Digital advertising guidance: Data Security, Retention and Storage

November 2022

Table of Contents

- Appendix 1: Risk Assessment Methodology
- Appendix 2: Retention guidance
    - Annex A: Retention Schedule Template
    - Annex B: Retention Period Assessment Template

Part 1: Data Security, Retention and Storage

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 and ePrivacy legislation (while recognising that individual companies remain accountable for deciding what approaches they should take in practice).

The purpose of this guidance is to help educate the digital advertising industry about the legal requirements relating to personal data security, retention and storage, to help companies understand their obligations, and how to comply with them in practice.

This guidance is intended as a high-level overview for companies engaged in digital advertising in the UK, based on relevant UK law - namely the UK GDPR, Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

This guidance is intended to bring clarity and consistency to the application of this law to the digital advertising industry, and to help establish benchmarks so that companies can understand what may be expected of them. You are not required to follow this guidance, and the guidance may not be applicable, or suitable, for all cases and circumstances, given the wide variety and nature of companies operating in this sector and of their activities. If you choose not to follow this guidance, you should have a clear rationale for the approach you take to these matters.

Nothing in this guidance, or any accompanying documentation or resources, constitutes legal advice. Following the guidance is no guarantee of compliance. Companies remain responsible for their own compliance with applicable laws and industry self-regulatory rules, so should take their own legal advice where necessary.

Part 1 of this guidance provides an overview of organisational and technical security measures that can help enable the digital advertising industry to comply with its personal data security obligations.

Part 2 of this guidance provides the digital advertising industry with specific

examples of appropriate security measures in different industry contexts, and includes guidance on how to determine data retention periods.

We recommend that you review your personal data security, retention and storage practices and ensure that you are operating in line with the relevant legal requirements.

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 The ICO Update report into ad tech and RTB

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

One of the six key points in the ICO's Update report was that the complexity of the RTB data supply chain, the inconsistent use of technical and organisational security measures and the inadequate governance of data sharing represents risks to the integrity of personal data and create risks that data processing may be non-compliant with the UK GDPR, the DPA 2018 and/or PECR. We recommend that you read the Update report and familiarise yourself with the ICO's positions on the data supply chain.

This guidance forms part of the actions set out in IAB UK's response to the Update report.

2. Data Security

2.1 Background

The UK GDPR updates the obligations set out in the 1998 Data Protection Act to put in place appropriate data security measures to protect the personal data that you process. The 1998 Act already obliged similar security measures, which have now been updated in the UK GDPR and DPA 2018.

Article 5(1)(f) of the UK GDPR stipulates that personal data must be processed in a manner that ensures 'appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

2.2 What is personal data?

Article 4 of the UK GDPR defines personal data as information which relates to living, natural persons who are **directly or indirectly identifiable** and can be identified using that information itself, or by combination with other data.

Data is identifiable if you can identify one individual from another using this data. Identifiers can include

- name;
- identification number;
- location data;
- online identifiers.

Online identifiers can include IP Address and Cookie IDs.

If you process cookie identifiers, IP addresses, location data or direct identifiers such as name/ID number, it is very likely that you are processing personal data. There are some specific examples of the types of personal data likely to be processed for RTB purposes in Part 2 of this guidance, Data security in practice, and in the template retention schedule in Annex A of Appendix 2.

The ICO provides detailed guidance on defining personal data.

2.3 Risk-Based Approach

The UK GDPR does not define appropriate security measures. In deciding which security measures are appropriate, the UK GDPR mandates that organisations take a risk-based approach. Article 32(1) states that organisations must 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' and sets out some examples. This means that in addition to reading and understanding this guidance, you should conduct appropriate risk

assessments for all personal data processes, flows and stores.

Which security measures are appropriate is determined by the context of the data processing, the nature, volume and scale of the personal data and the state of the art/implementation costs. It is your responsibility to decide on the best way to implement data security measures, based on the level of risk to the data subject and to your organisation. The ICO provides useful guidance here.

Appendix 1 of this guidance covers Risk Assessment Methodology, and Part 2, Data Security In Practice provides examples of the application of appropriate security measures in practice in some typical RTB data processing contexts.

2.4 Data mapping and Record of Processing Activities (ROPA)

In order to make informed decisions about appropriate organisational security measures, you need to first understand the exact nature of the personal data that is processed by your organisation, and the nature of the processing itself.

Article 30 of UK GDPR obliges you to produce a written Record of Processing Activities (ROPA), and specifies what it must contain (depending on whether you are a controller or processor). The ICO has produced guidance on documentation under UK GDPR.

Your ROPA records, in some detail, the sources and destinations of personal data you process, as well as the purposes for which you process it. Your ROPA documents will help you to understand the flow, or lifecycle, of data through your business and will form a key component of your risk assessments.

Article 30 leaves some flexibility to determine the precise structure and content of your ROPA, depending on the nature of your business and systems, but it is highly recommended that you begin with a data mapping exercise to produce a detailed, accurate and complete picture of your relevant data processing activities. While you should have conducted this exercise in preparation for UK GDPR implementation, your ROPA should be kept up-to-date, and therefore you should review and update it regularly.

Some of the required contents of your ROPA specified in Article 30[1] are caveated with 'where possible.' Including this information as part of your ROPA should be possible in almost all cases that this guidance applies to. With respect to Article 20 (1)(f), which relates to time limits for erasure, companies engaged in digital advertising activities should have discrete retention periods and well understood deletion or anonymisation procedures for all personal data (see Section 4). And, as

[1] Art. 30(1)(f),(g) and Art. 30(2)(d) https://www.legislation.gov.uk/eur/2016/679/article/30

elaborated further below, all companies should have detailed security policies and programs that can be referenced from their ROPA.

You should also consider compiling an Information Asset Inventory, if feasible. An asset inventory lists the databases, servers, devices or other assets that contain personal data. It is up to you what level of abstraction makes the most sense for this inventory. This is not a regulatory obligation, but can help you to understand your personal data systems architecture and may serve as a very useful guide to structure your ROPA.

When you have completed the ROPA and Information Asset Inventory, you can use them in your risk assessments, which will inform the decisions that you make regarding the appropriateness of your security measures.

2.5 Risk assessment

There are many ways to conduct risk assessments from a data security perspective, and example approaches are provided in Appendix 1 and Part 2, Data Security In Practice.

Risk is determined by examining the **severity** and **likelihood** of any impact on either the organisation or individual data subjects, although risk to the data subject should be the primary consideration.

You must assess the impact of any personal data processing on the data subject and decide how likely you think this to occur.

Once you have conducted risk assessments on all personal data processing within your organisation, you are in the position to make informed decisions regarding the appropriateness of any security measures, or whether the processing should go ahead at all. You should prioritise high risk activities.

2.6 High risk processing and Data Protection Impact Assessments

As well as the specific data security requirements in Articles 5 and 32, Article 35 establishes the legal requirement to conduct a Data Protection Impact Assessment (DPIA) for any processing operations likely to result in a high risk to the rights and freedoms of natural persons. It defines such high risks as:

- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred

to in Article 10;
- systematic monitoring of a publicly accessible area on a large scale.

Other factors which are likely to heighten risk are:

- processing data relating to children
- routinely processing very large volumes of data
- processing data relating to financial activity of data subjects
- transferring data outside of the UK

Guidance from the European Data Protection Board provides a list of criteria that organisations can use to determine whether their processing is likely to result in a high risk to the rights and freedoms of individuals, and therefore whether a DPIA is required.[2] Additionally, under Article 35(4) of the UK GDPR, the ICO has published a list (which reflects the EDPB guidelines) of processing operations likely to result in such a high risk, **for which DPIAs are mandatory**. The list is at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/. These include operations that could apply to digital advertising activities, including 'invisible processing' and 'tracking'. The ICO provides detailed guidance on when to complete a DPIA.

For any activities that you assess as likely to result in a high risk, including (but not limited to) those in the ICO's list, you must complete a DPIA. This should include (among other things) an assessment of the security risks, including sources of risk and their potential impact. As RTB processes often involve high risk processing as described above, DPIAs will likely be essential in many cases. For more information see our separate guidance on DPIAs under the GDPR.

2.7 Governance

Information security is not just a technical challenge: there are cultural and organisational aspects which are equally important.

It is important that data security has senior sponsorship and that someone in a leadership position has ultimate responsibility for organisational data security. You should ensure that data security responsibilities are clearly assigned to an appropriate person/team, and that they have sufficient resources and authority.

[2] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment*, published 13 October 2017 and endorsed by the European Data Protection Board on 25 May 2018. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

You should have a formal Information Security Policy that sets out your organisational approach, defines roles and responsibilities and details necessary technical security measures. This will enable you to demonstrate how you are taking steps to comply with the security principle and related requirements. Policies need to be reviewed and updated regularly.

