VERSION 1
NOVEMBER 2020

GUIDANCE:
GDPR DATA PROTECTION IMPACT ASSESSMENTS (DPIA) FOR DIGITAL ADVERTISING UNDER GDPR

IAB EUROPE LEGAL COMMITTEE

iabeurope.eu

About IAB Europe

IAB Europe is the European-level association for the digital marketing and advertising ecosystem. Through its membership of media, technology and marketing companies and national IABs, its mission is to lead political representation and promote industry collaboration to deliver frameworks, standards and industry programmes that enable business to thrive in the European market.

About the Legal Committee

The Legal Committee brings together legal experts to help member companies and National IABs understand and assess the impact of EU legislation, European Court of Justice (CJEU) rulings and enforcement by Data Protection Authorities (DPAs) as they pertain to digital advertising. It works to develop agreed interpretations of the law and compliance guidance to the market on key issues such as definition of consent, legitimate interest, pseudonymization, verification for access requests and other data subject rights, that can be promoted with key external stakeholders, including EU and local regulators, advertisers and consumer associations. The Legal Committee is also involved in the preparation of IAB Europe responses and comments to EDPB and national guidelines, and other policy documents.

Contacts

Townsend Feehan (feehan@iabeurope.eu)
CEO, IAB Europe

Filip Sedefov (sedefov@iabeurope.eu)
Legal Director (Privacy), IAB Europe

Contents

GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR

Note: IAB Europe and IAB UK have worked to develop this guidance jointly. This version is not intended to specify the rules applicable in individual jurisdictions and does not assume data processing is governed by a particular regulator. While it provides specific examples from different jurisdictions, it is mainly based on a direct interpretation of the requirements in GDPR. Companies whose data processing is regulated by the UK's ICO, can refer to the equivalent version of this guidance, available from IAB UK at www.iabuk.com.

1. About this Guidance

1.1 Purpose of this guidance and how to use it

The purpose of this guidance is to provide a practical guide to carrying out data protection impact assessments (DPIAs) in line with the EU's General Data Protection Regulation (GDPR). The document provides background and describes the DPIA process 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. The aim is to provide an accepted, widely adopted, standard for evaluating and managing risks associated with personal data processing in the industry, which may evolve over time in accordance with regulatory developments and market practices.

The European Data Protection Board (EDPB) has specifically encouraged this kind of industry-specific DPIA framework because of how it can be shaped to the particular types of data,

processing, and risks that arise in an industry.[1] This guidance aims to particularise existing guidance[2], in the context of typical digital advertising activities and data processing.

This guidance document is not intended to provide a form to be filled, or to provide specific content for your DPIA, but rather is a roadmap for incorporating the DPIA process into a company's normal course of product design and development. Companies should adapt this approach into whatever format fits best with the way they work. You might build it out in a wiki or a spreadsheet or an issue tracking tool, or some combination thereof.

The guidance is also intended to be straightforward enough that it can be put to successful use in the hands of front-line employees, in companies of varying sizes, especially those not large enough to have armies of lawyers, compliance professionals, and outside consultants. It should not rely on an in-depth academic understanding of applicable privacy law and risk management theory. In fact, the main qualification for successful and proper use of the DPIA framework is a strong understanding of the data processing in question, all of the possible risks that could stem from the processing, and the effectiveness of available risk mitigation approaches.

In that spirit, note that this guidance does not provide legal advice or analysis. It provides a roadmap and guideposts to building a correct process for conducting DPIAs in the industry. It highlights key issues and suggests approaches to certain concept relevant to our industry, in a way that that engineers, product managers, and other non-privacy/legal staff can appreciate. One should keep in mind that a significant amount of legal nuance and detail is necessarily left to your privacy and legal professionals to bring to the table.

---

[1] 'The EDPB encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation.' EDPB Guidelines, p. 17. The EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679 are available at https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[2] See for instance 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

The guidance is not a standalone document and should be read and used in the context of a full understanding of wider GDPR principles and requirements, including whether and when a DPIA is required, and the role of the DPO, and should be read alongside other relevant guidance. We have signposted to some of this guidance throughout the document, and the Annex at the end provides a detailed list.

1.2 Who is the guidance for?

The guidance is primarily intended for use by digital advertising technology companies of varying natures and types, and the advertisers, agencies, and publishers that work with them and share data with, or receive data from, them. Within companies using the guidance, it is recommended that a cross-functional team, including such roles as product managers, engineers, business managers, privacy professionals, and lawyers, be convened to translate the guidance into a form and format that works well with the company's own processes.

Ownership over the DPIA process should be given to one or more employees having a level of knowledge and seniority that enables them to ensure the proper completion of the process from start to finish. However, every employee involved in the data processing should have an understanding of, and ownership over, their particular role in the process. The DPIA is a team effort. Therefore, training of relevant employees should be a key part of implementing the DPIA process.

Companies who have a DPO – and most using this DPIA process should – must consult their DPO when carrying out the DPIA and document their advice as part of the process[3] (see section 3 for more details of who should be in your DPIA team).

[3] GDPR, Art. 35(2).

1.3 Scope of this guidance

This approach is geared toward the assessment of risk from data processing functions associated with programmatic digital advertising, i.e. ad tech and RTB. It is not intended for general business data processing, even in ad tech companies.

The approach is built around common data and risks associated with digital advertising activities. The guidance and examples are not comprehensive, exhaustive or definitive. Companies using this guidance must bring the full legal nuance to their circumstances and must consider whether there are types of data or risks that are applicable to their circumstances but not represented in these materials.

This guidance makes use of the taxonomy of processing activities – or *purposes* and *features*– elaborated in IAB Europe's Transparency & Consent Framework (TCF).[4] We make use of the TCF both because it provides a comprehensive and useful taxonomy, but also because many, maybe most, companies in the industry will be using the TCF and therefore aligning their compliance activities with the TCF definitions. By aligning our guidance with the TCF, for example, a company can directly tie their DPIA process to their legal basis analysis for the TCF purposes they are engaged in.

That said, it is each company's responsibility to ensure they are comprehensive with respect to their own unique data and processing activities. A key tenet at the heart of this process is that it is not a pro forma exercise, and must not be done by rote, but rather must be thoughtfully tailored to each circumstance. It is not a paint-by-number and one size does not fit all. Bear in mind also that under the GDPR accountability principle you must be able to demonstrate your compliance and your record of your DPIA should therefore be sufficiently detailed and descriptive so that your reasoning and decision-making is clear and comprehensible to others (for example an SA, should they need to review it).

[4] https://iabeurope.eu/tcf-2-0/

1.4 Relationship between LIAs and DPIAs

You may notice a resemblance between a legitimate interest assessment (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 identify and mitigate the likelihood of high risks to data subjects, a LIA is legal analysis – in the situation where you have identified legitimate interests as your intended lawful basis for processing personal data – that you must undertake prior to processing, to determine whether the controller's and data subject's interests are sufficiently balanced to allow the processing without acquiring the data subject's consent.

In almost all cases, a company should have completed a DPIA process prior to finalising a LIA. And, if legitimate interests is the intended legal basis for processing, the LIA balancing test should be kept in mind as the DPIA is in progress. As the LIA is begun, the results from the DPIA, in particular the residual risks, will be important inputs into the LIA. In fact, if your DPIA is thorough and correct, it should include most of the underlying work for the LIA. If you are processing personal data on the basis of legitimate interests, or are intending to do so, and have not yet completed a DPIA process, you should consider whether one is necessary, particularly if your LIA identifies significant risks. For more details on LIAs, see our forthcoming LIA guidance.

2. About DPIAs

2.1 What is a DPIA?

A DPIA is a risk management process not unlike other risk management processes. Under the GDPR, DPIA 'is a tool for managing risks to the rights of the data subjects, and thus takes their perspective.'[5] The aim of the DPIA, therefore, is to objectively assess the risks and then take steps to mitigate those risks. It should not be treated as a post-hoc justification exercise.

