to your legitimate interests
- whether there are less intrusive alternatives that use less, or no, personal data (the ICO's guidance says: 'If on the face of it there are potentially other

[14] UK GDPR, Art. 18(1)(d).
[15] UK GDPR, Art. 21.
[16] For example, a claim that a product "will produce increased efficiency in ad spend" is considerably weaker than being able to state that "research and testing has shown up to 5% improvement in ROAS."
[17] ICO, *What is the 'legitimate interests' legal basis?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#when_is_processing

less intrusive alternatives you need to be clear in your LIA why these are not reasonable alternatives.'[18])

In practice, this means you should examine all aspects of the proposed processing for the interests identified and justify the processing under this test. Some examples to illustrate:

- Are there models that can achieve your aims with non-personal or de-identified data?
- While geographic information might be important to the proposed processing, is it necessary to use 5 decimal place GPS coordinates or would less precise data suffice?
- While it might be useful to retain raw data for many months or even years, is it really necessary, or could you obtain your objectives while aggregating the data in a much shorter time frame?
- If your processing involves sharing the data, think about why and whether sharing is really necessary, which data precisely needs to be shared. Could any of it be anonymised?

Do not skimp on this step. Give it thorough consideration and substantiate your analysis wherever possible. If you can, produce empirical evidence to demonstrate that your proposed processing is necessary to your objectives.

Step a: data minimisation

The IAB DPIA guide offers detailed guidance regarding data minimisation approaches in the industry.[19] But, in general, you should thoroughly consider how you might achieve your purposes and interests with less data:

- What possible alternatives that use less, or no, personal data, or less processing of such personal data, have you considered and ruled out? What is your basis for choosing this processing over the alternatives?
- Have you minimised the data to be processed? (If you have done a DPIA, then you should have already gone through a process of data minimisation.)
- If the processing involves sharing data, can you account for the necessity of each piece of data to be shared, in the form it is to be shared?

Step b: is the need for the processing supported?

You have to show that the proposed processing for the identified interest is reasonably necessary and proportionate to your objectives. As noted above, it is not a strict necessity standard, but you should be able to demonstrate the need for the processing, particularly in comparison to possible alternatives. [20]

[18] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#LIA_process
[19] See IAB UK digital advertising guidance: Data Protection Impact Assessments under the GDPR p.14 and Appendix B
[20] 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/?q=proportionate#when

- How is this processing necessary for your intended interests and to achieve the benefits described in the 'Purpose' test above?
- Can you draw a connection from each aspect of the processing to the intended purpose and interest?
    - How is each element of data to be processed necessary for the purpose and interest?
    - How is the period of retention for all of the data justified?

Part 3: Balancing test

The balancing test is, as they say, where the rubber meets the road. First, you will elaborate on the potential risk to and impacts on data subjects from the processing based on the interest that you have identified. You must be thorough and take the data subject's perspective, with an understanding of what are the data subject's reasonable expectations. Understanding that many impacts are subjective, be generous in taking into account a wide range of possible views, and evaluate them later in the process. Just because there is a possible negative impact on data subjects does not mean you cannot use legitimate interest as your legal basis,[21] but you must take these impacts into account, and your consideration of a number of factors will help you determine whether the impacts on data subjects should override your identified legitimate interests.

Second, you will consider a range of factors that weigh against or in favour of the processing. As with the previous stages, you should specify these factors in detail. Sweeping assessments, such as "users expect data to be used for advertising," may be relevant, but are not sufficient. Drill down. To what extent would users expect this particular processing? Can you support your assertions about user expectations with evidence? What is the nature of the data? Safeguards you put in place, such as additional transparency and control, may weigh in your favour.[22]

Finally, you will weigh the data subject's rights and interests against the legitimate interests being pursued, in light of the aggravating and mitigating factors considered in Part 2, and make a determination as to whether the processing is justified under a legitimate interests legal basis. Be objective in this determination, and if it is not justified, you must either use another legal basis (i.e. consent) or amend the processing to improve the balance of interests.

---

[21] ICO, *What is the 'legitimate interests' legal basis?*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#when_is_processing (last visited Jun 2, 2020).