3. Data Security Recommendations

It is likely that most organisations within the RTB ecosystem are processing at least some data with a higher degree of risk, especially regarding the volume of data that flows throughout the supply chain. The following are therefore recommendations for data security best practice, and measures you can take or implement to comply with DPIA requirements (as appropriate). It is the responsibility of your organisation to make risk-based decisions regarding the appropriateness and necessity (including in the context of DPIA requirements) of the application of the measures set out in this section. You can consider the state of the art and cost implications as factors in your decision. See part 2 of this guidance for some illustrative worked examples.

3.1 Data minimisation

Data minimisation is one of the central principles of the UK GDPR. You should understand exactly what personal data you need for your stated purpose, and process only that data, and no more. Data minimisation is also a security measure, because if personal data is minimised then data breaches will potentially have less impact on data subjects.

Data minimisation means always striving to achieve your objectives using the least personal data. It is an ongoing process and is relevant at all stages of processing. For example, you could consider:

- if you use geographic information to target an ad, do you need to process it in precise form, or would less precise information/targeting be sufficient?
- do you need to store full referrer URLs in your logs or would the domain suffice?
- what is the minimum period for which the data in question is needed for the stated purpose? Delete the data at the end of this period; do not retain it just in case it might become useful in future (see section 4).
- how quickly can you delete or aggregate data, to reduce the amount of data you have in your systems?

When you share personal data, only share what is necessary for the recipient's intended and allowed purposes (see section 5). The ROPA and data mapping work

discussed in section 2 will provide your organisation with the opportunity to assess exactly what data is needed for your processing activities.

3.2 Encryption

Although the UK GDPR does not in general define appropriate security measures, Article 32 does specify encryption as an example of an appropriate measure.

The impact caused by unlawful processing, loss, damage or destruction of personal data can be mitigated if that data is encrypted and ICO guidance suggests that regulatory action may depend partly on the encrypted state of data in a data breach incident.

Encryption is often a low cost and easy to implement safeguard. You should encrypt personal data in storage and in transit, where you determine that it is necessary or appropriate, in accordance with your understanding of the type of data that you process and the associated risks.

Where you do not encrypt personal data, you should ensure other, appropriate security measures are in place commensurate with the risk, and you should be able to justify why you have not encrypted data.

There are many ways to encrypt data and it is up to you to decide how best to implement encryption. However, we recommend that you adhere to accepted industry practices and guidance. For more on encryption see the ICO's guidance and https://www.nist.gov/itl/current-fips.

3.3 Pseudonymisation and anonymisation

Typically, in this industry, pseudonymisation of personal data removes directly identifying information (such as name, ID number) from data records, and replaces it with a non-identifying reference number. Much data in the industry, cookie IDs or MAIDs (Mobile Advertising IDs) for example, is inherently pseudonymous.

Data which has undergone pseudonymisation is defined as data that can no longer be attributed to a data subject without the use of additional information. This would require that the additional information is kept separately, and appropriate technical and organisational controls are in place to ensure that re-identification of an individual is not possible.

Recital 26 of the UK GDPR makes clear that pseudonymised data is still considered personal data, and is still within the scope of, and governed by, the UK GDPR, although pseudonymisation is still a useful way to limit the risk and impact of a data breach.

You should consider pseudonymising all personal data, if it is not already pseudonymous, especially if identifiers such as name are not of use to you. In this respect, pseudonymisation is a form of data minimisation.

Anonymisation requires that personal data is stripped of its identifiers, and that it is technically and logically impossible to resynchronise this data with its original identifiers, using direct or indirect means. The term 'anonymous' is often misused to refer to pseudonymous data. True anonymisation is technically difficult to achieve and renders the data subject and their device completely unidentifiable in a non-reversible manner, i.e., it is not possible to single out, or infer the identity of, the data subject, or to link data from another source to re-identify an individual or device (including via a cookie ID or MAID).[3]

If you have no need to ever identify a data subject, you should anonymise the personal data, and be careful to ensure that the data cannot be made identifiable by direct or indirect methods. In assessing whether the data is truly anonymous, you should consider all available means reasonably likely to re-identify an individual, taking into account the time taken, costs and available technology at the time of processing. The anonymous nature of the personal data should be re-assessed if technological advances in re-identification techniques are introduced.

User ID

Historically, most data processing in the RTB context would be unlikely to be possible using truly anonymous data. RTB has been built on an infrastructure that generally has required at least device-level identification and synchronization across business partners, generally including cookies or MAIDs, other proprietary customer or device IDs, obfuscated email addresses, or combinations thereof, none of which are anonymous. These identifiers have been necessary to engage in routine frequency-capping and campaign reporting, while also powering combined data sets across parties, and at times, links to full identity information.

While RTB has been powered by this data structure to date, there are many innovations underway, in part due to the GDPR and changes at the browser and operating system levels (see https://www.iabuk.com/user-identity for more information). In addition, advertisers and adtech companies have been exploring campaign models that require less data and various other privacy by design approaches. In the future, RTB systems may be able to transact, at least in part, using truly anonymous data. However, you must still ensure your processing of personal data under existing mechanisms is legally compliant, and bear in mind that any new mechanisms or processes that involve processing personal data will

[3] Note: at the time of writing, the ICO is revising its anonymisation guidance. See https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/

also be subject to the same security (and other) requirements set out in the UK GDPR (and to PECR requirements, if they involve storing or accessing information on a device).

Responding to these market developments, In November 2021 the ICO, under its advisory powers, published an Opinion on Data protection and privacy expectations for online advertising proposals. It outlines the Commissioner's overarching expectations that any development seeking to address the risks posed by adtech should meet. These include expecting market participants to address the issues highlighted in the 2019 report.

3.4 Physical security

Many data breaches occur due to failures of physical security, for example the theft of devices containing personal information. You must ensure that physical premises are secure, especially if premises contain servers or other large stores of personal data.

You should consider measures such as:

- secure entrances and exits, ensuring the quality of doors and locks
- secure premises with alarms and CCTV
- enforce access controls such as ID badge verification
- ensure strict premises visitor processes in place
- ensure that paper containing personal information is disposed of securely
- consider how to physically secure IT equipment and mobile devices

Security frameworks, such as ISO 27001 or SOC II include principles and guidance related to physical security, in addition to measures for digital security.

3.5 Cyber security

The ICO and NCSC have produced security outcome guidelines that outline a recommended approach to risk-based information security decision making.

Securing your organisational IT systems is potentially complex and difficult process, but you must put in place reasonable measures to safeguard your information systems. What this means in practice depends largely on the scale and complexity of your systems architecture, and you should make information security decisions based on the context of your organisation.

This guidance provides an overview only. It is recommended that you appoint a technical information security lead if appropriate, and to put in place an Information Security Management System (ISMS) to govern the process.

The National Institute of Standards and Technology produce a very useful framework, consisting of standards, guidelines, and practices for organisations to better manage and reduce cybersecurity risk. This framework can be used to help plan, deliver and risk assess your cyber security arrangements.

You should aim to achieve accreditation to ISO27001 standard or SOC 2. ISO27001 and SOC 2 represent the gold standard for information security accreditation, but can be a resource-intensive process, and may not be appropriate for all companies, especially at an early stage of maturity. Even if your company is not yet ready to complete accreditation, you should start now to use these standardised approaches to guide your security programme and aim to achieve accreditation as soon as it is appropriate for the size and nature of your business. You might also consider signing up to other certification schemes, such as Cyber Essentials.

It is important to note that none of the above frameworks are UK GDPR certification schemes and do not represent a way to guarantee an appropriate personal data security environment or regulatory compliance. Accreditations can provide helpful baselines, but you should ensure that gaps are continually analysed and addressed.

Network security
Every device that processes personal data should be protected by a correctly configured firewall (or equivalent network device), as set out in ISO27001 or SOC 2 standards.

Configuration
Computers and network devices should be properly configured, with default passwords, access controls and installation security settings updated before use in the data processing environment.

Devices
You should manage all devices within the organisation, taking measures such as:

- removing unnecessary or unused user accounts regularly
- changing any default passwords
- removing unused software
- disabling auto-run without authorisation

Authentication and user access control
You should put in place appropriate access controls on all devices. Based on the context, you should consider two factor authentication for systems containing bulk or sensitive personal data. Basic password hygiene rules should be maintained

which satisfy current authentication standards, such as those published by NIST. Some examples of current password hygiene best practice:

- account locks after unsuccessful logins
- set a minimum password length
- avoid obvious or common or repeat passwords

You should ensure that all user accounts are assigned only to authenticated users, and access rights should only be given to users as required, especially relating to administrative users. User access should be controlled according to least privilege, meaning that users are restricted to accessing systems and data that are minimally required to complete their normal functions, and no more. Admin accounts should only be used to conduct admin tasks.