[5] EDPB Guidelines, p. 17.

Take note of the characterisation of a Data Protection Impact Assessment as a process.[6] Think of the term 'assessment' as referring to a dynamic action, not a static record. To the extent a DPIA is a document, it is an ongoing record of a product development process that pays close attention to, and works hard to mitigate, the risks associated with processing personal data.

Therefore, the DPIA process described in this guidance is not designed as a standalone piece of documentation – though you must document your DPIA process – but rather as an industry-specific approach for incorporating DPIA into the product development process of digital advertising companies. Although each individual organisation must take their own particular circumstances into account in undertaking a DPIA, using this approach helps ensure you are taking an approach to your process that is in line with industry standards, and which includes commonly used data and commonly understood risks in the industry.

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.

2.2 When is a DPIA required?

All data controllers are required to consider the likelihood and severity of risk to individuals in relation to their processing regardless of whether they are also required to do a DPIA. Article 24 (general controller obligations), Article 25 (data protection by design) and Article 32 (security) all require a controller to consider whether they have appropriate technical and organisational measures to ensure and demonstrate compliance with the GDPR.

DPIAs are a further statutory requirement to perform and document an assessment of risk where processing is likely to be high risk. Under GDPR Art. 5, a Data Protection Impact Assessment (DPIA) is required where a data processing activity is 'likely to result in a high risk to the rights and freedoms of natural persons.'[7] While the GDPR itself (Art. 35(3)) includes a handful of specific

[6] 'A DPIA is a process for building and demonstrating compliance.' EDPB Guidelines, p. 4

[7] GDPR, Art. 35.

cases where a DPIA is required, under Art. 35(4) and (5) local Supervisory Authorities (SAs) are also to produce their own lists of processing operations that trigger a DPIA requirement.

The EDPB has published extensive guidance on DPIAs, including nine criteria that should be taken into account by SAs when producing their lists. 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679,' (originally published by the Article 29 Working Party and revised and adopted by the EDPB on 4 October 2017.) Additionally, the EDPB have provided opinions applying their criteria to the national lists, through the consistency mechanism, as provided for in the GDPR.

In practice this means that upon contemplation of any new personal data processing, a determination must be made as to whether a DPIA is required, with consideration given to the GDPR and any applicable triggers promulgated under Art. 35(4). The DPIA must be completed prior to commencing the processing, to inform your decision about whether or not to go ahead and may cover a single processing operation or a group of similar processing operations. At the start of every process to evaluate new data processing activities, if you choose, you can justify (and document) why a DPIA is *not* needed. Otherwise, you will work through the DPIA process to identify and manage risk associated with the processing. The EDPB explicitly recognise that a processing operation may meet the criteria, but still not require a DPIA;[8] however, these cases will be the minority in the context of digital advertising and RTB. Taking a default approach to DPIAs provides not only the obvious benefit of compliance with the law but will help companies to incorporate and refine a privacy by design process, and ensure a high degree of awareness within companies of the nature of processing and the associated risks.

If you do make a determination that a DPIA is not needed, you should be certain as to your basis for doing so. Non-compliance can lead to fines.[9] Moreover, keep in mind that DPIA is a useful tool regardless of the requirements, and the process described here closely resembles privacy by

[8] 'A processing operation may meet the EDPB's criteria for high risk, but still may be considered by the controller not to be 'likely to result in a high risk'. In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.' EDPB Guidelines, p. 12.

[9] EDPB Guidelines, p. 4.

design and default approaches that companies should be incorporating into their product development irrespective of DPIA requirements.

For our purposes, because most of the processing that takes place within the digital advertising industry generally, and RTB specifically, will meet default triggers for a DPIA as established by the EDPB and various national SAs[10] pursuant to the GDPR, we start from a position of assuming that a DPIA process will be necessary. Despite the fact that under the risk-based approach embodied by the GDPR, 'carrying out a DPIA is not mandatory for every processing operation,'[11] because of the nature of most of the processing involved in RTB and related or ancillary functions, we suggest that DPIA should be the default for the industry (while recognising that, ultimately, whether or not a DPIA is required is a legal decision for each organisation to take itself).

Please note that our position on DPIA by default **does not** mean that we consider that all processing in the industry is necessarily high risk, but rather that in our view, because so much processing in the industry has *indicators* of likely high risk, as identified by the EDPB and SAs, it is a best practice to employ a DPIA process as a regular part of product development.

3. How to do a DPIA

As we have emphasized above, a DPIA is a process, not a product. It should be an iterative process, done in the normal course of product development, at least when required (as set out above), if not by default for all processing, as we suggest.

Moreover, the results of the DPIA must be considered: the processing should not commence until the DPIA process has been applied and a decision made as to whether to proceed, and if at the

[10] For example, the EDPB's nine criteria include: evaluation or scoring, including 'behavioural or marketing profiles', systematic monitoring, sensitive or highly personal data, data processed on a large scale, matching or combining data sets, and innovative use of technology. The national SA lists consistently include triggers that implicate various functions within the digital advertising industry, such as tracking, invisible processing, big data analytics, profiling for marketing, collecting browsing and viewing history, data collected via third parties, observing data subjects' online behavior, and so on.

[11] EDPB Guidelines, p. 5.

conclusion of your DPIA there is residual high risk, Art. 36 requires consultation with the SA before processing.[12] If this is the case, use this information to carefully consider why there are residual high risks and whether the processing is necessary, can be justified, and meets other GDPR requirements, such as the fairness principle.

As noted above, irrespective of DPIA requirements, the GDPR requires data controllers to assess the risk to data subjects of their data processing. However, your development process works, DPIA, and more generally, privacy-by-design – as a GDPR requirement [13] – should be incorporated as part of it, not a process in parallel and not a checkpoint at the end.

Most companies will not be starting from scratch. They will be adapting and enhancing existing processes to implement this DPIA guidance. It may be the case for some companies that to a large extent they are already doing DPIAs but need to add formality and documentation. For others, incorporating DPIAs will involve a lot of net new process, and probably considerable trial and error before they get to a place where it works well and enables them to draw relevant conclusions as to the legality and impact of any processing operation.

3.1 General observations

i. Note on objectivity and necessity

Throughout this document, reference is made to objective analysis or the data subject's perspective, as well as the necessity of the processing. Objectivity means stepping back and taking a view from outside your company. Necessity implicates the question of whether a less privacy-intrusive alternative could be used. There is something of an art to this analysis, as it depends on your perspective and your level of abstraction. A full discussion of objectivity, balance,

[12] When a Supervisory Authority is consulted, it will assess the DPIA. For example, in its guidance, the UK's ICO notes: 'We will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases we may advise you not to carry out the processing because we consider it would be in breach of the GDPR. In appropriate cases we may issue a formal warning or take action to ban the processing altogether.' See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#dpia5

[13] GDPR Art. 25 sets out the requirement for data protection by design and by default.

and GDPR principles is beyond the scope of this guidance, but your DPO and privacy/legal professionals should be able to guide you.

ii. When to start your DPIA

Your DPIA should begin early in the product development process. It is recommended to weave in privacy considerations at the conception and ideation stages, to help ensure that development reflects privacy-by-design and default, which is a requirement under GDPR. If privacy and impact assessment is brought in too late in the process, it wastes time, misses opportunities for better privacy, forces suboptimal compromises, and risks non-compliance (for example with Articles. 24, 25, 32, 35, 36 that cover data controller responsibilities; data protection by design and default; security; and DPIA requirements).

iii. Who is involved

DPIA should be carried out cross-functionally, with a group of experts who individually and collectively represent the knowledge, expertise, and experience necessary to deeply understand the context of the processing and the risks to the rights of the data subjects. For example, a DPIA team might consist of the normal product team – product managers, engineers, designers, information security staff – supplemented with a privacy professional, and periodically including the DPO for consultation, including at the end point when you are making the final decision as to whether or not to proceed with the processing.

iv. Using the guidance materials

These guidance materials are not intended to be used off-the-shelf and there is no 'one size fits all' approach. Take the materials provided here as a basis to guide you, and incorporate them into your own tailored process that fits with the way your company operates, and the scenarios you are assessing. Use whatever tools you want: spreadsheets, bug trackers, version control systems, wikis.