[22] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (Apr 2014), available at https://ec.europa.eu/justice/article–29/documentation/opinion-recommendation/files/2014/wp217_en.pdf ("At the same time, pseudonymisation and encryption, just like any other technical and organisational measures introduced to protect personal information, will play a role with regard to the evaluation of the potential impact of the processing on the data subject, and thus, may in some cases play a role in tipping the balance in favour of the controller. The use of less risky forms of personal data processing … should generally mean that the likelihood of data subjects' interests or fundamental rights and freedoms being interfered with is reduced.")

Step a: Risks and impacts

Consider the data subject's perspective and elaborate on all reasonably foreseeable risks to their rights and freedoms. Remote or edge case concerns should be included; the significance of the risk will be considered in the next step, and you will take into account the likelihood of occurrence.

While not exhaustive or applicable to all cases, Appendix A lists some common concerns for our industry that should be considered. You must consider whether there are others that are applicable to the processing that is under consideration.

For each risk identified, consider – in the context of the specifics of the processing and the nature of the data – the likelihood that the risk will occur and the severity of impact if it does occur. You must consider the level of risk in the balancing test.[23] Again, if you have done a DPIA, you should have this information in the form of your documentation of residual risk at the conclusion of the DPIA process.

Risk level is determined multiplying the likelihood of an adverse event by the severity of its consequences.

Risk = likelihood x severity of impact

For guidance on risk assessments please see Appendix A of IAB UK digital advertising guidance: Data Protection Impact Assessments under the GDPR.

You can choose to take note of risks that are highly unlikely or not present at all, either because of the nature of the processing or because of safeguards you have put in place. For example, identity theft and financial fraud are in most cases not considered risks in our industry.

Step b: aggravating and mitigating factors

- Nature of the data: The more sensitive the data, the more it is likely to intrude on the data subjects' interests, or to create risks to data subjects' fundamental rights and freedoms, and therefore the more it weighs against your legitimate interests. (Though, the sensitivity can be balanced by things like notice and choice.) Factors to consider (and you may be able to draw on information you have documented these elsewhere, for example in your record of processing activities) include:

  Does the data contain Art. 9 special category data? Bear in mind that special category data could be created or arise from other data, depending on a

[23] For further guidance on assessing risk, see for example, ICO, *How do we do a DPIA?*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia and IAB UK's DPIA guidance https://www.iabuk.com/sites/default/files/public_files/IAB-UK%20Digital-advertising-guidance-Data-Protection-Impact-Assessments-under-the-GDPR.pdf

- number of factors (the nature of the data, whether it is combined with other data, what it will be used for, etc.). See our separate guidance for more information.[24]
- Is the data about vulnerable populations, such as children[25] or elderly?
- Does the data contain precise location data?
- Does the data contain information about data subjects' online activity?
- Does the data contain demographic or psychographic information?
- Is the data pseudonymised? If so, what is the risk of re-identification?[26]
- Is the data anonymised?[27]

See Appendix A for more detail and illustrative examples of risks specific to the digital advertising industry.

- Nature of the relationship and context of collection: The nature of your connection to the data subject and the context of where and how the data was collected and received by you can weigh in favour of, or against, your claim to legitimate interest. For example, you may be a 'vendor' providing services to advertisers, and the data subjects are the advertisers' customers. In contrast, you could be a data provider that is four degrees separated from the publisher on whose media property the data was initially collected.

  The availability of notice, transparency, and choice is also an important factor that bears on the data subject's reasonable expectations and on the impact of the processing on the data subject. The more a data subject can understand and/or can control the data collection and processing, the stronger your case in favour of legitimate interest. Conversely, opaque and hard-to-control collection and processing weakens your case for legitimate interests. Factors to consider include, for example (again, you may have this information documented elsewhere, that you can draw on):
  - What is the nature of your relationship with, or connection to, the data subjects?