Malware protection
Computer viruses, worms, spyware and other malware can infect systems via email attachments, download and direct installation, and could lead to a serious data breach.

You must protect your organisation from malware. You can do this by:

- using an anti-malware and antivirus product, according to industry best practice
- only using actively approved software so that non-trusted software cannot execute.
- sandboxing untrusted software.
- stay up to date with industry standards for anti-malware.

Patch management
You must ensure that you have an industry standard patch and vulnerability management program to ensure that all software and systems are up to date, as appropriate.

Penetration testing and vulnerability assessment
A penetration test is a simulated cyber-attack against your computer system, while vulnerability assessment is the process of identifying and prioritizing vulnerabilities in your computer systems that might lead to such an attack.

You should regularly conduct penetration testing and vulnerability assessment processes, at least on an annual basis.

3.6 Business continuity

In the event of an adverse event or incident that renders your information systems unavailable or threatens the integrity of the data, you must be able to demonstrate resilience.

You should draw up detailed business continuity plans that explain how the organisation will react during any incident.

3.7 Staff training

All staff who access, view, manage or process personal data in any capacity must undergo regular data security training.

You should ensure that new staff are trained as part of induction procedures and that all staff receive annual refresher training.

The ICO's Accountability Framework contains guidance on implementing training as part of ensuring that your policies and procedures are being applied and followed in practice https://ico.org.uk/for-organisations/accountability-framework/training-and-awareness/.

4. Data Storage and retention

Storage limitation is one of the central principles of the UK GDPR, as set out in Article 5(1)(e). You must not keep personal data for longer than necessary for the purpose(s) for which it is being processed. Retaining personal data for longer than necessary is unlawful, inefficient, and increases the risk of personal data breaches as defined in the UK GDPR, and the possible impact on data subjects.

The ICO has detailed guidance on storage limitation.

There are no set timeframes for how long personal data can be retained for: it is your responsibility to decide and to justify this decision. However, once you no longer need personal data for a specific purpose, you cannot retain it in its identifiable format, but must either delete or anonymise the data. A good example in the RTB context is failed bid data. Unless there is a legitimate and justifiable reason for retaining personal data relating to failed bids, this data should be deleted or anonymised immediately.

4.1 Retention schedule

You should have a policy which documents and justifies your retention periods where possible. If this is not possible, you must be able to strongly justify why you don't have one.

In practice, you should record the timeframes for retaining personal data in a retention schedule. There are no set timeframes under UK GDPR, although there may be other regulatory requirements that oblige you to keep personal data for a certain period of time, and you must understand whether such obligations apply to your data and factor those into your decision-making.

You should review the processing activities identified in your ROPA documentation and ensure that you carefully consider the necessary retention period for each activity. You must be able to justify your decisions.

Retention schedules should be reviewed regularly and personal data that has reached the end of its retention period should be reviewed to check whether it is still needed.

For further guidance see Appendix 2: Retention guidance.

4.2 Secure deletion

When you no longer need to process personal data, you should either permanently delete it, or irreversibly anonymise it (see section 3.3).

The ICO guide to data deletion provides useful information on how to go about deleting data securely.

5. Data Sharing

Data sharing is a broad topic, and this guide focuses only on personal data sharing in the context of data security. Organisations are responsible for their own data security environment, but when personal data is transferred to a third party, organisations must conduct due diligence checks to ensure that the third party is also processing the data in a secure manner.

If you share personal data with third parties, it is incumbent upon you to do so in compliance with data protection regulations, and to be able to demonstrate this compliance.

You should consult the ICO Data Sharing Code of Practice. This code is a practical guide for organisations about how to share personal data in compliance with data protection legislation.

Data recipients with whom you share, or whom you enable to collect, personal data should be processing data with appropriate safeguards as outlined in sections 2 and 3 of this guidance, and must offer assurances and guarantees to you that they will process personal data in compliance with UK GDPR.

In practice, consider the below arrangements as important to ensuring the security of data as it flows through the digital advertising supply chain.

5.1 Contractual agreements

You should have in place contractual agreements with every recipient with whom you share personal data.

Article 28 of the UK GDPR obliges certain contractual arrangements in the context

of personal data sharing with data processors, in order to meet the requirements of Article 32. In terms of data security, contracts with a data processor should contain all of the requirements set out in Article 28 and should oblige the processor to ensure that the same level of security is applied as would have been applied by you as the controller. In particular, the contract should elaborate on:

- full details of the appropriate security measures
- details of audit and monitoring arrangements
- provisions for end of contract, return or secure deletion of data
- the rights and obligations of both parties
- data breach processes

When sharing data with another controller, either as a third party or in a joint controller situation, Article 28 requirements set out above do not apply. However, this does not mean that no due diligence or contractual arrangements are needed. If you are sharing data in a Joint Controller arrangement, Article 26 obliges you to enter into an arrangement with the other controller to determine both parties' responsibilities regarding the exercising of the rights of the data subject and their respective duties to provide the transparency information referred to in Articles 13 and 14.

The ICO provides useful guidance on contracts and controller-processor liabilities.

Monitoring and due diligence

You must perform due diligence activities prior to sharing data with processors and you should, as required under Article 28, continue to monitor the activities of your processors:

- complete a due diligence form prior to sharing data
- insist on detailed evidence of your processor's security measures. Where your processor has undergone an annual third-party security audit, request to view the results. Audits against established frameworks, such as ISO 27001 or SOC II are strong indicators of appropriate security.
- use your Article 28 rights to audit compliance.

- review the TCF[4] signals sent by CMPs/vendors, to verify they are well formed and don't appear to be anomalous.

You should place contractual limits on recipients' use of the data, and should take measures to ensure those limits are respected. The ICO has stated that they do not view contractual measures alone as sufficient to ensure compliance. Therefore, further diligence is required. The ICO's Update report[5] states:

> 'Organisations cannot rely on standard terms and conditions by themselves, without undertaking appropriate monitoring and ensuring technical and organisational controls back up those terms. For example, ICO guidance on controller/processor[6] and contracts and liabilities[7] states that controllers must:
> - assess the processor is competent to process personal data in line with the UK GDPR;
> - put in place a contract or other legal act meeting the requirements in Article 28(3); and
> - ensure a processor's compliance on an ongoing basis, in order for the controller to comply with the accountability principle and demonstrate due diligence (such as audits and inspections).'

Data minimisation, as discussed in section 3.1, is a good place to start. Share only data that is reasonably necessary for the intended purposes with a valid lawful basis for processing. If your recipient participates in the TCF, you can check the consent string to determine whether the recipient has any lawful basis to process the data. For example, if the recipient does not have opt-in consent for precise location data in the consent string, then this data should not be shared.

Additionally, requiring your recipient to engage in data minimisation efforts is a good idea. As discussed above, data minimisation is one of the central principles of the UK GDPR. Recipients should understand exactly what personal data they need for the stated purpose, and process only that data, and no more. Finally, all personal data transfers should be reflected in your ROPA.[8].

---

[4] The IAB Europe Transparency and Consent Framework
[5] Section 3.5 https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf
[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/key-definitions/controllers-and-processors/
[7] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/contracts-and-liabilities-between-controllers-and-processors-multi/
[8] You should also understand the UK GDPR transparency requirements that apply to data transfers.

6. What this means in practice

6.1 Summary

Security in the context of digital advertising and RTB relates to both the technical security of individual companies, as well as systemic security, including the ability of the ecosystem to make and enforce commitments to the data subject about the limits to data sharing and processing that will take place after a data collection event. The ICO has repeatedly voiced concern about the proliferation of personal data in the RTB ecosystem without sufficient transparency or controls to address the risk of misuse of the data.

As outlined in the earlier parts of this guidance, UK GDPR requires data minimisation, such that unnecessary personal data is not collected from the data subject or otherwise processed. It also requires detailed documentation and consideration of all personal data a company processes. A thorough and risk-based security programme must begin with this step.

Third party validation of security practices and the application of public audit standards can provide objective feedback and ensure benchmarked compliance. As set out in the previous section, the ICO does not view contractual assurances to be a sufficient safeguard in and of themselves to ensure that a company is receiving personal data that was collected and shared in a compliant manner, or that the recipient of personal data from a company has an appropriate lawful basis for processing the data, or will protect the data in a compliant manner.