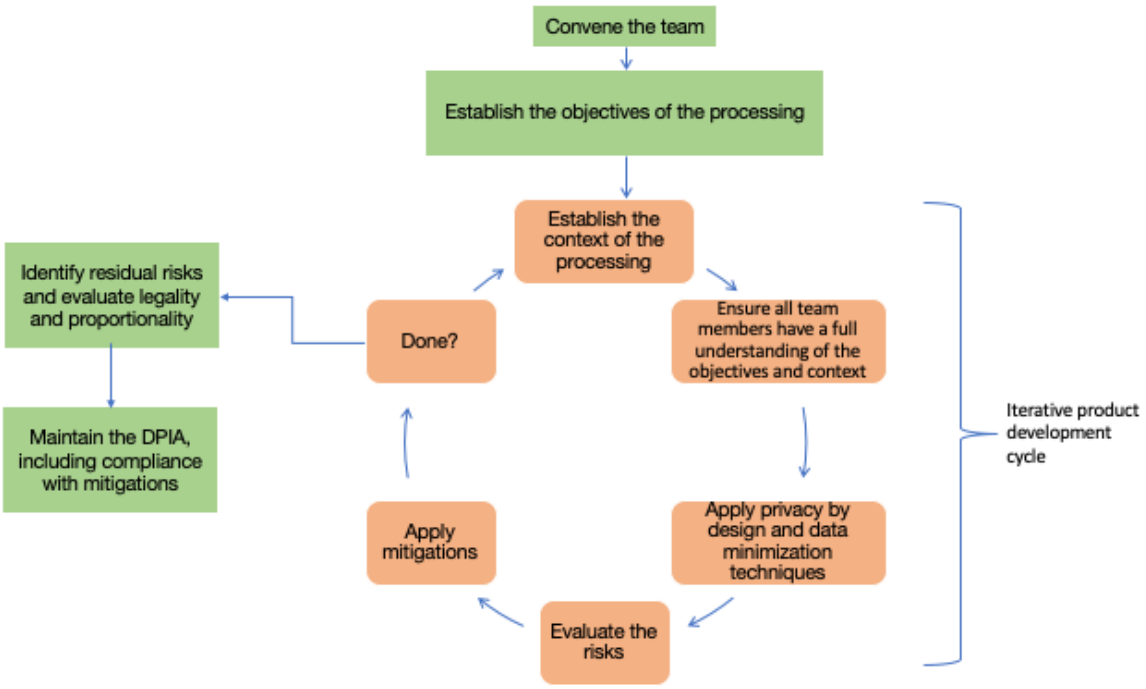
Whatever you use, it should include a record of your process and the decisions you make as you go, and it should be kept up to date. In the end, you should be able to point to records that demonstrate the soundness of your DPIA process, and your documentation needs to be

sufficiently detailed and descriptive for a someone who is not an expert in your sector or industry (such as a regulator) to understand.

3.2 Overview of the process and stages

DPIA, and privacy by design, requires a process of iteration (and sometimes negotiation.) As shown in the diagram below, at the core of the process is an iterative cycle whereby data use is evaluated, risks understood, mitigations applied. The cycle is repeated as needed until a somewhat final state is reached, after which a decision made on whether the effects on data subjects (individually or collectively) of a processing activity are disproportionate and should not be carried out, and the 'final' product can be assessed for full compliance with the GDPR. Of course, if any high risk remains from the processing after going through a DPIA process, you must consult your Supervisory Authority as required by Art. 36 (as described in Section 3.3). You should approach the process objectively and with an open mind, using it as a tool to guide your decision-making, and be prepared for different outcomes, including that you may identify risks that cannot be appropriately mitigated and that mean the processing you are assessing cannot go ahead.

Note: the cycle shown here is illustrative, based on typical product development cycles, but is not prescriptive. It shows the steps you should go through, but the precise ordering and sequencing can be adapted to suit your specific circumstances.



In reality it is not done in such delineated stages, but rather there is a quality of doing, or at least keeping in mind, all of the stages at once as product development proceeds. From the earliest stages of product development, you should be thinking about your path to ensuring that the processing is necessary, fair, proportional, and of course, legal.

Overview of the stages

(See the guidance that follows this table for a full description of each stage).

Convene the DPIA team.	When does product development start? Is it at the conception of the idea or the identification of the need? Is it during ideation? The research and experimentation phase? Each company will have its own process, but the DPIA process should begin early. Privacy considerations should be taken into account from the earliest stage, reflecting data protection by design and default, which means bringing in the right people early, and identifying the right people to be responsible for review and sign-off at the end.
Establish the objectives of the processing.	Clearly lay out, objectively, what it is that the data processing is intended to accomplish, and how the processing leads to the intended result. This is essential for most steps of the process: mitigations, legality, proportionality. It is sensible and acceptable to group related or similar processing activities, so you may have multiple objectives.
Establish the context of processing.	The context includes all of the relevant facts about the processing: the data to be used, the flow through different systems, the time to be retained, location of storage, transborder transfers, transfers to third-parties, etc. The context may be fleshed out and may evolve over time as the team iterates through the process.
Ensure all team members have a full understanding of the objectives and context.	It is imperative to ensure all members possess a thorough understanding of, and agree on, the objectives and the context. Without a full understanding of the objectives and the context, a team member cannot fully participate. He or she is not fully equipped to identify risks and propose mitigations that are consistent with the objectives. Similarly, without agreement among the team, the process will not operate correctly. Too

	often, because the product development process is moving quickly, people gloss over details or disagreements, and let things pass without asking questions. It is not unusual to waste considerable time talking past each other because the people involved do not have a common understanding of the objectives and/or context. That is why it is included here as an explicit step.
Apply data minimisation and privacy by design (PBD) techniques.	Every company should be taking this approach in its product development process. The GDPR requires it.[14] This means making design choices in favour of privacy - implementing the data protection principles and protection of data subjects' rights and freedoms – from early in the development process, and it means reducing data processing to the minimum necessary to meet your objectives, or even consider more privacy-friendly alternatives. There is further discussion below regarding common techniques.
Evaluate the risks.	Given the context – the data to be processed, the retention, the sharing, etc. – and after data minimisation and PBD techniques are applied, what are all of the possible risks to the rights and freedoms of the data subject? See below for further discussion of how to identify and evaluate risks, as well as discussion of common risks associated with processing in the digital advertising industry.
Apply mitigations.	This is a distinct step from data minimisation and privacy by design (both of which are requirements in themselves), even though those also serve as mitigations to privacy risks. The aim in this step is to apply further mitigations given the risks that remain after the minimisation and privacy by design stages.
Iterate until done.	At some point the cycle is roughly complete. Risks have been identified and evaluated, mitigations applied, and not much more can be done. At that point you have a 'final' product design that

[14] See Arts. 24, 25, and 32, (data controller responsibilities; data protection by design and default; security) and Recital 78 (appropriate technical and organisational measures).

	can be given a final assessment, under the next stage, as to whether it is ready for production.
Identify residual risks and evaluate under GDPR principles, such as fairness and proportionality.	Once at an appropriate stage in the design process, you can look at what you have and evaluate whether the processing is proportionate to the need and the risk, whether you have met the legal bar for achieving the legal bases under which you will conduct the processing, and whether the processing otherwise adheres to the principles and requirements of the GDPR. This must be an objective analysis, and if the processing proposed in this 'final' state still produces high risk you must either go back and find alternatives; decide not to proceed; or consult with your Supervisory Authority as required under Art. 36. You'll include your DPO and possibly senior management (and/or whoever you have identified as having ultimate approval) in this analysis.
Maintain the DPIA, including compliance with mitigations	The DPIA creates an ongoing obligation. You must ensure that your analysis remains true. You do this by keeping the context of processing up to date, and re-evaluating when changes occur. You also ensure that privacy by design features, data minimisation and risk mitigations are complied with.