[24] https://www.iabuk.com/news-article/digital-advertising-guidance-special-category-data-under-gdpr
[25] UK GDPR, Art. 6(1)(f) makes specific reference to data subjects who are children.
[26] Note that not all indirect identifiers are properly pseudonymous. Pseudonymous data is personal data that can no longer be attributed to a specific data subject without the use of additional information. This means that, in practice, the additional information needs to be sufficiently separate in terms of how it is stored, and the controls that are in place to ensure that re-identification of an individual is not possible. For example, an identifier that is directly linked to a social media profile may not be considered pseudonymous, because it does not require matching with additional, intermediate information to personally identify the data subject. Contrast that with a randomly generated cookie ID, which on its own does not lead to personally identifying the data subject; doing so would require an intermediate, transitive match to tie the cookie to a profile. This is an involved and often misunderstood topic. It is recommended you consult your experts to ensure that you have properly classified pseudonymous data.
[27] Be careful about properly anonymising data. 'Anonymised' has a very specific meaning in the context of the UK GDPR. It means there is no reasonable way to match the data back to an individual, even using additional data from other sources. Properly aggregated data is likely anonymous. However, individual records with identifiers removed may not be anonymous. There is considerable research into the re-identifiability of supposedly anonymised data. As with pseudonymous data, anonymisation is often misunderstood and the term misapplied. Consult your experts to ensure you have it correct.

- How did you receive the data? Did you collect it directly from the data subject? Did you collect it from the browser or app? Did you receive it from a party that has a direct relationship with the data subject or did you receive it from an intermediary?
- What notice was provided to the data subject at the point of collection? If the data processing would be dependent on the use of technologies regulated by PECR Regulation 6, did the notices meet the relevant requirements?[28] Did the notice provide information about this type of processing? Were you, as the controller, disclosed to the user at the time of collection, or at some subsequent time?
- How transparent is the collection? Can the user see it? For example, cookies and tags are relatively transparent compared to probabilistic identification. Client-server calls are more transparent than server-server transfers.

- User expectations: Again, be specific and objective about the processing. As the ICO's guidance puts it:

  'This is an objective test. You do not have to show that every individual does in fact expect you to use their data in this way. Instead, you have to show that a reasonable person would expect the processing in light of the particular circumstances.'[29]

  "Users like ads" or "users don't like ads" or "users know that data is collected for advertising" is too general. What do users know and how would they feel about this particular processing? How can you substantiate your analysis? Consider referencing sources such as your privacy policy, publisher privacy policies, TCF UI requirements and policies, public articles, etc. Also include any evidence you have that helps to demonstrate users' expectations, such as surveys, market research, focus groups, and the like, where possible. You may be able to draw on pre-existing information for this purpose.

  - How likely are users to understand and expect the processing?
  - How did they get this understanding?
  - How would they know that your company, specifically, is processing the data, particularly if you do not have a direct relationship with them?
  - Is the processing novel, or is it consistent with what has been done for some time?
  - How old is the data? Would the data subject be surprised that it is still being processed?
  - How likely would users be to object to the processing or find it intrusive?
  - What evidence do you have of the above?
  - Would you be comfortable disclosing the processing publicly to data subjects?

[28] See https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/
[29] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/#LIA_process

- Safeguards and control: Measures you have taken to protect against the risks, and give users control, may weigh in favour of your legitimate interests.[30] The aim, of course, is to address potential harmful impacts that your processing might cause. For example, short retention spans reduce risks that stem from breach. Anonymisation prevents disclosure risks. Giving data subjects control lets them manage some of the risk.

  Again, if you have done a DPIA, you can draw generously from that work.[31] Line up the risks and impacts with the safeguards and controls. Some of the areas to consider:

  - How aligned is the processing with data subjects' expectations? What can you do to bring it more closely in line?
  - What retention periods will apply to the data?
  - How can a data subject exercise control over the processing? Cookie blocking? Opt-out?
  - How does the data subject learn about their ability to exercise control?
  - What is the scope of the control? Does it cease all of the processing or only a portion?
  - How persistent is the control?
  - What security controls are applied to the data?
  - What internal and external policies are in place to regulate the processing, and how do you ensure they are complied with?
  - Are there additional safeguards you could put in place to protect against the risks you have identified?

3.2 The decision

As set out at the beginning of this guidance, the LIA process is an objective assessment that should be approached without a predetermined expectation of the outcome of the balancing test.