What this means in practice

- Companies must secure all personal data in transit and at rest. In practice, this means operating with encryption for all personal data, where appropriate, including any data associated with a device identifier, and using technical security measures for personal data in storage to protect against breach.
- Companies need to take stock of the personal data they need to fulfil their commercial goals and avoid receiving, collecting or storing data that exceeds these requirements.
- Companies need to view contractual assurances of compliance as a first step, to be followed by additional steps to establish confidence that the contract is adhered to, on an ongoing basis. This is likely to involve completing robust due diligence activities before commencing data sharing, and subsequently engaging suppliers in an ongoing audit and monitoring regime to ensure continued compliance.
- Ensure that your staff are fully trained (including annual refresher training) on UK GDPR and PECR,

6.2 What this means for media properties

- Third parties processing personal data from your site will be bound to a range of regulatory requirements and obligations, as well as commercial restrictions, when they are processing data.
- Take active steps to limit personal data collection by partners other than what is necessary to fulfil their stated purposes.
- Always have clarity with respect to the processor or controller nature of the partners to whom you transfer personal data or whom you enable to collect data from your site, and make sure their designations match the merits of their data usage models. This status should be documented in data processing contracts, data sharing agreements or data processing addendums, for example.
- All companies loading on your properties should be bound to specific contractual language ensuring compliance with the law and properly restricting their data collection to appropriate purposes. This means passing through contractual and diligence requirements, and ensuring participation in a self-regulatory framework, such as the TCF.
- Tag managers and header bidders can be used to impose some control on the third parties that have access to your properties, but in all cases, you will need to augment these controls with periodic audits or scanning technologies to ensure you are exercising appropriate control over the third parties that are collecting personal data on your properties.
- Ensure that your staff are fully trained on the technical and business model specifics of the partners they are allowing on your properties, including a full understanding of the personal data these partners are able to collect from your properties, and the purpose of the processing that the partners are engaged in.
- When personal data is ready for removal or end of life processes, ensure that deletion or anonymisation is complete and irreversible.

6.3 What this means for third party technology/intermediary companies

- Always have clarity with respect to the processor or controller nature of your partners, and make sure their designations match the merits of their data usage models. This status should be documented in data processing contracts, data sharing agreements or data processing addendums, for example.
- All companies operating on your behalf should be bound to specific contractual language ensuring compliance with the law and properly restricting their data collection to appropriate purposes.
- For data sharing within the TCF, you must look at the TCF consent string and make sure the recipient has a lawful basis for processing the personal data before you share it.
- For sharing personal data outside of the TCF, you should ensure that the recipient has an appropriate lawful basis and you should seek contractual

limitations and assurances regarding how data will be processed. Do not share personal data that is not required for allowed purposes under the contract.
- When personal data is ready for removal or end of life processes, ensure that deletion or anonymisation is complete and irreversible.

6.4 What this means for advertisers

- Ensure that your vendors are taking sufficient technical security precautions with personal data in transit and at rest. These assurances should be formally documented and reviewed in robust vendor due diligence work, completed before vendor data sharing takes place, and subject to ongoing monitoring/audit on a regular basis.
- Always have clarity with respect to the processor or controller nature of your partners, and make sure their designations match the merits of their data usage models. This status should be documented in data processing contracts, data sharing agreements or data processing addendums, for example.
- All companies operating on your behalf should be bound to specific contractual language ensuring compliance with the law and properly restricting their data collection to appropriate purposes.
- For your first party personal data, you should put in place appropriate technical and organisational measures to ensure that this data is processed securely and in compliance with UK GDPR by you and any third parties that you choose to share it with.
- When personal data is ready for removal or end of life processes, ensure that deletion or anonymisation is complete and irreversible.

7. Further Reading and Resources

ICO guidance
ICO Guide to data security
ICO Guide to Encryption
ICO Guide to deleting data
Security outcomes
ICO Data sharing code (Draft)
Direct marketing code (Draft)
Data minimisation
Purpose limitation
Data protection by design
Contracts and liabilities
Controller/processor contracts and liabilities

Case law examples

- British Airways fined £183million for poor security arrangements that failed to stop a cyber attack
- Uber fined £385,000 after a poorly controlled cyber-attack. Further fines in other European territories.
- Doorstep Dispensaree Ltd. (Pharmacy) fined £320,000 for failing to dispose of data correctly
- Marriott International fined £100million after a cyber-attack exposed failure to carry out due diligence following an acquisition.
- Tucker's Solicitors fined £98,000 for failing to protect against unauthorised or unlawful processing and against accidental loss of personal data after a ransomware attack.
- Cabinet Office fined £500,000 for failing to put appropriate technical and organisational measures in place to prevent the unauthorised disclosure of people's information.

Part 2: Data Security in Practice

1. About this guidance

The purpose of this part of the guidance is to provide the digital advertising industry with specific, illustrative examples of when and how appropriate security measures should be applied in different industry contexts. This guidance should be read in conjunction with Part 1, which offers detailed information on each security measure.

Note: this guidance does not address risks or mitigations not related to security. Our separate guidance on Data Protection Impact Assessments includes information about other risks that may arise from processing data typically used in digital marketing, and potential controls and mitigations for those risks (see Appendix B).

2. The risk-based approach to data security

This guidance document offers recommended data security good practices for three specific digital advertising example contexts. This guidance takes a risk-based approach to personal data security, meaning that the recommendations about appropriate data security measures are informed by a risk assessment methodology. Appendix 1 contains full details and further guidance on how to conduct a risk assessment in this context.

It is important to note that the processing activities and risk assessments contained within this guidance are illustrative examples only. It is your responsibility to conduct your own risk assessments that relate to your specific processing activities, although the recommended security measures outlined in this document can serve as a basis for good practice.

This guidance identifies three common digital advertising processing contexts, i.e. the typical use of personal data for the following typical RTB-related activities:

- Example 1: Precise location data in RTB
- Example 2: Ad profiling data collected over time from various sources
- Example 3: Device linking using hashed emails

Each of these examples presents, for each stage of the data processing, the likely risk grade and appropriate good practice security measures. Whilst the security measures discussed should be applicable to any digital advertising company processing the particular data types, the examples are necessarily presented from particular contexts. They don't cover all possible contexts or scenarios and it is your responsibility to conduct your own risk assessments and apply the most appropriate security measures based on your specific processing activities and circumstances.

This risk-based approach to data security has been developed based on the methodology set out in more detail in Appendix 1 and the table below, which details the necessity of each type of security measure, based on the risk grade. Each security measure is discussed in detail in Part 1 of this guidance. Taking encryption as an example: encryption is an essential security measure for high risk processing activities, is recommended for moderate risk processing activities and is optional for low risk processing activities.[9]

Table 1: Necessity of security measures based on risk

Note: this is intended as a guide, and is not prescriptive. You may decide to apply different measures depending on the circumstances and nature of the risk.

	Risk grade*		
Security measure	Low	Moderate	High
Encryption	Optional	Recommended	Essential
Pseudonymisation and/or anonymisation	Recommended	Essential	Essential
Data minimisation	Essential	Essential	Essential
Information security: security accreditation (ISO27001 or SOC2)**	Optional	Recommended	Essential
Data sharing: third party recipients have contractual processing obligations	Essential	Essential	Essential
Information security: third party recipients have security accreditation (ISO27001 or SOC2)**	Optional	Recommended	Essential

*for anything that is 'very low' risk, consider the necessity of applying measures that are recommended or essential from the 'low' risk category, as appropriate.
**refer to 'Data sharing' section detailed in Part 1

[9] Although not always essential, where you do not encrypt personal data, you should ensure other, appropriate security measures are in place commensurate with the risk, and you should be able to justify why you have not encrypted data.

3. *Example 1*: Precise location data used for ad serving in RTB

Context
Precise location data may be processed in the context of a mobile ad impression when an impression is offered up in RTB. Sometimes the precise location information is provided by the publisher or via the exchange, and other times the buyer might have this information from first-, second- or third-party sources.

While location data in latitude and longitude format is often relayed in RTB, in many cases this data is inferred based on IP location, which may not actually be precise. Where the underlying data is precise, as when the location is sent directly from the operating system as lat/long coordinates, extra precautions are appropriate. In this example, let us assume that the data is precise GPS coordinates.

The IAB Transparency and Consent Framework considers data to be precise if it is precise to a radius of less than 500 meters or for, GPS coordinates, has two or more decimal places.[10]

Precise location data can represent the physical behaviour of a data subject and can include or potentially be used to reveal sensitive information (such as location of a data subject at school, in hospital, at a place of worship). A third party may be able to infer special category data from location data, in certain circumstances, and you should evaluate this risk as part of your risk assessment. See our guidance on Special Category Data for more details.

A. Processing activity and data involved

The below table provides some simplified details of an *example* processing activity using precise location data in the RTB context.