Note that there are factual and analytical stages of the process. Don't give either short shrift. A solid foundation of factual information is necessary to build your analyses on.

3.3 DPIA process

Stage 1: Convene the team

Convene the DPIA team.	When does product development start? Is it at the conception of the idea or the identification of the need? Is it during ideation? The research and experimentation phase? Each company will have its own process, but the DPIA process should begin early. Privacy considerations should be taken into account from the earliest stage, reflecting data protection by design and default, which means bringing in the right people early, and identifying the right people to be responsible for review and sign-off at the end.

Determine who is involved in the DPIA process.

- Product managers and engineers developing the product(s)
- Privacy Product Managers/Engineers
- Information security staff
- UI/UX designers
- Privacy specialist/lawyer
- DPO[15]

Who has ultimate ownership over completing the DPIA?

Who other than the DPO must sign off on the DPIA, in particular with respect to residual risk?

Stage 2: Establish the objectives of processing

Establish the objectives of the processing.	Clearly lay out, objectively, what it is that the data processing is intended to accomplish, and how the processing leads to the intended result. This is essential for most steps of the process: mitigations, legality, proportionality. It is sensible and acceptable to group related or similar processing activities, so you may have multiple objectives.

[15] The DPO's involvement is required under Art. 39, and the DPO's participation must be independent per Recital 97.

Describe broadly what product or products are being developed, the nature of the personal data processing involved, and the objectives for the products/processing. Include consideration of the following:

- What do you hope, or intend, to accomplish?
- What are the benefits to your company, society, the data subject?

This can be done in prose, or in the form of a presentation, diagram, or whatever works best for you, as long as you can be as thorough as is required and the materials provide a sufficient basis on which all involved personnel can participate. The point is to have a record and to have reference materials available to the teams working on the product.

You will need to be able to match up the processing to the objectives and show the necessity of all of the processing for the particular objectives. As you do this you need to think about objectives and necessity from differing perspectives. While certain processing may be necessary to make a particular product work, this does not necessarily mean you can or should be seeking to justify it on that basis. It could be that there is an alternative product or design that would meet objectives with less intrusion on or risk to individuals' privacy.

Stage 3: Establish the context of processing

Establish the context of processing.	The context includes all of the relevant facts about the processing: the data to be used, the flow through different systems, the time to be retained, location of storage, transborder transfers, transfers to third parties, etc. The context may be fleshed out and may evolve over time as the team iterates through the process.

You must identify in detail all of the factual circumstances of the processing. This context will be updated over time, as the product design evolves. You must explain how all of the processing is necessary to meet your objectives.

Below are some things to consider as you do this. This list is by no means comprehensive. Think broadly about your specific circumstances. Additionally, you should plan on taking into account more detailed guidance on these issues from the IAB, regulators, and other sources.

- What types of personal data are being processed? (Consult Appendix A for a non-exhaustive list of commonly used data types, along with some notes about each.)
- What identification and state maintenance methods will you use?
- Will you process any sensitive or special category data? (Is it possible you may do so, even if you do not intend to, for example, from bid requests or pixels calls?)[16]
- Will you store and/or access information on a device (TCF purpose 1)? If so, how will you acquire consent?
- From what geographical areas will the data be collected?
- From approximately how many data subjects will data be processed (in orders of magnitude, i.e. thousands, hundreds of thousands, millions)?
- What is your relationship with the data subjects?
- Where will the data be stored?
- Are any processors involved? If so, you'll need to elaborate on how you are managing risks that stem from using processors.
- Any transfers or storage across national borders? If so, where?
- For all of the data, what is your schedule for de-identification, anonymisation, and/or deletion of the data? (See notes about this topic in the minimisation and mitigations sections.)
- Will you combine data from different sources or contexts? Is so, describe all of the sources and the process for matching and combining the data. Bear in mind that combining data can, depending on a number of factors (the nature of the data, what it will be used for, etc.), potentially increase the risk of special category data arising.
- Will the processing involve the creation of profiles?
- Describe **in detail** the purposes of the processing. Categorise the purposes according to the TCF taxonomy, as possible. (Refer to Appendix A of the TCF policies for definitions and guidance on the content of each purpose.[17]) Describe separately purposes that do not fit squarely within TCF definitions. **Note**: these TCF purposes are a useful framework for describing the context of processing and for matching the processing to legal bases (if

[16] Note that IAB UK has, for instance, produced dedicated guidance on special category data and risk: https://www.iabuk.com/news-article/digital-advertising-guidance-special-category-data-under-gdpr
[17] https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

you use the TCF) but should not be considered a shortcut to fully describing the processing and its purpose.

  - Create a personalised ads profile (TCF purpose 3)
  - Select personalised ads (TCF purpose 4)
  - Create a personalised content profile (TCF purpose 5)
  - Select personalised content (TCF purpose 6)
  - Measure ad performance (TCF purpose 7)
  - Measure content performance (TCF purpose 8)
  - Apply market research to generate audience insights (TCF purpose 9)
  - Develop and improve products (TCF purpose 10)
  - Ensure security, prevent fraud, and debug (TCF special purpose 1)
  - Technically deliver ads or content (TCF special purpose 2)
  - Match and combine offline data sources (TCF feature 1)
  - Link different devices (TCF feature 2)
  - Receive and use automatically sent device characteristics for identification (TCF feature 3)
  - Use precise geolocation data (TCF special feature 1)
  - Actively scan device characteristics for identification (TCF special feature 2)
- Other purposes that fall outside of the above?
- Where and how does a data subject receive notice of the processing?
- To what extent, or in what ways, is the processing new? Is it a well-established model or a novel use of data?
- What choices does a data subject have with respect to the processing?
- For any data will be shared with third parties:
  - What are the reasons for sharing?
  - What specific data will be shared?
  - If recipients participate in the TCF, will you filter data based on the TCF Consent String?
  - What controls are in place with respect to this sharing and any subsequent processing, and how are these controls enforced?

Stage 4: Ensure all team members have a full understanding of the objectives and context

Ensure all team members have a full understanding of the objectives and context.	It is imperative to ensure all members possess a thorough understanding of, and agree on, the objectives and the context. Without a full understanding of the objectives and the context, a team member cannot fully participate. He or she is not fully equipped to identify risks and propose mitigations that are consistent with the objectives. Similarly, without agreement among the team, the process will not operate correctly. Too often, because the product development process is moving quickly, people gloss over details or disagreements, and let things pass without asking questions. It is not unusual to waste considerable time talking past each other because the people involved do not have a common understanding of the objectives and/or context. That is why it is included here as an explicit step.

Have all DPIA team members reviewed the objectives and context of processing?

Is it agreed that the objectives and context of processing are accurate and complete?

Are there any open questions, or areas of confusion or disagreement, that must be resolved before proceeding to the next stage?

Stage 5: Apply privacy by design and data minimisation techniques

Apply data minimisation and privacy by design (PBD) techniques.	Every company should be taking this approach in its product development process. The GDPR requires it.[18] This means making design choices in favour of privacy - implementing the data protection principles and protection of data subjects' rights and freedoms – from early in the development process, and it means reducing data processing to the minimum necessary to meet your objectives, or even consider more privacy-friendly alternatives. There is further discussion below regarding common techniques.

[18] See Arts. 24, 25, and 32, (data controller responsibilities; data protection by design and default; security) and Recital 78 (appropriate technical and organisational measures).