There is no set algorithm that you can plug your answers into to get a determination at the end of your analysis above. It is more art than science. This is where expertise, experience, and objectivity are crucial, and why trained privacy professionals – often lawyers – are best situated to make the determination.

Taking into account all of the above, can you justify legitimate interests as a legal basis? Your analysis could be broadly summarised as: "We are doing A processing, with B data, to achieve C benefits for ourselves and others. This processing is necessary, because of _____. The processing has X/Y/Z risks to/impact on

[30] Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP217) (9 April 2014), available at https://ec.europa.eu/justice/article–29/documentation/opinion-recommendation/files/2014/wp217_en.pdf ("Here it is important to highlight the special role that safeguards may play in reducing the undue impact on the data subjects, and thereby changing the balance of rights and interests to the extent that the data controller's legitimate interests will not be overridden.")

[31] See our separate DPIA guidance for more details, including example risks, impacts, and mitigations. https://www.iabuk.com/news-article/digital-advertising-guidance-dpias-under-gdpr

data subjects. After applying X, Y safeguards, the residual impact on data subjects is _____. We believe our interests outweigh those impacts for the following reasons _____." If you are thorough, and can support your analysis, then you may be able to rightly claim a legitimate interests legal basis for the processing. However, there will be scenarios where relying on legitimate interests cannot be justified.

There are many resources you can, and should, consult to understand how to do the balancing test. Some links are provided in the Resources section below, but here are some particular considerations:

- The foundational principles of the UK GDPR require that data be processed "lawfully, fairly and in a transparent manner." Of course, you will not achieve a valid legitimate interests legal basis if these principles have not been met.
- Recital 47 explicitly states that fraud prevention and direct marketing may represent legitimate interests of the controller. Keep in mind, however, that your analysis cannot stop there; one cannot automatically process data for those purposes under a legitimate interests legal basis. The controller's interests might still be overridden by the data subject's.[32]
- Direct marketing is defined in s.122 of the UK Data Protection Act 2018. Do not employ an over-broad notion of what it is. There are specific requirements in PECR[33] for direct marketing that you should consult and ensure that you meet before proceeding with direct marketing under a legitimate interests legal basis. The cases where an ad tech intermediary can take advantage (as a controller) of the direct marketing caveats in PECR and UK GDPR are rare. The ICO (in the Experian Limited Enforcement Report[34]) noted that little weight can be attached to supposed benefit of the data subject consumer receiving direct marketing communications more 'appropriate' to them, when this is a consequence of processing and profiling to which they have not consented.
- Recital 47 also provides some hints about the controller's legitimate interests and when they might be overridden by a data subject's interests, including "where personal data are processed in circumstances where data subjects do not reasonably expect further processing." While EDPB guidance states that contractual necessity[35] is not an appropriate legal basis for advertising "simply because such advertising indirectly funds the provision" of the content,[36] the guidance does acknowledge that legitimate interest may be an appropriate legal basis as long as other legal requirements are met, including the notice

[32] See ICO, *Can we use legitimate interests for our marketing activities?*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/#marketing_activities.
[33] For more details see https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/
[34] https://ico.org.uk/action-weve-taken/enforcement/experian-limited/
[35] UK GDPR, Art. 6(1)(b)
[36] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (8 Oct 2019) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

requirements of Arts. 13 and 14.[37] Using the TCF helps toward meeting these requirements, but possibly not all of the way.