Example 1: precise location data in RTB used for ad serving

Data type and purpose	Data subjects	Data categories
Bid request information to facilitate RTB transaction	Mobile users	IP address GPS coordinates Device data Various user IDs

[10] https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/#Special_Feature_1__Use_precise_geolocation_data

B. Risk **Assessment**

As described in Part 1 of this guidance, decisions regarding the appropriate implementation of data security should be based on a risk assessment. Full guidance on how to conduct a risk assessment can be found in Appendix 1.

Below is an *example* risk assessment for this processing activity. This risk assessment applies to **risks that may affect the data subject**, although as discussed in the Risk Assessment Methodology in Appendix 1, other types of risk (to the business itself) are possible and should be considered. The table below is for illustrative purposes:

Example 1: precise location data in RTB used for ad serving

Processing activity	Risks	Risk grade (likelihood x severity)
Collection and use	*Data misuse* Susceptible to misuse by parties with access	Unlikely + major harm = **moderate risk**
Storage/ retention	*Data breach* Data breach could expose data subjects to misuse of the data	Unlikely + major harm = **moderate risk**
Sharing	*Non-compliance by third parties* All of the risks above in the hands of the recipient	Possible + moderate/major harm = **moderate/high risk**

C. Risks and mitigations: 'at a glance' overview

The chart below summarises the recommended security measures that can be used to mitigate the identified risks, based on the likely risk grades for this processing identified in section B above, and the risk-based application of security measures shown in Table 1 in the first section of this guidance.

Section D below explains the application of each of the security measures in more detail.

Example 1: precise location data in RTB used for ad serving

Risk assessment (see section B)			Security measure (see table 1)				
Processing activity	Risk type	Risk grade	Encryption	Pseudonymisation/ anonymisation	Data minimisation	Information security	Data sharing measures
Collection and use	• *Data misuse*	Moderate	●	●	●	●	●
Storage/retention	• *Data breach*	Low		●	●		●
Sharing	• *Non-compliance by third parties*	Moderate/high	●	●	●	●	●

D. Security measures

Some aspects of this processing activity involve **moderate** to **high risk**, and so the data security measures implemented should be decided with this in mind.

Example 1: precise location data in RTB used for ad serving

Security Measure	Which risks might this mitigate?	Details
Encryption	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	We have identified that a data breach concerning this type of data would be low risk, but inappropriate access or misuse by first or third parties is a moderate risk. Therefore, encryption of this data is strongly recommended, though not essential. For more information on encryption, refer to our guidance in Part 1.
Pseudonymisation	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	This processing activity includes innately pseudonymised personal data (user IDs, IP address etc). No further anonymisation or pseudonymisation of data is required. (Note: anonymisation is not an appropriate security measure in this instance because the processing activity in the context of RTB depends on the ability to synchronise the personal data with an individual.)
Data minimisation	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	Data should be minimised, so that only the minimum data needed for the processing activity is used. In this context, a number of data minimisation techniques should be used, including: • Reducing geolocation precision prior to using/storing/sharing it by removing coordinate decimals, if feasible given the commercial application.

Example 1: precise location data in RTB used for ad serving

Security Measure	Which risks might this mitigate?	Details
		• Geo-fencing sensitive geographical places (hospitals, schools, places of worship) prior to transmission of the bid request. (Note: These techniques, and the principle of data minimisation in general, apply to all types of digital advertising company involved in processing this type of data, though in these examples apply more specifically to publisher measures).
Information security (accreditation)	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	Because of the risks associated with processing precise geolocation data, a high standard of information security should be applied. Entities that process this type of data, as well as third party data sharing recipients, should have achieved accreditation to a recognised and independently audited security standard such as ISO27001 or SOC2. For more information about information security measures and accreditations, refer to our guidance in Part 1.
Data sharing measures	• *Non-compliance by third parties*	Sharing precise geolocation data with third parties is a moderate/high-risk activity. Before sharing precise geolocation data, stringent contractual obligations should be put in place and due diligence processes completed to ensure that this data is only shared with parties who are able to ensure adequately secure and lawful processing of data. Data sharing audits should be carried out before sharing data and monitoring should be ongoing once data sharing begins (see Part 1). The TCF can facilitate some of these requirements. If third parties are unable to provide satisfactory assurances, you should not share this data.

4. *Example* 2: Ad profiling data collected over time from various sources.

Context

Location data via lat/long, or inferred from IP and URLs visited, are often combined with demographic information and other data provided from third party sources to infer segmentation that assigns device IDs into behavioural and other clusters of interest to advertisers. For example, a device that is seen on a French IP, browsing sites reviewing high end sports cars, that other third parties believe belongs to a household with children and several Mac-based devices, could be added to various segments that would inform ad targeting decisions. Over time the amount of data linked to a household or an individual increases, and on occasion might be combined with direct identifiers.

A. Processing activity and data involved

The below table provides some simplified details of an *example* processing activity which uses directly collected pseudonymised browsing data in combination with other directly identifiable third-party data sets to build a cross-device or household graph.

Example 2: Ad profiling data collected over time from various sources

Data type and purpose	Data Subjects	Data Categories
Ad targeting using first or third-party data combined with directly collected browser data	Mobile/web users	IP address GPS coordinates Device data Various user IDs Cross device browsing history, including inter-household data Demographic data Name Address Email address Purchase history Financial information

B. Risk Assessment

As described in Part 1, decisions regarding the appropriate implementation of data security should be based on a risk assessment. Full guidance on how to conduct a risk assessment can be found in Appendix 1.

Below is an *example* risk assessment for this processing activity:

Example 2: Ad profiling data collected over time from various sources

Processing activity	Risks	Risk grade (likelihood x severity)
Collection and use	*Special category data arising* Combining browsing data with other first, second- or third-party sources, especially if techniques such as machine learning and AI are used, present the possibility of discovering special category data-based segmentation, even if the company does not intend to do this.	Possible + major harm = **moderate risk**
	Data misuse Susceptible to misuse by parties with access	Possible + major = **moderate risk**
Storage	*Data breach* Data breach could expose data subjects to misuse of the data. Note that this is an example only, and as such the 'remote' chance of a data breach detailed here is also part of the example only. In practice, this would need to be determined on a case-by-case basis.	Remote + major = **low risk**
Sharing	*Non-compliance by third parties* All of the risks above in the hands of any third-party recipient.	Likely + major harm = **high risk**

C. Risks and mitigations: 'at a glance' overview

The chart below summarises the recommended security measures that can be used to mitigate the identified risks, based on the likely risk grades for this processing identified in section B above, and the risk-based application of security measures shown in Table 1 in the first section of this guidance.

Section D below explains the application of each of the security measures in more detail.

Example 2: Ad profiling data collected over time from various sources

Risk assessment (see section B)			Security measure (see table 1)				
Processing activity	Risk type	Risk grade	Encryption	Pseudonymisation/ anonymisation	Data minimisation	Information security	Data sharing measures
Collection and use	• *Data misuse*	Moderate	●	●	●	●	

	• *Special Category Data*	Moderate	●	●	●	●	●
Storage/retention	• *Data breach*	Low	●	●	●	●	
Sharing	• *Non-compliance by third parties*	High	●	●	●	●	●

D. Security measures

Some aspects of this processing activity involve **high risk**, and so the data security measures implemented should be decided with this in mind.

Example 2: Ad profiling data collected over time from various sources

Security measure	Which risks might this mitigate?	Details
Encryption	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	We have identified that the collection and use of this data, as well as the sharing of this data with third parties might be high risk. Therefore, encryption of this data is **essential.** For more information on how to implement encryption, refer to our guidance in Part 1.
Pseudonymisation	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	Combining data from various sources over time heightens the risk that this data becomes directly identifiable, and that sensitive or special category data may be inferred. Steps should be taken to maintain this type of data in a pseudonymous state throughout the entire digital advertising ecosystem.. This could mean removing possible or likely identifiers, especially from third-party data sets, if not needed, and implementing contractual obligations to maintain the pseudonymous state of the data if shared with third parties. For more information on pseudonymisation of data, refer to our guidance in Part 1. For more details on the risks of special category data arising or being inadvertently processed, and mitigating those risks, see our Special Category Data guidance, particularly Section 3.
Data minimisation	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	Data should be minimised, so that only the minimum data needed for the processing activity is used. Precision of data should be reduced, e.g.: • Delete time stamps if possible. Otherwise, reduce their precision. Consider using days/weeks rather seconds/hours. • Device and browser information can also be made less precise by removing certain data if not needed, such as build-ID or device-ID. • Location data should be made less precise, as described in example 1.