Much has been written about how to do privacy by design. We will not review it here but will cite some resources in the resources section (see Annex) below. The gist of it is that you should – are required to – make privacy considerations integral to the design process and the design, wherever possible, rather than treating privacy as something that is grafted onto an already finished product. However, most (if not all) companies in this sector are engaged in activities that the EDPB national DPAs have flagged as likely to be high risk (see section 3 of this guidance), so GDPR compliance is likely to require retrospective review and adaptation of existing products. Of course, for companies participating, the TCF may be a considerable help in that it provides a means of transparency and choice that was not available pre-GDPR.

Therefore, the work in this stage is to apply data minimisation and privacy-by-design techniques to your in-process product design, or, for existing products, to review them through this lens. As part of this you should always be thinking about whether the product path you are on is the right one, or whether less privacy-intrusive alternatives might be available.

So, for each purpose of processing and type of personal data described in the context of processing:

- Can you meet your objectives with less, or even no, personal data?
- Where can you use less privacy-intrusive processing to achieve your objectives?
- Can you make the processing more transparent to the data subject?
- Where can you reduce the precision of data?
- Have you reduced the retention to the minimum necessary? You must have a discrete retention period for all data.[19]

Consult Appendix A for considerations in relation to particular data types. Bear in mind that you must comply with the principles of the GDPR[20] as well as its practical requirements, and these principles are a useful guide for this stage of the DPIA process.

[19] The IAB is producing separate guidance that will cover retention periods, and a template retention schedule. This will be available on our website once published: www.iabuk.com/gdpr-hub
[20] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Other considerations:

- Where and how does the data subject receive notice of the processing? Can you offer more transparency?
- What choices does the data subject have with respect to the processing? Can you offer more choice?
- Have you properly implemented the TCF, and are you applying TCF signals to this processing?
- Where does the data come from and where does it go? Is it sourced properly (legally, etc)? Do you have appropriate controls in place when transferring on?
- Does, or will, your privacy policy sufficiently describe the processing?
- Is, or will, the processing be accurately reflected in your records of processing (ROPA), as required under Art. 30?

Stage 6: Evaluate the risks

Evaluate the risks.	Given the context – the data to be processed, the retention, the sharing, etc. – and after data minimisation and PBD techniques are applied, what are all of the possible risks to the rights and freedoms of the data subject? See below for further discussion of how to identify and evaluate risks, as well as discussion of common risks associated with processing in the digital advertising industry.

You need to consider, given each of your intended processing operations and the data involved, as elaborated in your context of processing, and with the data minimisation and privacy by design approaches applied in Stage 5, what risks remain? For each risk, you need to objectively examine the potential impact, and the severity of that impact, on the data subject and the likelihood of it occurring. There are many ways to conduct risk assessments, and an example methodology is provided in Appendix A: Risk Assessment.

Consult the table of common risks in digital advertising in Appendix C (note, this is not exhaustive, and you need to think about your own products and processes, and the attendant risks of those). For each type of data and each processing operation, which of these apply? What other risks can you think of?

What other risks apply to your circumstances? Be broad and inclusive. List them all for the team to consider. Think from the perspective of data subjects who may have various levels of ability to understand the processing that is taking place, and the consequences of the processing, and may have varying subjective views on the risks. Some SAs have expressed the concern that '…in RTB the privacy information provided often lacks clarity and does not give individuals an appropriate picture of what happens to their data'.[21]

Stage 7: Apply mitigations

Apply mitigations.	This is a distinct step from data minimisation and privacy by design (both of which are requirements in themselves), even though those also serve as mitigations to privacy risks. The aim in this step is to apply further mitigations given the risks that remain after the minimisation and privacy by design stages.

As previously explained, your DPIA should be an iterative process, done in the normal course of product development, that helps you to understand, evaluate and mitigate the privacy impact and risks to data subjects. At this stage, you must take each of the outstanding risks identified in the previous stage and try to apply further mitigations to reduce those risks or privacy impacts.

Common mitigations used in the industry include:

- Additional transparency and control for data subjects
- Internal policies for purpose limitation, retentions, security
- Contractual limitations (for cases of sharing)
- Further data minimisation

You should also consult the considerations relative to particular data types in Appendix B, and the notes related to common risks in Appendix C, for ideas about how to think about risks in our industry.

[21] See UK's ICO Update Report on RTB at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf, p19

Notice and transparency:

- How will you provide notice to the data subject of the processing?
- Does the notice thoroughly describe the processing in easy-to-understand terms? For example, the UK's ICO has published guidance on privacy notices, including on drafting the content, and ways to provide privacy information.
- If using the TCF, does your processing fit within TCF-defined purposes and features? If not, how will you deal with the processing that does not?
- Is the processing transparent to users? For example, cookies are visible to the user, probabilistic IDs are not.

Policy:

- What is the security policy applicable to the data?
- Is access to the data controlled under a 'least privilege' model?
- What internal policies govern the use and sharing of the data? For example, and as applicable to the processing:
    - Do you have policies banning certain types of segments?
    - Policies banning ads to vulnerable populations?
- What controls are in place to ensure compliance with the policies? These are essential to ensuring that your policies mitigate risk in practice.

Storage and retention:

- Do you know where the data will be stored?
- If data will be stored or transferred across borders do you have appropriate safeguards in place, including required contractual terms?
- Do you have a discrete retention period for all data?
- How will you ensure that data is deleted?

Data subject rights[22]:

- How are you honouring all data subject rights, as required under the GDPR?
- How have you implemented the right to object to processing, and to withhold and/or revoke consent?
    - What are the limitations of your implementation? Can you compensate?

Sharing data with other parties:

- What diligence will be done with respect to data recipients before sharing?
- Do you have contracts with all recipients?
- Are, or will there be, contractual limitations on the recipients' processing of the data? If so, what are they?
- How have you minimised the data that will be shared?
- How are data subjects informed of new controllers receiving the data?
- How will you monitor and enforce compliance with contractual limitations?
- For recipients that participate in TCF, are you filtering data based on the TCF consent string?
- For recipients who do not participate in the TCF, what measures do you take to make sure they have a legal basis for processing the data?

Working with processors:

- How do you vet processors to ascertain their trustworthiness and reliability before sharing data with them?
- Do you have a DPA in place with all processors?
- How have you minimised the data shared with the processors?
- What measures will you use to monitor compliance with the DPA?

[22] For more details on data subjects' rights, and guidance, see e.g., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Stage 8: Done?

Iterate until done.	At some point the cycle is roughly complete. Risks have been identified and evaluated, mitigations applied, and not much more can be done. At that point you have a 'final' product design that can be given a final assessment, under the next stage, as to whether it is ready for production.

Do you feel you have sufficiently completed the prior stages? If high risk remains, you may have to compromise on your objectives in order to apply more aggressive mitigations. You should be keeping in mind whether or how your product stacks up against GDPR principles and compliance requirements.

If you are not ready, update the context of processing and do the cycle again. A DPIA should be a cyclical, iterative process, embedded within your product development, of methodically analysing risk and reducing privacy impact. You should review and update the information and decisions you made at each stage in the previous iteration(s), to reflect any changes (such as to objectives, product design, etc.).

If you are ready, proceed to Stage 9.

Stage 9: Identify residual risks and evaluate against GDPR principles and requirements

Identify residual risks and evaluate under GDPR principles, such as fairness and proportionality.	Once at an appropriate stage in the design process, you can look at what you have and evaluate whether the processing is proportionate to the need and the risk, whether you have met the legal bar for achieving the legal bases under which you will conduct the processing, and whether the processing otherwise adheres to the principles and requirements of the GDPR. This must be an objective analysis, and if the processing proposed in this 'final' state still produces high risk you must either go back and find alternatives; decide not to proceed; or consult with your Supervisory Authority as required under Art. 36. You'll include your DPO and possibly senior management (and/or whoever you have identified as having ultimate approval) in this analysis.