- The TCF, if you use it, is not in itself sufficient to establish a valid legitimate interests basis. You must have done the work to back it up before configuring legitimate interest as your legal basis in the GVL.
- The Article 29 Working Party published guidance on legitimate interests, which though the EDPB have not adopted, nevertheless remains relevant and continues to be cited. That guidance[38] lists some common contexts where legitimate interests may arise and is included here as useful context:
  - exercise of the right to freedom of expression or information, including in the media and the arts
  - conventional direct marketing and other forms of marketing or advertisement
  - unsolicited non-commercial messages, including for political campaigns or charitable fundraising
  - enforcement of legal claims including debt collection via out-of-court procedures
  - prevention of fraud, misuse of services, or money laundering
  - employee monitoring for safety or management purposes
  - whistle-blowing schemes
  - physical security, IT and network security
  - processing for historical, scientific or statistical purposes
  - processing for research purposes (including marketing research)
- Risks and harms associated with data are not binary. You can often attenuate risk, by minimising data.
- Risks and harms are also on a spectrum from more abstract, e.g. creepiness, to more concrete, e.g. identity theft. Of course, concrete harms will be given more weight, but take the full spectrum seriously. Be considerate of the wide range of concerns that your data subjects may have.
- Be cautious about data collected in association with cookies and the fact that the cookies require the provision of clear and comprehensive information to users, and consent for their use (to UK GDPR standards). This is a developing area of law, but there is a need to ensure that subsequent processing of data collected with cookies is disclosed and otherwise taken into account in legal basis analyses.[39]

---

[37] "In other instances, Article 6(1)(f) may provide a more appropriate lawful basis for processing. The legal basis must be identified at the outset of processing, and information given to data subjects in line with Articles 13 and 14 must specify the legal basis."

[38] Article 29 Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP217) (9 April 2014, *archived*) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[39] See, e.g. EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679* (May 2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/edpb-guidelines-052020-consent-under-regulation-2016679_en; ICO, *Update report into adtech and real time bidding* (June 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf; Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (June 2010, *archived*), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

- Relying on contractual controls alone is not sufficient. You need measures to ensure that contracts are adhered to.

If you have done all of the work above, and given the state of the art, though people may disagree about it, you should at least come to a *reasonable*, *supportable* conclusion. There will be ongoing debate among industry, regulators, and other stakeholders over what constitutes a sufficient LIA and when a legitimate interests legal basis is valid, or not. Eventually there may be regulator decisions or court opinions that shift the analysis one way or the other. That said, while there is some uncertainty, non-compliance can have consequences and DPAs will expect you to have due regard to relevant guidance on the legitimate interests legal basis, and LIAs.

3.3 Maintenance

Once complete, the LIA must be maintained. You should review it periodically to ensure it remains current, and update it when circumstances change.

Appendix A: Common risks in the digital advertising industry

This is a non-exhaustive list of common risks from processing activities in the digital advertising industry, with some particular considerations relative to each. It is provided as a useful reference. You should take care to think about risks to data subjects' rights and freedoms present in your circumstances that may not be represented here. For your own LIA you will need to analyse the impact and likelihood of the specific risks you identify. Some types of risk will have a more harmful impact on data subjects, if they are realised, than others, and you should take that into account in your analysis. The ICO and other data protection authorities will take this factor into account themselves when determining the appropriate level of regulatory action in the event of an infringement/breach.

Note: we are producing separate, specific guidance on Data Security, Retention and Storage that will contain some worked examples of risks that may occur in practice, and what measures can be used to mitigate those risks, and may be an additional useful reference here (once published).[40]

Risk	Considerations
Expectations and rights of the data subject	
Data subject would not expect the processing	Is the processing something data subjects expect or would they be surprised? Do you have an existing relationship with the data subject that may affect this? Particular things that could cause surprise include, for example, processing across seemingly unrelated contexts, matching data from different sources, cross-device, household, and social graphing. Providing sufficient information and transparency into the processing can help ensure data subjects are not surprised.[41]
Embarrassment	Could a data subject feel embarrassed if, for example, they receive an ad based on web browsing on a sensitive topic? What if someone else sees the ad, or the ad is delivered across a device graph?
Unwanted disclosure	Could data about the data subject be disclosed to other parties in ways that the data subject would be surprised by and wouldn't want? For example, could browsing history be matched to a retailer's CRM data?
Discomfort – a feeling of privacy invasion	Users may be made uncomfortable by certain processing, when they become aware of it. For example, many users feel discomfort when they are retargeted. The level of intrusion into a user's privacy should be considered in assessing the impact of the risk.
Inhibition of expression	Related to the above, there are concerns that when online users feel they are being observed, they are more inhibited in their online expression. For example, might they be less inclined to research a health condition or connect with other users of similar political persuasion, if they worry that their behaviour is being observed?
Not honouring data subject rights	Be careful about your ability to honour data subject rights. Be thoughtful about when and how you honour data subject rights, and where there are challenges, try to find a balance that is beneficial to the data subject and within the spirit (as well as the letter) of the law.