Example 2: Ad profiling data collected over time from various sources

Security measure	Which risks might this mitigate?	Details
		You should review whether there is a risk of special category data arising or being inadvertently processed as a result of processing ad profiling data, and put in place measures to mitigate that risk. For example, that may mean changing what data you collect, or the form in which it is collected, or it may mean recognising certain types of data as it comes into your system and not recording it in an identifiable form. For more details about how special category data may arise or be inadvertently processed as a result of the way in which other data is processed, and evaluating and mitigating that risk, see our Special Category Data guidance, particularly Section 3.
Information security (accreditation)	• *Data misuse* • *Data breach* • *Non-compliance by third parties*	Because of the risks associated with processing this data, a high standard of information security must be achieved. Entities that process this type of data, as well as third party data sharing recipients, should have achieved accreditation to a recognised and independently audited security standard such as ISO27001 or SOC2. For more information on information security measures and accreditations, refer to our guidance in Part 1 of this document.
Data sharing measures	• *Non-compliance by third parties*	Sharing this type of data with third parties is a high-risk activity. Before sharing such data, stringent contractual obligations should be put in place and due diligence processes completed to both restrict the third party's ability to process inferred special category data and to ensure that the data is adequately secure. Data sharing audits should be carried out before sharing data and monitoring should be ongoing once data sharing begins. If third parties are unable to provide satisfactory assurances, you should not share this data.

5. *Example 3*: Device linking using hashed email addresses

Context
An email address that has been collected from a consumer with consent and connected to a device ID, is often hashed for the protection of the underlying data, and then shared for matching purposes with other companies, who might have the same email hash connected to additional device IDs. As this process repeats, companies assemble a graph of device IDs that are linked by a common email hash. This device graph is used to connect ad targeting across the consumer's devices.

A. Processing activity and data involved

The below table provides some simplified details of an *example* processing activity using hashed email addresses in the digital advertising context:

Data type and purpose	Data Subjects	Data Categories
Hashed email address collected for cross device matching	Website visitor	Hashed email address Device ID

B. Risk Assessment

As described in Part 1 decisions regarding the appropriate implementation of data security should be based on a risk assessment. Full guidance on how to conduct a risk assessment can be found in Appendix 1.

Below is an *example* risk assessment for this processing activity:

Example 3: Device linking using hashed email addresses

Processing activity	Risks	Risk grade (likelihood x severity)
Collection and use	n/a	n/a
Storage	Data breach could expose data subjects to misuse of the data	Remote + minor = **very low risk**
Sharing	All of the risk above in the hands of the recipient	Possible + minor harm = **low risk**

C. Risks and mitigations: 'at a glance' overview

The chart below summarises the recommended security measures that can be used to mitigate the identified risks, based on the likely risk grades for this processing identified in section B above, and the risk-based application of security

measures shown in Table 1 in the first section of this guidance.

Section D below explains the application of each of the security measures in more detail.

Example 3: Device linking using hashed email addresses

Risk assessment (see section B)			Security measure (see table 1)				
Processing activity	Risk type	Risk grade	Encryption	Pseudonymisation/ anonymisation	Data minimisation	Information security	Data sharing measures
Storage/retention	• *Data breach*	Very low	n/a	n/a	●	●	●
Sharing	• *Non-compliance by third parties*	Low	n/a	n/a	●	●	●

D. Security measures

This processing activity is **low risk,** and so the data security measures implemented should be decided with this in mind.

Example 3: Device linking using hashed email addresses

Security measure	Which risks might this mitigate?	Details
Encryption	*n/a*	We have identified that the collection, storage and sharing of this data with third parties is likely low risk. Therefore, encryption of this data is not essential. Where you do not encrypt personal data, you should ensure other, appropriate security measures are in place commensurate with the risk, and you should be able to justify why you have not encrypted data.
Pseudonymisation	*n/a*	This processing activity includes partly pseudonymised personal data (hashed email address and device ID) meaning that direct personal identifiers are not processed. Note: anonymisation is not an appropriate security measure in this instance because the processing activity in the context of RTB depends on the ability to link the data together.
Data minimisation	• *Data breach* • *Non-compliance by third parties*	Although this processing activity is low risk, to comply with the GDPR, data should still be minimised, so that only the minimum data needed for the processing activity is used.

Example 3: Device linking using hashed email addresses

Security measure	Which risks might this mitigate?	Details
Information security (accreditation)	• *Non-compliance by third parties* • *Data breach*	Entities that process this type of data, as well as third party data sharing recipients, should have robust information security practices, which you should check as part of your due diligence and ongoing monitoring processes, but would likely not need to have achieved accreditation to a recognised security standard. For more information about information security measures and accreditations, refer to our guidance in Part 1.
Data sharing measures	• *Non-compliance by third parties* • *Data breach*	Although processing of this data is generally low risk, contractual obligations should be put in place with any third-party recipients and due diligence processes completed to ensure that this data is only shared with parties who are able to ensure adequately secure and lawful processing of data. The TCF can facilitate some of these requirements.

Appendix 1: Risk Assessment Methodology

Risk assessment methodologies are part of the wider organisational risk management framework. There are many approaches to information risk management, and you should develop a framework that best suits your organisational context, but the process should be formalised and documented.

Below is a suggested approach to organisational risk management:

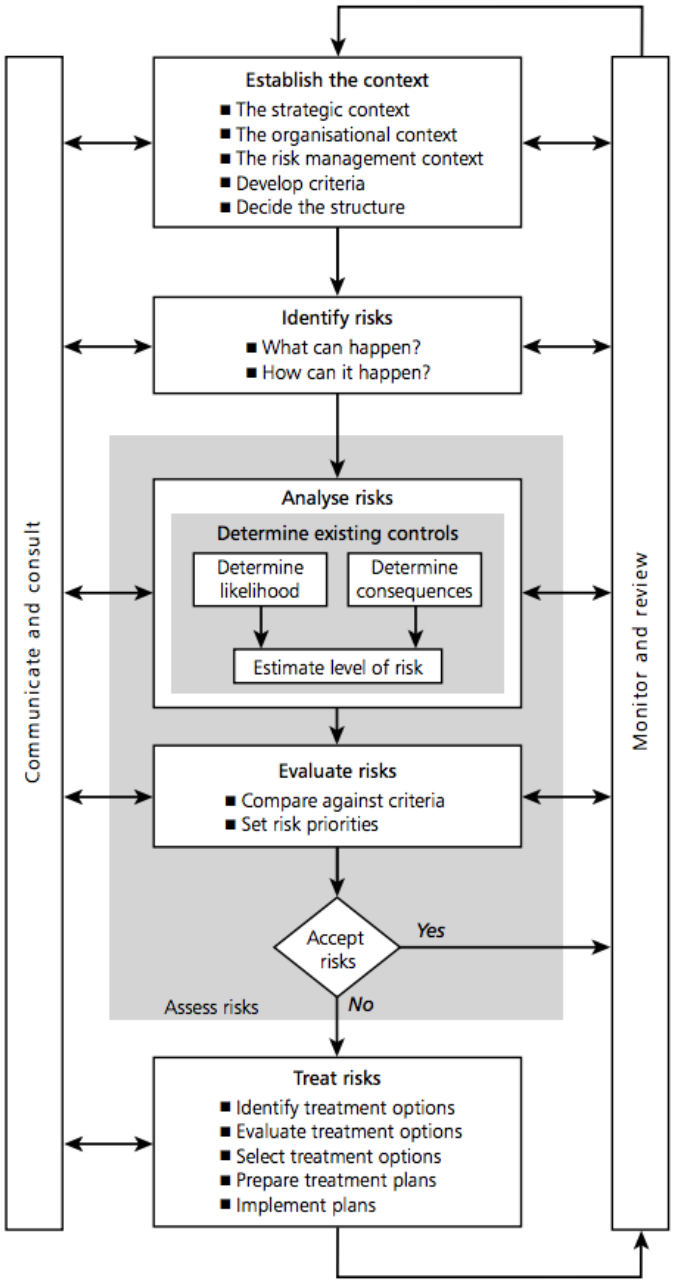

Figure 1: Risk Management Process, reprinted from Standards Australia: Risk Management Guidelines

Appendix 1: Risk Assessment Methodology

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? This will likely take the form of a Record of Processing Activity (see the relevant section of Part 1).

b) **Identify risks.** Think about information risks facing your organisation and the individuals whose personal data you are processing. What could happen to the data that you process? Why? How might this occur?

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

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.

e) **Report.** If you have identified any high risks, you must conduct a DPIA. DPIAs are also required for activities set out in the ICO's list published under Article 35(4) of the UK GDPR (see section 2.6 of Part 1 of this guidance). As RTB processes often involve high risk processing, DPIAs will likely be essential in many cases. For any risks which remain residually high after mitigation, you must consult the appropriate supervisory authority before starting processing. For further details, please refer to our separate guidance on DPIAs under the GDPR.