The first step in this stage is to identify the residual risk after having applied data minimisation and privacy by design in Stage 5 and risk mitigations in Stage 7. This means identifying, objectively, the risks or privacy impacts that remain to the rights and freedoms of data subjects after all of the mitigations you have applied. For example, the ICO's guidance says: 'A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.'

It is necessary to understand the residual risk both because the outcome of your DPIA must be reviewed and signed off by your DPO (and possibly other senior leaders in your organisation, depending on your process/governance arrangements), and because the residual risk is a requisite part of your proportionality and legal basis analyses. You, with participation from the DPO, legal staff, and senior leaders will have to assess whether, given the remaining risk or privacy impact, the processing can be justified: is it proportional, fair, legal, etc., all in compliance with GDPR requirements?

Go through each type of data and each processing operation. Taking into account data minimisation, PBD, and risk mitigations, what risks remain? See Appendix B and Appendix C for examples of data types and common risks. Some examples of residual risks that may remain include:

- Even with contractual limitations, and compliance procedures (such as ongoing monitoring, audits, due diligence, etc.), data recipients may misuse data or be subject to a breach.
- Even with short retention periods and appropriate security controls, data may be subject to a breach or misuse by internal employees.
- Even with notice, data subjects may not fully understand the consequences of some types of processing.

Evaluate all such residual risks and take them into account during your legality and proportionality analyses. Consult Appendix B for pointers.

Legality

Of course, you need to ensure a legal basis and overall legality for your processing. This is a good point at which to assess whether, given your product, you are able to meet the requirements of your chosen legal basis, and how you are meeting other formal requirements of the GDPR.[23]

For each processing operation for which consent will be your legal basis:

- Where do you get consent?
- Does consent meet the legal bar of being a freely given, specific, informed and unambiguous indication of the data subject's agreement?[24]
- If accessing or storing data on a device, e.g. reading/setting cookies, how do you ensure consent prior to accessing the device?
- How do you store the consent?
- How is the data subject able to withdraw consent?
- Is it as easy to withdraw as it was to give?
- Will you renew consent on a periodic basis?

For each processing operation for which legitimate interest will be your legal basis:

- Have you completed a legitimate interest assessment (LIA) using an accepted framework or template, and does that assessment conclude, reasonably, that the interest pursued is not overridden by the data subject's rights and freedoms? You must conduct an LIA before you commence processing on that basis. The IAB is producing a separate guide on undertaking LIAs for digital advertising activities, which we recommend you refer to and use if you are considering legitimate interests as a legal basis for your processing.
- How is the data subject able to object to the processing?

[23] As does the TCF, this template assumes that of the six possible legal bases in the GDPR, only consent and legitimate interest are viable legal bases in practice for processing operations in digital advertising.

[24] Note: participation in the TCF is not a substitute for individual participants taking responsibility for their obligations under the law. In addition, some aspects of consent are intentionally not covered by TCF, as differing national-level interpretations apply.

How will you honour data subjects' right to deletion? How will you honour data subjects' right to access? Do you have Data Processing Agreements with all processors involved, as required by Art. 28?

Necessity, Proportionality, Fairness

Beyond the more formal requirements for legality of processing under the GDPR, such as establishing a legal basis, or transparency, the GDPR incorporates a set of principles that must be taken into account to ensure overall legality of the processing. All of the work of assessing against these principles should have been done implicitly in the prior stages. Now look back and complete a final evaluation of your work.

- Is the processing necessary to achieve the objectives or is there a less intrusive means?
- Are there alternative means to achieve comparable objectives?
- Have you thoroughly applied data minimisation and PBD techniques?
- Have you thoroughly implemented risk mitigation techniques to manage residual risk?
- Where you have made trade-offs in favour of using more data or more intrusive processing, how do you justify those trade-offs as necessary?
- How is the residual risk proportional to the benefits of processing?
- How well do the disclosures to data subjects, whether TCF or not, inform the user of the nature of the processing? Can a user reasonably understand the consequences of the processing?
- Have you consulted with data subjects or other stakeholders?
- Are you able to fulfil data subjects' rights with respect to this data and processing?
- How do you justify the retention periods of all data?
- How will you ensure the security the data and processing?
- What are your measures to ensure ongoing adherence to this DPIA, and to prevent function creep, i.e. gradual expansion of the processing?

There is an art to this analysis, and much guidance available outside of this document. Look to the resources section for pointers. You should consult your DPO and other privacy professionals here.

As explained earlier in this guidance (e.g. the Overview section, pages 8-10), if any there are any high residual risks remain that you cannot mitigate, you must consult your SA before processing can commence.

Stage 10: Maintaining your DPIA

Maintain the DPIA, including compliance with mitigations	The DPIA creates an ongoing obligation. You must ensure that your analysis remains true. You do this by keeping the context of processing up to date, and re-evaluating when changes occur. You also ensure that privacy by design features, data minimisation and risk mitigations are complied with.

Your DPIA for any particular product or activity is not a one-off exercise and you should ensure that you review and update it as necessary, reflecting any changes to the objectives, context, risks, etc. You should also to ensure that your controls and mitigations are complied with, and remain effective, on an ongoing basis.

3.4 Consulting with stakeholders

The GDPR sets out what a DPIA involves, and Art. 35(9) says:

> Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

You should consider this requirement and whether it is appropriate for the processing/product in question. Some SAs such as the ICO have DPIA guidance with a section on consultation: 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/#how7.

It is not common practice for advertising technology companies to consult directly with data subjects, and there are legitimate reasons why bringing data subjects into the product development process is infeasible. It may be appropriate to consult their representatives instead.

There exists a wealth of public information in the form of surveys, articles, regulator publications, and more that evince perspectives on the nature and consequences of data processing in the industry. Companies must remain aware of these perspectives and incorporate them explicitly into their DPIA, particularly if you have decided not to consult directly.

Moreover, companies can consider how to gather more data subject views to incorporate into their DPIA thinking, especially with respect to the use of particular processing or types of data that may not be well reflected in publicly available perspectives. There are many privacy NGOs that claim to represent data subject interests and might be good resources to consult.

Companies should document their use of data subject perspectives, possibly, for example, in the form of a bibliography attached to the DPIA process.

Whatever you decide to do, you should explain your reasoning in your DPIA. Where you are not directly soliciting input from data subjects (or their representatives), you should record this decision and document your justification for not doing so.[25] [26]

3.5 Deciding not to do DPIA

As stated above, we take the position – without pre-determining that all processing in the industry is high-risk – that engaging in a DPIA process should be the default, even where not explicitly required (see 'When is DPIA required?' above). If DPIA and PBD are built into your product development processes, and your review of existing products, then DPIA should be done in the

[25] '[T]he controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable.' EDPB Guidance, p. 15.