[40] The guidance will be published at www.iabuk.com/gdpr-hub
[41] The ICO has published guidance on privacy notices, including on drafting the content, and ways to provide privacy information.

Risk	Considerations
	Consider the overall impact on the data subject of the data you process and share with others. Look beyond your own four walls and consider the ecosystem you are in. Can the data subject effectively exercise his or her rights with respect to the data you process?
Fairness[42] discrimination and nature of the data	
Undue influence on a vulnerable population	Could data be used to identify vulnerable populations to influence or take advantage of them? For example, could income information or web search data be used to identify people with financial problems and offer them usurious credit products? Similarly, the elderly and children are often vulnerable to being taken advantage of – demographic information could be used to identify them online.
Disruption of politics	Related to concerns about influencing vulnerable populations, past elections have now shown how data can be used to segment and micro-target messages to specific populations, often to incite divisions and/or spread misinformation. Demographic data, political interest data, and location data in particular are susceptible to this type of use. **Note**: personal data revealing political opinions constitutes special category data under Art. 9 of the UK GDPR, which cannot be processed unless certain specific conditions apply/are met. For the purpose of this guidance we assume that there is no intentional processing of special category data. However, you should be aware of, and mitigate against, the risk of unintentional processing of special category data.[43]
Effects on eligibility for, or availability of, a product or service, such as insurance, financial or other	Could data be used to affect eligibility for offers of credit, insurance, or other products and services? Note that the ways audiences are selected for particular ads can potentially be used in a discriminatory way. For example, location information could be used to prevent ads for credit from showing in certain neighborhoods.
Effects on employment	Could data affect offers of employment, not only whether or not someone gets a job, but even whether or not they see an ad for the job?
Vulnerable groups	
Processing of data from vulnerable groups, such as children	Though you may not intend to, you might end up processing data about children. Not that you should try to identify children, but you might be able to identify and filter data that could indicate a data subject is a child. For example, you could identify websites directed at children and treat data from those sites differently, for example by not storing the data in personal form. The ICO's Age Appropriate Design Code is a statutory code under the UK Data Protection Act 2018 and applies to 'information society

[42] Personal data must be processed fairly. Some of the potential risks described here may also indicate that the intended processing is not fair. The ICO's guidance says: 'Processing of personal data must always be fair as well as lawful… In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually.' For more details see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/?q=fair#fairness

[43] For more details see our separate guidance: https://www.iabuk.com/news-article/digital-advertising-guidance-special-category-data-under-gdpr

Risk	Considerations
	services' likely to be accessed by children. It sets out standards for safeguarding children's personal data online. [44]
Data security and data sharing[45]	
Breach and misuse of the data	Even pseudonymous data presents risks from a data breach or other unintended access to data.
Misuse of the data by a legitimate possessor (as breach of contract or otherwise)	When you give employees access to data, or you share data with other parties, there is risk that they will misuse the data. You should have security and access controls, and policies, in place, and should make sure they are effective and adhered to on an ongoing basis. Contractual limitations when sharing data are helpful, but not enough. Use technical limitations when possible, and have procedures for compliance monitoring/enforcement where you must rely on contracts. See separate guidance, once published.
Non-compliance by processors	The UK GDPR requires certain contractual provisions to be in place with data processors. You, as controller, are responsible for monitoring/enforcement to ensure they adhere. Processors are another vector for data breach and data misuse. Use technical limitations, i.e. by minimising the data you share with the processor, and exercise your rights to monitor/audit processors' compliance.
Access by law enforcement or other legal process	Data collection by commercial entities can affect data subjects' legal rights in various ways, including that it is susceptible to access by law enforcement and through other criminal or civil legal processes. You should, of course, comply with the law, but you can take steps to reduce the risk. Minimising or deleting the data is helpful. You can also ensure that such legal requests are warranted and not overbroad. Use legal mechanisms available to you to protect the rights of the data subjects whose data you hold.
Re-identification of pseudonymous data	Data in the industry is often collected and processed in pseudonymous form. We generally consider there to be less privacy risk when we do not know the real identity of a data subject. Howeverit is sometimes possible to re-identify the data and match it to someone's real identity. This can happen well downstream from the context where the data was initially collected, and the parties involved in the initial collection, including the data subject may have had no expectation at the time that the data would ever become directly identified. Once data is re-identified, the risks are increased.