Analysing risks: calculating the risk level

Determining the level of risk should be an objective process. 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:

Table 1: 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.**

Consequences can affect data subjects, organisations and even the wider society and don't always have to be privacy related. It is important that you consider how an event will affect all relevant parties.

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.

The table below gives examples of consequences of different severities related to organisational events. The consequences will vary based on the circumstances, including the nature of the risk and the type of data being processed, and you should undertake your own assessment for your organisation and activities.

Table 2: Example consequences

Note: the examples in this table refer to the risks that might affect any organisation; they are not specific to organisations engaged in digital advertising or RTB specifically, but you can use the same methodology for your risk assessment process for your specific business activities. The main body of this guidance provides examples of assessing risks relating to RTB.

Risk context type/ descriptor	Severity of consequences				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Subject Privacy E.g. arising from disclosure of confidential or sensitive information.	Negligible harm to the individual, no sensitive, private or special category data processed.	Minor harm with no material detrimental effect on the person. Possibly processing some special category data, or able to infer special category data.	Moderate harm, for example minor damage to personal relationships and social standing.	Major harm, for example ID theft with potential adverse effects. Can include special category data, or able to infer special category data.	Extreme harm, for example ID theft with financial loss, losing a job, risk to life or health. Very likely to involve special category data, or able to infer special category data.
Project For example – a data breach affects an ongoing project.	Barely noticeable reduction in scope / quality / schedule of a new system	Minor reduction in scope / quality / schedule	Reduction in scope or quality, project objectives or schedule	Significant project over-run	Inability to meet project objectives, reputation of the organisation seriously damaged
Customer Service	Minor reduced quality of	Unsatisfactory user experience,	Unsatisfactory user experience,	Unsatisfactory user experience	Unsatisfactory user experience

Appendix 1: Risk Assessment Methodology

Risk context type/ descriptor	Severity of consequences				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
e.g. poor access/integrity/ quality of data leads to poor user experience.	user experience	easily resolvable	short term effects – expect recovery <1wk	long term effects – expect recovery - >1wk	continued ongoing long term effects
Complaints / Claims In the event of a data breach or other data governance failure	Locally resolved verbal complaint	Written complaint	Complaint and valid request for compensation to losses	Multiple complaints taking extensive investigation and compensation	Complaint to regulator
Business Interruption Business Continuity issues due to cyberattacks or server unavailability for example.	Minor interruption in a service with no consequences	Short term disruption with minor impact	Some disruption in service with unacceptable impact on business Temporary loss of ability to provide service	Sustained disruption with serious impact on business. Major contingency plans being invoked.	Permanent loss of service.
Financial e.g. derived from compensation rights ransomware, fines	Negligible organisational / personal financial loss (£<10k)	Minor organisational / personal financial loss (£10k-100k)	Significant organisational / personal financial loss (£100k-250k)	Major organisational / personal financial loss (£250 k-1m)	Severe organisational / personal financial loss (£>1m)
Inspection / Audit e.g. ICO audit	Minor quality improvement issues needed. May include voluntary, internal audits or ICO consensual audits.	Recommendations made which can be addressed by low level of management action. May include voluntary, internal audits or ICO consensual audits.	Challenging recommendations that can be addressed with appropriate action plan. May include voluntary, internal audits, ICO consensual audits or compulsory audits/investigations.	Enforcement action as a result of non-compliance. Small fine	Enforcement action/ prosecution as a result of non-compliance. Large fine
Adverse Publicity / Reputation e.g. media attentions due to data	No media coverage Little effect on staff morale	Local media coverage – short term. Minor effect on staff morale /	Local media – long-term adverse publicity.	National media / adverse publicity, less than 3 days.	National / International media / adverse publicity, more than 3 days.

Appendix 1: Risk Assessment Methodology

Risk context type/ descriptor	Severity of consequences				
	Negligible	Minor	Moderate	Major	Extreme
breaches or cybersecurity attacks		public attitudes.	Significant effect on staff morale and public perception of the organisation	Public confidence in the organisation undermined Use of services affected	Parliamentary discussion Court enforcement Public enquiry

III. Calculating the risk level: risk assessment matrix

Use the risk matrix below to calculate the risk level.

Note that any event or incident might have risks across multiple user groups and contexts/activities. You should apply risk assessment methodologies to all affected areas.

In terms of grading risks, the following grades have been assigned within the matrix.

- Very Low Risk (VLR)
- Low Risk (LR)
- Moderate Risk (MR)
- High Risk (HR)

Table 3: Risk grade matrix

Likelihood	Consequence				
	Negligible	Minor	Moderate	Major	Extreme
Almost certain	LR	MR	HR	HR	HR
Likely	LR	MR	MR	HR	HR
Possible	VLR	LR	MR	MR	HR
Unlikely	VLR	LR	LR	MR	MR
Remote	VLR	VLR	VLR	LR	LR

References and Further Reading

British Standards Institute: Risk Management Vocabulary
https://shop.bsigroup.com/ProductDetail/?pid=000000000030078231

Standards Australia: Risk Management Guidelines
http://www.epsonet.eu/mediapool/72/723588/data/2017/AS_NZS_4360-1999_Risk_management.pdf

Appendix 1: Risk Assessment Methodology

Northern Ireland Department of Health, Social Services and Public Safety. How to Classify Incidents and Risk. A guidance document. Contact Heather.Shepherd@dhsspsni.gov.uk

Appendix 2: Retention guidance

The purpose of this section of the guidance is to provide the digital advertising industry with guidance on how to determine and apply retention periods in practice. This guidance should be read in conjunction with the main body of this guidance document, which offers detailed information and background on data security and retention best practices.

Storage Limitation is a central principle of the UK GDPR. To comply with this principle, **personal data must not be kept for longer than is necessary.** If personal data is retained for longer than it is legitimately needed, it is likely that this processing is not fair or lawful. The ICO has produced detailed guidance on data retention and storage limitation.

This guidance contains the following resources:

- Appendix 1: Retention Schedule Template
- Appendix 2: Retention Period Assessment Template

Data retention
The GDPR does not provide retention periods and does not mandate that you destroy personal data within a prescribed timeframe. Each organisation processing personal data must determine, justify and document its own retention periods and is accountable for these decisions.

You can retain personal data for as long as you have a genuine, fair and lawful purpose for processing this data. Although personal data can be retained for as long as it is genuinely needed, the retention period should be balanced against the expectations of and risks to the rights and freedoms of the data subject.

If you have no justifiable and lawful purpose for retaining personal data, you must securely delete or anonymise this data - you cannot keep personal data indefinitely, without a justified purpose. For further guidance on deletion and anonymisation, please refer to the IAB's Data, Security and Retention Guidance.

It is your responsibility to determine the appropriate retention period for your organisation's processing of personal data, depending on the specifics of your local context.

How to determine retention periods
We have developed a Retention Period Assessment (RPA) approach for this guidance, along with an RPA Template (see Appendix 2) which can be used to inform, document and justify the decisions that you make.

Appendix 2: Retention guidance

The RPA is similar to other privacy assessments that you may be familiar with (such as a Privacy Impact Assessment (PIA) or a Legitimate Interest Assessment (LIA)), particularly as the assessment relies on your own judgement in determining the appropriate retention period on a case-by-case basis.

We suggest that you determine your retention periods in relation to the purposes of your processing activities. This is because you can retain personal data for as long as at least one of your purposes for processing still applies. It is not possible to determine an appropriate retention period for discrete personal data elements (for example a cookie_id, or name and contact information) without first understanding what the purpose is for holding and processing this information.

It is possible that certain data types serve more than one purpose, and there may therefore be different retention periods for different processing activities that use the same data. As long as one purpose of processing still applies, you can retain the data.

You should be able to identify the purposes of your processing activities by drawing on the information contained in your Record of Processing Activity (ROPA) which details all of the processing activities, their purposes and other contextual information within your organisation.

You should consider all of the factors in the RPA, plus any others you believe are relevant, and come to a balanced and justifiable conclusion. Documenting and justifying your decisions on personal data retention in this way will also help you to satisfy the GDPR accountability principle.

In determining retention periods for personal data, you should consider the following factors for each of your processing activities (note: this is not necessarily an exhaustive list; include any other relevant considerations that you identify):

Appendix 2: Retention guidance

Primary Considerations	
About the Data	*The context of the processing*
	Lawful basis for processing
About the Processing	*Necessity and utility*
	Relationship with the data subject
External Factors	*Future legal claims*
	Legal obligations
	Regulatory guidelines
Supplementary Considerations	
Other factors	*Fairness*
	Risks

How to complete a Retention Period Assessment (RPA)
The RPA process is an objective assessment that should be approached without a predetermined expectation of the outcome.

There is no set algorithm that can be used to determine your retention periods at the end of the analysis – it is up to you to come to a reasonable and balanced determination based on your assessment. This is where expertise, experience, and objectivity are crucial, and why trained privacy professionals are best situated to make the determination.

In the below guidance we discuss what factors you should consider when determining your retention periods and how they relate to each other. At the end of the assessment, you are asked to come to a justifiable and balanced decision regarding the retention period, detailed in the Making the Final Determination section of this guidance.

Primary considerations

About the data

Understanding the context of the processing will help you identify the purpose for processing the data and document the types of data and data subject that the processing relates to. You can then use this information to inform your decision-making, considering the other relevant factors.

The Context of the Data Processing
You should accurately document the contextual information relating to the processing activity. Similar to an LIA or DPIA process, the nature of the data and data subjects will directly inform your consideration of risk later in the RPA process. For example, processing data that is more private or sensitive will likely increase the risks associated with the processing, including retention. You should

Appendix 2: Retention guidance

document:

- Processing activity and purpose
- Data types (e.g., name, address, DoB, ID number, cookie ID, MAID, etc.)
- The nature of the data, including, for example:
    - is it data which people are likely to consider particularly 'private'?
- Data subject types: whose data are you processing? Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

The Lawful Basis for Processing
The lawful basis can have an impact on retention periods. For example, for consent-based processing, the retention period may be linked to the consent status and the possible need to renew consent. Although unlikely in an ad-tech context, if the data is processed in order to satisfy a contract with the data subject, then the retention periods may be tied to the performance of that contract. You should document and consider:

- What is the lawful basis for processing the data?
- Does this affect the retention period?

<u>About the processing</u>
This information is key to understanding the maximum potential length of the retention period, as you can keep the data for as long as genuinely necessary, and no longer (unless there are legal reasons for doing so – see next section).

Whether or not the data is necessary in some cases *might* be influenced by how long the data remains useful for the specific purpose for which you are processing it, and this may change over time.

Necessity and utility
Data retention in most cases is going to be primarily defined by the organisation's genuine need to keep the data. In the absence of legal obligations and regulatory guidelines, this is likely the most important section to use in determining your retention period. Data can be retained for as long as it is legitimately needed to satisfy the purpose of the processing. Use these questions to determine the period for which the data is genuinely and legitimately needed:

- Necessity:
    - How long is this data genuinely needed for the purpose, and why?
    - Will there come a point when the purpose of the processing no longer applies to the data?
- Utility:

- Are there diminishing returns of utility over time? Does data become less useful over time?
- Does data accuracy diminish over time?
- When will the data likely stop being useful? (Be specific and quantify where possible).
- What are the data storage costs? Will these eventually outweigh the benefits of retaining the data? As long as data is retained, all GDPR obligations and data subjects rights will remain, and appropriate storage limitation will help to manage this situation.

Relationship with the data subject
Your relationship with the data subject might impact on your decisions regarding retention periods, and so you should consider and document the nature of the relationship. For example, your relationship with the data subject might be only temporary and have a natural end.

- What is the nature of your relationship with the data subject?
- Will this relationship come to an end (and if so, when/how)?

<u>External factors</u>
In addition to identifying how long you need to retain the data for the processing purpose, there may be legal requirements or regulatory guidance that specify either a minimum or maximum retention period. You need to identify those and use them to help determine your overall retention period. Where there are minimum periods for which you must retain the data (i.e., for legal claims or legal obligations), you should still determine whether or not you can and will retain the data beyond that period (based on the other relevant factors).

If you are required to keep data for future legal defences or because of legal obligations, you can only retain it for other purposes so long as those other purposes continue to apply.

Future legal claims
Sometimes you may need to retain data to defend against possible legal claims, although in an advertising context this unlikely to be necessary. You should consider:

- How likely is it that data is needed to defend against future legal action relating to the processing?

Legal obligations
There may be legislation that mandates that you retain particular data for a certain period of time, typically a minimum period, although this is also unlikely in an advertising context. Note that a legal obligation to

retain data for a specified time should take precedence over the other factors listed in the RPA. You should consider:

- Are there legal obligations to keep personal data for a specified time?
- If there is a minimum specified period, consider if it is this shorter or longer than the period for which you otherwise need to retain the data. If it is shorter, then you need to determine and document any additional retention. If it is longer, consider whether you need to keep the data in its original form and whether any other data minimisation is appropriate.

Regulatory guidance
Regulators and/or industry bodies may issue guidance or best practices on data retention. If relevant regulatory guidelines on retention exist, then these should likely take precedence over other considerations (with the exception of legal obligations). If you deviate from applicable regulatory guidelines on maximum retention periods, by keeping the data for longer than advised, then you should be able to justify this robustly. You should consider:

- Are there any retention guidelines for this type of data and/or this processing activity?
- If so, what are they? How will you apply them in practice?

Supplementary Considerations

Although the legitimate necessity of the data for the processing purpose is the most important consideration, in practice your assessment should also take into consideration the fairness of the retention period as it relates to the expectations of the data subject as well as the risks to the data subject associated with the processing.

Fairness

Data subjects' expectations are important in considering how you meet the fairness principle of the GDPR, including in relation to retention of their personal data, which must be fair and lawful.

For example, it is possible that organisations may consider it necessary to retain data for long timeframes, and have justifiable and legitimate reasons for doing so. However, due consideration should be given to the expectations of the data subject about how long their data would be retained and used for the activity/purpose in question.

You should use the below questions to prompt an analysis of the expectations of the data subject regarding the retention of their data. You should consider:

Appendix 2: Retention guidance

- How long would the data subject expect you to keep their data?
- Is the nature of your relationship with the data subject likely to affect their expectation about how long you retain their data?
- Is there any research or other information that you can use to understand data subjects' expectations?'
- What are the possible impacts on individuals caused by retaining their data?

Risk

You may also wish to consider the risks associated with the data processing (including its retention) and how they should be managed. Even if you determine that you have a legitimate need to retain personal data, you can choose to keep it for a shorter period. Shorter retention periods can potentially mitigate some of the risks associated with high-risk processing activities, including risks related to data security (see Part 2 of this guidance: Data Security in Practice for more details). You should also be able to draw on other risk assessments that you have carried out for your processing activities, such as DPIAs. You should document:

- What is the risk level for this processing activity?
- Do the risks vary over time?
- Do the risks you've identified impact on the length of the retention period and if so, how?

Making the final determination

You should first assess whether any of the external factors apply (legal claims, legal obligations, regulatory guidelines) as these will give you a strong steer as to the appropriate retention period for your data. In the absence of external factors you should consider your legitimate need for retaining the data given the purpose of the processing. This is the most important factor to consider as you can legally retain data for as long as you legitimately need it, and your retention remains fair and lawful. Finally, you should balance your legitimate needs against the expectations of the data subject and the risks that the processing may have on individuals.

You should then determine a retention period and record the justification for your decision.

Annex A: Retention Schedule Template

Processing Activity	Data Types	Data Source	Retention Start	Retention period	Action at end of retention period	Link to Retention Period Assessment Documentation

Annex B: Retention Period Assessment Template

RPA Domain	Details
The Context of the Processing	
Processing Activity	
Data Types	
Data Subject Types	
Is the data special category data or criminal offence data?	
Is it data which people are likely to consider particularly 'private'?	
Are you processing children's data or data relating to other vulnerable people?	
Is the data about people in their personal or professional capacity?	
Lawful Basis	

Annex B: Retention Period Assessment Template

What is the lawful basis for processing the data?	
Does this affect the retention period?	
Necessity and utility	
How long is this data genuinely needed for the purpose, and why?	
Does the data become less useful over time?	
Does data accuracy diminish over time?	
What are the data storage costs? Will the costs of storage eventually outweigh the benefits of retaining?	
When will the data likely stop being useful?	
Relationship with the data subject:	
What is the nature of your relationship with the data subject?	

Will this relationship come to an end?	
Future Legal Claims	
How likely is it that data is needed to defend against future legal action relating to the processing?	
Legal Obligations	
Are there legal obligations to keep personal data for a specified time?	
Regulatory Guidance	
Are there any retention guidelines for this type of processing activity	
Fairness and Risk	
How long would the data subject expect you to keep their data?	
Do you have any evidence about these expectations – e.g. from market research, focus groups or other forms of consultation?	

What are the possible impacts of the processing on people?	
What is the risk level for this processing activity?	
Do the risks vary over time?	
Do the risks impact on the length of the retention period?	
Retention Period	
Justification	