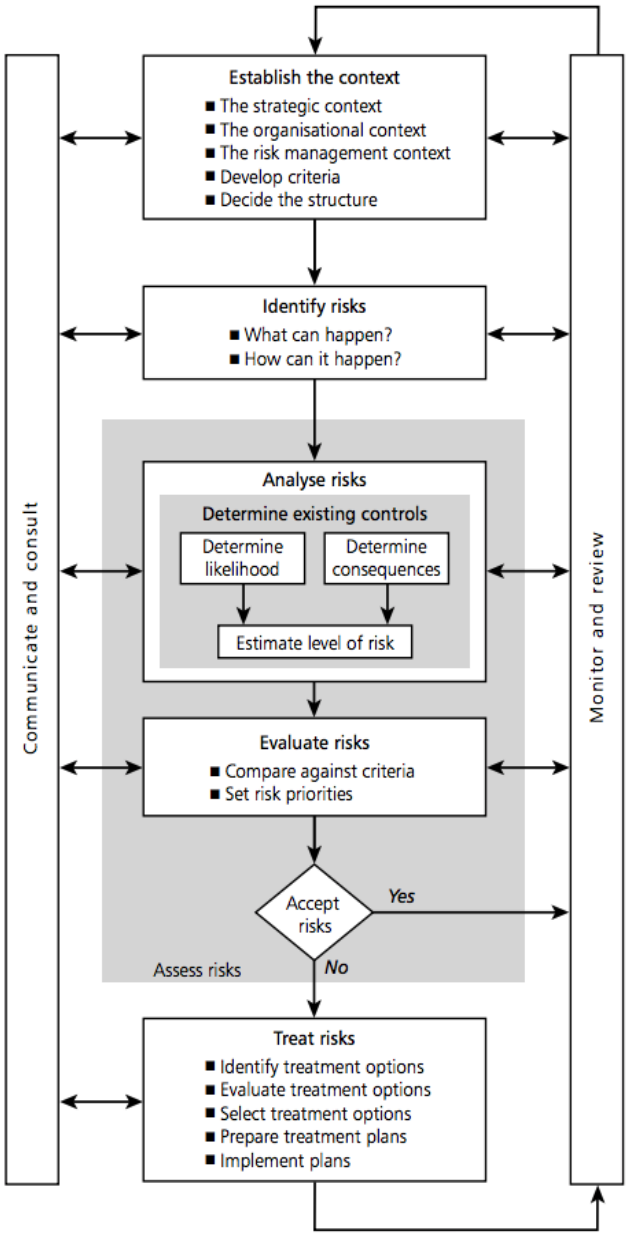
[26] 'In most cases it should be possible to consult individuals in some form. However, if you decide this is not appropriate, you should record this decision as part of your DPIA, with a clear explanation. For example, according to the ICO, you may be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.' 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/#how7

normal course. If the processing is not likely to pose a high risk to data subjects, then the DPIA will be relatively lightweight.

Nevertheless, there may be cases where a DPIA is not required by the law, and where you determine that it is not otherwise necessary. You may wish to consider recording your decision not to undertake a DPIA, and your reasons for it.

Appendix A: Risk assessment

Below is a suggested approach to organisational risk management but the same methodology can be applied in the context of a DPIA, which is focused on risks to **data subjects' rights and freedoms**. *Figure 1: Risk Management Process, reprinted from Standards Australia: Risk Management Guidelines*



a) **Establish the context**. Establish the strategic, organisational and sectoral context. What data do you process? What categories of data does this include? Is any of the data sensitive, private or special category? [Stage 3 of your DPIA]

b) **Identify risks.** Think about information risks facing your organisation. What could happen to the data that you process? Why? [Stage 5 of your DPIA]

c) **Analyse risks.** Analyse risks in terms of consequence and likelihood to calculate the risk level. **This step is set out in detail below**. [Stage 5 of your DPIA]

d) **Evaluate and treat risks.** Prioritise risks and decide whether to accept or reject the level of risk facing the organisation. For higher risks, develop a risk mitigation plan and implement projects to enable mitigation. [Stages 6, 7 & 8 of your DPIA]

e) **Report.** For any risks which remain residually high after mitigation, you must consult the appropriate supervisory authority before starting processing. [Stage 9 of your DPIA]

Analysing risks: calculating the risk level

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

Risk = likelihood x severity

i. How to determine the likelihood

You should make an informed decision about the likelihood of a particular risk, based upon:

- Your understanding of the possible causes of an event. You should ask yourself:
  - why might this event occur?
  - What are the underlying issues that might cause this to happen?
  - What might be the catalysts/triggers for the event?
  - How will the risk unfold?
  - Who is responsible for this risk?

- You should assess any previous occurrences. You may need to audit previous incidents within your organisation or seek input from wider stakeholders.
  - Has this event occurred in the past?

- How often? For example, you might investigate how many times a data breach was reported due to this type of issue in the last month/year/decade within your organisation and within the wider community.

You can use a likelihood assessment scale to quantify your assessment.

Likelihood assessment scale

	Likelihood				
	Remote	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Descriptor	Will probably happen in exceptional circumstances	Unlikely to occur, even though a definite potential exists.	May occur and has happened before on occasion. There is a reasonable chance of occurring	Very likely that this will occur	This is expected to occur frequently / in most circumstances. It is significantly more likely to occur than not.

ii. How to determine the consequences

In determining the likely consequences of an event, and their severity, use the **reasonably foreseeable worst-case scenario.**

The consequences will vary based on the circumstances, including the nature of the risk and the type of data being processed.

As well as considering the impact on data subjects, you should give consideration as to the number of data subjects affected. Processing that potentially impacts on many thousands of data subjects, even if the impact is moderate, may well be high risk. You should consider the scale of the risk and modulate your risk assessment based upon this.

For example:

	Severity of consequences				
Context type/descriptor	**Negligible**	**Minor**	**Moderate**	**Major**	**Extreme**
Subject Privacy E.g. arising from disclosure of confidential or sensitive information.	Negligible harm to the individual.	Minor harm with no material detrimental effect on the person.	Moderate harm, for example damage to personal relationships and social standing.	Major harm, for example ID theft with potential adverse effects.	Extreme harm, for example ID theft with financial loss, losing a job, risk to life or health.

Appendix B: Example Data, risks and mitigations

The table below describes data typically used in digital marketing, the risks that may arise from processing that data, and potential controls and mitigations for those risks. These are intended as inspiration and an attempt to create some alignment among industry around these issues. This list is by no means exhaustive or complete. You'll need to look to outside resources and your internal privacy professionals to bring the full nuance.

Note: in relation to sensitive or potentially special category data, as defined by Article 9 of the GDPR, we have assumed that such data is not intentionally processed for digital advertising purposes. However, it is possible that processing of non-special category data can lead to a risk of special category data being processed, depending on what it is, how it used, and for what purpose. This risk may be a relevant consideration in relation to certain data types, for example, browsing history, interest segments, location, and precise geolocation. You should be aware of, and mitigate against, unintentional processing of special category data. IAB UK has produced specific guidance on special category data: https://www.iabuk.com/news-article/digital-advertising-guidance-special-category-data-under-gdpr

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
Identifiers	These are the various types of identifiers typically used in the industry. They all may be considered personal data.	Any identifier can facilitate the re-identification of pseudonymous data. There is a risk that not originally intended to be directly identified becomes so through ID matching.	Using pseudonymous data is a PBD technique. It can reduce risk from re-identification and combination of data sets. Salted hashes can improve protection against those risks. However, keep in mind

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
			that pseudonymous data is still personal and carries re-identification risk. Mere hashing of identifiers is not be a reliable means of de-identifying data. Also note, beware of known vulnerable hashing algorithms, such as MD5 or SHA1. You should keep the lifespan of identifiers and identified data as short as possible. Delete identifiers from data as soon as practicable.
- Pseudonymous identifiers[27]	Inherently pseudonymous identifiers, such as IP address, and cookie and device IDs.		See above. Note that a truncated IP address is not necessary considered as non-personal; it depends on the context.
- Pseudonymized identifiers, such	Pseudonymous identifiers derived from direct identifiers,	Beware of re-identification risks in your hands or in the	See above. As noted above, hashing has limits. So, while

[27] Note that 'pseudonymous' is not 'anonymous' and may be considered personal data. See, e.g., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
as hashed email address	including for example hashed email address.	hands of recipients of the data. Can data collected pseudonymously against these identifiers be re-correlated to the underlying direct identifier?	hashing the email address (or other direct identifier) improves privacy, beware that this data is vulnerable to a rainbow table attack. Also, there are techniques for keeping the match one-way to prevent data that has been collected pseudonymously from being re-correlated to the direct identifier.
- Probabilistic device identification	Synthetic, non-deterministic identifiers derived from probabilistic and/or machine learning models using inputs such as IP address, user agent, and other network, device, or browser characteristics.	Probabilistic identifiers are non-transparent and harder for the data subject to control than deterministic identifiers.	Transparency and control is hard to achieve. On the other hand, the inaccuracy or 'fuzziness' of the identification can be considered as helpful to privacy. How much accuracy and precision do you need for your objectives?
- Direct identifiers	Non-pseudonymous identifiers such as email address, username, account	Historically, most of the data collected in the industry has been pseudonymous.	Use pseudonymous identifiers instead, if possible. Consider the heightened security