[44] For more details and to check whether it applies to your product/services, see https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services

[45] More details about risk and mitigation in this area will be provided in our forthcoming guidance on Data Security, Retention and Storage, which will be published at www.iabuk.com/gdpr-hub

Annex: Resources

Legislation

UK GDPR: The original content of the Regulation based on the EU GDPR is published at https://www.legislation.gov.uk/eur/2016/679/introduction. At the time of writing, the amendments that will be made to reflect the UK's exit from the EU have not yet been made to this version. The UK Government has published a 'Keeling Schedule' showing the changes to the original text at https://www.gov.uk/government/publications/data-protection-law-eu-exit

UK Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Privacy and Electronic Communications Regulations (PECR)
https://www.legislation.gov.uk/uksi/2003/2426

ICO Guidance/resources

ICO, *UK GDPR* https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/

ICO, *Legitimate Interests* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/

ICO, *Sample LIA Template*, https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx

ICO, *How do the cookie rules relate to the GDPR?*, https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/#GDPR3

ICO, *Update report into adtech and real time bidding* (June 2019)
https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

Article 29 Working Party and EDPB guidance/resources

In respect of the status and relevance of these resources, the ICO's guidance states (as at March 2021[46]):

> 'The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the UK GDPR. EDPB guidelines will no longer be directly relevant to the UK regime and will not be binding under the UK regime. However, they may still provide helpful guidance on certain issues.

[46] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

There are no immediate plans for EDPB guidance on legitimate interests under the UK GDPR, but WP29 Opinion 06/2014 (9 April 2014) gives detailed guidance on the key elements of the similar legitimate interests provisions under the previous Data Protection Directive 95/46/EC.'

Note: some, but not all Article 29 Working Party opinions have been endorsed by the EDPB, though they may still provide useful considerations. You should check for updates to EDPB documents and ensure you are referring to the latest versions (see https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en and https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (June 2010, *archived*) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (Apr 2014, *archived*) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (Nov 2019) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* (May 2020) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/edpb-guidelines-052020-consent-under-regulation-2016679_en

European Data Protection Board, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (Oct 2019) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (As last Revised and Adopted on 6 February 2018) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

IAB UK guidance/resources

GDPR hub https://www.iabuk.com/GDPR-hub

Cookies, consent & the GDPR https://www.iabuk.com/policy/digital-advertising-guidance-cookies-consent-gdpr

Special category data & the GDPR https://www.iabuk.com/news-article/digital-advertising-guidance-special-category-data-under-gdpr

Data Protection Impact Assessments under the GDPR https://www.iabuk.com/news-article/digital-advertising-guidance-dpias-under-gdpr

Note: guidance is forthcoming on Data Security, Storage and Retention

IAB Europe guidance/resources

IAB Europe Transparency & Consent Framework Policies https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

Other guidance/resources

Data Protection Network, *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation* (Version 2.0, 2018) https://dpnetwork.org.uk/dpn-legitimate-interests-guidance/

Irene Kamara and Paul De Hert, *UNDERSTANDING THE BALANCING ACT BEHIND THE LEGITIMATE INTEREST OF THE CONTROLLER GROUND: A PRAGMATIC APPROACH* https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Future of Privacy Forum, Nymity, *Processing Personal Data on the Basis of Legitimate Interests under the GDPR* https://info.nymity.com/hubfs/Landing Pages/Nymity FPF - Legitimate Interests Report/Deciphering_Legitimate_Interests_Under_the_GDPR.pdf

The Information Accountability Foundation, *Legitimate Interests and Integrated Risk and Benefits Assessment* https://secureservercdn.net/192.169.221.188/b1f.827.myftpupload.com/wp-content/uploads/2020/04/Legitimate-Interests-and-Integrated-Risk-and-Benefits-Assessment.pdf