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
	number. These are becoming more common in the industry.	People have often said, 'we don't know or care who you are, all we have is a cookie ID.' However, with more direct identifiers in the mix now, there is a heightened risk of, for example, re-identifying browsing history that was originally collected with a cookie.	risk of processing this data. Also consider that processing this data may lead to more expansive obligations for fulfilling user rights, as they connect more data and are more persistent.
Browsing or app usage history	A recording, whether intended or not, of data subjects' online activity. Note that something like web server logs recording sync pixel calls would qualify. The point is that a particular user's or device's online activity can be reconstructed from the data.	This data can reveal a lot about a data subject, including some very personal things. Additionally, it is commonly understood that the feeling of being surveilled will inhibit free expression.	Delete or properly de-identify the history as soon as possible. Consider removing URL parameters, directory paths and other information as an interim measure to reduce information.
Interest segments	Interest categories, however derived.	Segments can reveal personal information, and sometimes may be	Cap the lifetime on segments. Regulate what segments are

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
		used in ways that affect the data subject in undesired ways (see Appendix C).	allowed. Consider giving transparency into the specific segments you are using.
Demographic information	Information about a data subject's demographic characteristics.	Same as segments. Beware of the risk of discriminatory use of this information.	
Precise geolocation	There is not a legally defined threshold for precise versus imprecise; however, current TCF policy considers data not precise if it is precise to a radius of greater than 500 meters or greater and/or for GPS coordinates has two or fewer decimal places.	This data can represent the physical behaviour of a data subject, and can include some very sensitive information, such as visits to medical facilities or places of worship. You should consider population density. Precise geo in a city has different privacy implications than in a rural area.	You can reduce the precision of GPS coordinates by dropping decimal places, or converting to postal code, city name, or some other larger geographic region. You should consider levelling up geo to areas with some minimum population density. There are various ways to do this. Be careful about sensitive locations, such as schools, churches, medical facilities, government facilities, and so forth.

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
			Be especially careful about sharing this data.
Imprecise geolocation	See above re precise geolocation.	Even in imprecise form, geolocation data can reveal sensitive information. For example, showing that someone was in a city or neighbourhood where they weren't expected to be, or subjecting someone to suspicion because they were in the vicinity of a crime.	As noted, imprecise geolocation comes with privacy risks. The note about precise geo and population density applies here, too.
Geo segments	Segments based on data subjects' physical behaviour, for example, 'went to a grocery store,' or 'went to a Sainsbury's,' or 'went to the Waterloo Sainsbury's'.	In the more abstract form of segments, this geo information has the potential to reveal data that an individual would consider very personal, or sensitive. These do not have the same privacy characteristics as interest segments derived from *online* behaviour.	Exercise control over the allowed segments.

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
Date and time of the above	Date and time information associated with behavioural information described above.	This shows what someone was doing at a particular time, sometimes in a particular place. For example, they were surfing the internet at a cafe when they claimed to be home asleep.	Delete time stamps as possible. Otherwise, reduce the precision. Do you need seconds when hours are sufficient? What about dayparts or days? Weeks?
Device information	Information such as the make, model, version of a device or browser, also settings and device capabilities, etc. These are all characteristics that can facilitate distinguishing between devices or users and are often used as targeting criteria on their own.	The more granular this information is, the greater the risk that it can be used to distinguish users and devices.[28]	Reduce the precision as much as possible. For example, do you need the browser build number or is browser type enough?
Cross-device graph	Correlation of devices owned or used by a single user.	Cross-device graphing tends to be non-transparent. There is potential for	With all graph data, be careful about sharing the graph, especially in conjunction with device

[28] For example, the EFF's Panopticlick demonstrates how this kind of information can be used to measure the 'uniqueness' of a device.

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
		embarrassment or worse as behaviour on one device influences ads on another. Think about shopping for a wedding ring, or a divorce, for example. There is also the risk of correlating more data – data associated with different devices, possibly data that the user hoped to keep separate. Think about work vs personal devices.	IDs. It is possible to share data you believe came from the same user or household without revealing the particular devices. Consider controls on the ways this data can be used, taking into account the potential for cross-graph data leakage. For example, certain categories of ads may be inappropriate.
Household graph	Correlation of devices owned or used by users in the same household.	There is a risk that correlating household devices will cause data about one user in the household to be revealed to other users.	See above.
Social graph	Correlation of users thought to interact with each other socially.	This could be sensitive information, especially if the user did not explicitly reveal the information. People's social connects can	See above.

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
		reveal a lot about them. Also, this correlation could frustrate a user's efforts to silo social associations. And, as with household graphs, there is a risk of revealing information about one user in the graph to other users in the graph.	
Sensitive or special category data	Data about children or data that may fall into one or more of the Art. 9 Special Categories.	Even if you don't intend to collect this data, and don't identify it, there is often a risk that you may do so, or that it could arise from how other data (e.g. location, browsing history) is stored and used.	You should take measures to avoid collecting this data inadvertently. For example, that may mean controlling your sources of data, or it may mean recognizing the data as it comes into your system and not recording it in personal form.
Online-offline match	Matching of identifiers for the purpose of correlating offline and online behaviour, or more generally	This matching creates the risk of re-identification, and of correlating data across different contexts in	

Data Type	Description	Notes about risks	Minimisation, PBD, and risk mitigation considerations
	between different contexts. For example, matching records of online ads viewed to the user's purchase history with a retailer/advertiser.	ways the data subject does not expect.	

Note that some of the categories above are typically used as components in other processing but might require DPIAs in their own right. For example, building a cross-device or household graph should have a DPIA.

Appendix C: 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 considerations relative to each. It is provided as a useful reference. You should take care to think about risks present in your circumstances that may not be represented here. For your own DPIA you will need to analyse the impact and likelihood of the specific risks you identify (see main guidance). 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.

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? 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.
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.

Risk	Considerations
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. The nature of the data and the processing in the industry sometimes creates challenges to how those rights can be honoured. 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.
Fairness[29] and discrimination	
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 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.

[29] Personal data must be processed fairly. Some of the potential risks described here may also indicate that the intended processing is not fair. For example, 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

Risk	Considerations
	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 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.
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 neighbourhoods.
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.
Data security and data sharing	
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	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

Risk	Considerations
breach of contract or otherwise)	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 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. However, in many cases in the industry it is trivial 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

Risk	Considerations
	expectation at the time that the data would ever become directly identified. Once data is re-identified, the risks are increased.

Annex: Resources

Legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/oj

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://data.europa.eu/eli/dir/2002/58/oj

EDPB guidance/resources

European Data Protection Board, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk for the purposes of Regulation 2016/679' (as last revised and adopted on 4 October 2017) https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

European Data Protection Board, 'Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.' https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en

EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (Version 2.0, Oct 2020).

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

Data Protection Authority guidance/resources

Irish DPC 'Data Protection Impact Assessments' https://dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

CNIL, 'Privacy Impact Assessment Guidelines' https://www.cnil.fr/fr/PIA-privacy-impact-assessment-en

ICO, Data Protection Impact Assessments https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

ICO, Data Protection Impact Assessments (DPIAs), Detailed Guidance https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

ICO, 'Guide to the General Data Protection Regulation (GDPR)' (May 2019). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

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

IAB Europe guidance/resources

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

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

Other guidance/resources

Smart Grid Task Force, 'Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems' (Sept 2018).

https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

Center for Information Policy Leadership (CIPL), 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' (Dec 2016). https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf