2024

UK GDPR CHECKLIST AND GUIDE FOR PROFESSIONAL INVESTIGATORS

CONFEDERATION of
Professional Investigators UK
CoPI

CONTENTS

IMPORTANT
COPI UK advises that **all** investigations be conducted in accordance with UK GDPR and the Data Protection Act 2018, and as prescribed from time to time by the Information Commissioner's Office. This document is a **guide** to best practice, it is **not** a code of conduct.

INTRODUCTION

UK GDPR applies to most areas of business, including the Professional (Private) Investigation fraternity, whether a sole trader, limited company or multi-national organisation who collects, stores and/or processes personal data. On paper thanks to certain entities, it seems to be a complicated science that has had some Investigators in a state of total despair thinking they will go out of business if they don't do this or that, which costs them financial commitments they can ill afford. Panic not because the Guide you are about to read is intended to clarify the mysteries of UK GDPR and signpost you to ICO authoritative data protection information, it is totally free, as are the included example templates which are ready for use. Most important of all said Guide is for the Investigation Industry as a whole not possessively restricted to any one organisation, and practitioners nationwide regardless of affiliations are welcome to be part of the COPI UK community. Having said that lets get started.

WHAT IS PERSONAL DATA?

The official definition is said to be " any information relating to an **identifiable** living person", and there are two categories (a) **Personal** (b) **Sensitive special**.

UK GDPR and data protection may differ from one trading entity to another, however, sole trader or micro organisations should be able to incorporate GDPR into their daily operations without too much difficulty, taking a design and default approach to the required processes. Hopefully this guide will navigate you along the way.

WHAT IS PROCESSING?

The initial definition on first sight is quite frightening as follows:

- **Collecting**
- **Recording**
- **Organising**
- **Storing**
- **Adapting**
- **Altering**
- **Retrieving**
- **Consulting**
- **Using**
- **Disclosing by transmission**
- **Disseminating or otherwise making available**
- **Restricting**
- **Erasing**
- **Destroying**

In simpler terms the processing of personal data includes information from any source be it electronic, human, or written.

Important: Yes we are attempting to clarify UK GDPR, however this does not mean Investigators should think they don't have to have a thorough knowledge of the areas that are relevant to their work. You should embrace GDPR as much as possible as it is part of our daily routine.

It is interesting to note past comments from the ICO:

> ***"Every organisation is different and there is no one-size fits-all answer**. Data protection law doesn't set many absolute rules. Instead it takes a risk-based approach, based on some key principles. This means it's flexible and can be applied to a huge range of organisations and situations, and it doesn't act as a barrier to doing new things in new ways.*
>
> *However, this flexibility does mean that you need to think about - and take responsibility for - the specific ways you use personal data. Whether and how you comply depends on exactly why and how you use the data - and there is often more than one way to comply."*

Richard Newman, BA(Hons), C.I.P.I., Member I.P.S.A., says of this guide:

"Given that UK GDPR and the Data Protection Act is not an easy concise piece of legislation to understand, the Confederation of Professional Investigators UK have managed to produce a simplified check list and guide that in my opinion will assist the industry."

DISCLAIMER

Whilst this publication has been prepared from the Information Commissioner's Officer (ICO) guides, briefings and regular updates, along with research and contributions from knowledgeable sources**, the contents are not, repeat <u>not</u>, being presented as a definitive guide or source**. Furthermore no information presented in this publication should be treated as legal advice, as it has been prepared, and commented on above, by those not legally qualified, therefore in any case of difficulty or doubt the reader should obtain their own legal advice. Readers should refer to ICO guides for more detailed advice, updates and specific decision making.

UK authority for Data Protection :

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone helpline: 0303 123 1113

Website: www.ico.org.uk

Investigation Sequence of Events

STAGE 1

Initial discussion by potential client, check ID and contact details. Carry out due diligence if required *(example form is shown at Annex '1')*. Think about a Lawful Basis.

STAGE 2

Thorough assignment briefing from client and documented. Consider your Lawful Basis for the Investigation.

STAGE 3

LAWFUL BASIS

From the following under Article 6(1) of the UK GDPR at least one must prevail:

(a)	**Consent**	the individual has given clear consent for you to process their personal data for a specific purpose.
(b)	**Contract**	the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c)	**Legal Obligation**	the processing is necessary for you to comply with the law (not including contractual obligations).
(d)	**Vital Interests**	the processing is necessary to protect someone's life.
(e)	**Public Task**	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f)	**Legitimate Interests**	the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Many of the lawful bases for processing depend on **'necessity'** and must be more than just useful or standard practice. Processing must be targeted and a proportionate way of achieving a specific purpose. The lawful basis will not apply if the desired result can be achieved by a less intrusive means or by processing less data. There must be a lawful reason for processing, 'curiosity' is **not** such a reason : **NB** beware this is a grey area.

WHY IS THE LAWFUL BASIS IMPORTANT?

Article 5 of the UK GDPR sets out **7 Key Principles** that are required when processing data stating that personal data must be:

1. **Lawfulness, fairness and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality (security)**
7. **Accountability**

In addition the **Accountability** principle was introduced as a new concept in the UK GDPR, which means it is no longer enough just to do the right thing, there is now a requirement to **keep records** of processes and reasons for certain conclusions. Such as justifying the use of Legitimate Interests as a grounds for processing a person's personal data.

Accountability requires the following additional obligations:

1. Keeping detailed records of processing activities
2. Carrying out a Data Protection Impact Assessment (DPIA) for high-risk processing
3. Appointing a Data Protection Officer (DPO)
4. Implementing data protection by design and default
5. Maintaining a record of data breaches
6. Notifying the ICO of all breaches

This principle requires one to take responsibility for what is occurring with personal data and how to comply with the other principles. There must be in place appropriate measures and records to be able to demonstrate compliance.

Further information

ICO – A Guide to Lawful Basis

ICO – UK GDPR Principles at a glance

ICO – UK GDPR Accountability

LAWFUL BASIS ASSESSMENT

Depending on the aim of processing when deciding what lawful basis will apply consider the following:-

1. Who does the processing benefit?
2. Would the data subject expect processing to occur?
3. What is your relationship with the data subject?
4. Are you in a position of power over them?
5. What will be the impact on the individual?
6. Are they vulnerable?
7. Are individuals likely to object?
8. Are you able to stop the processing at any time on request?

Carry out a Lawful Basis Assessment and document it - see ICO interactive tool.
NB: For PI's **Legitimate Interests** is 'usually' the lawful basis, however, there are occasions when consent will be the Lawful Basis. **Refer to the ICO links below.**

Further information

ICO – At a glance : Lawful Basis for Processing

ICO – Lawful Basis Interactive Guidance Tool

Remember : once a lawful basis has been identified for an investigation and controlling/processing of personal data commences it should be handled in line with the UK GDPR principles, a check list could be kept to hand as a reminder, see example at Annex '2'.

STAGE 4

LEGITIMATE INTERESTS ASSESSMENT (LIA)

Before processing begins under the lawful basis of Legitimate Interest an LIA (Legitimate Interests Assessment) must be carried out in order to confirm beyond any doubt this basis will apply, and a written record made in order to demonstrate compliance in line with accountability obligations under UK GDPR Articles 5(2) and 24.

ICO have a sample Legitimate Interests LIA template click here, and an further non-ICO example Assessment template is set out at Annex '3'.

Further information

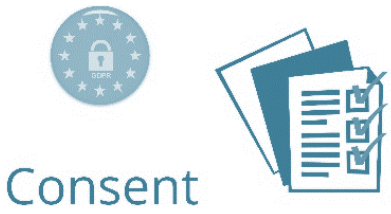
ICO – At a Glance : Legitimate Interests

ICO - Legitimate interest assessment (LIA)

ICO Legitimate Interests sample LIA Template

STAGE 5

CONSENT



This is an important Lawful Basis in certain situations.

EXAMPLE 1:

An investigation where Consent may apply is when working for **private clients**. For instance tracing the whereabouts of a long lost relative whose reason for avoiding contact is unknown. Whilst it seems appropriate to carry out a trace under the auspices of Legitimate Interests to process data that leads to the current address of the individual, it does not mean the investigator can inform the client of the relative's address under the Lawful Basis of Legitimate Interests. In fact to reveal someone's current address without their consent could be interpreted as a breach of UK GDPR. The suggested method of satisfying the client's request, whilst protecting the data subject's privacy is by way of a process known as **Consent to Share** also known as **Post Consent.**

Consent to Share suggested process –

- Have in place with the client an agreement that if the relative is located then they will be approached by the investigator who will explain the client's request.
- In the event the data subject agrees to their personal information being passed on then a signed 'consent to share' statement be obtained from the data subject.
- If consent is given the current address can be released to the client.
- In the event the data subject does not give consent then their personal data should not be released to the client.
- **NB** a letter from the client to pass to the relative located via the investigator might also be possible.

Note: Investigators have to be aware that there all manner of requests presented by private clients, some are genuine others are clearly not so and include requests from stalkers disguising their reasons with lies and deception. The criminal fraternity are known to falsify reasons for tracing people, along with divorced parents seeking to repatriate children from overseas locations. The list of fake private clients is endless, and all investigators should be alert to this fact. The method of detecting such cases is simply to conduct **in-depth due diligence** of individuals seeking to employ investigative services.

EXAMPLE 2: Corporate or other business clients

Many types of businesses frequently employ the services of Private Investigators in respect of enquiries where **Consent** is the Lawful Basis for processing personal data for instance:

- Job applications and checking CVs
- Applications for financial loans
- Consumer purchases on credit/HP
- Security Vetting of staff

These are but a few examples there are other similar types where Consent is required. Investigators should ensure that evidence of Consent has been obtained by the client before engaging in the processing of the data subject's personal data, such evidence should then be retained in the investigator's records.

Note: during all investigations great care must be taken to ensure the appropriate Lawful Basis prevails. Furthermore investigators should ensure detailed records are kept in accordance with UK GDPR . Finally, remember a Data Subject has an abundance of legally protected rights and for an investigator to ignore or breach these rights could result in criminal charges or a civil claim against not just the investigator but also the client.

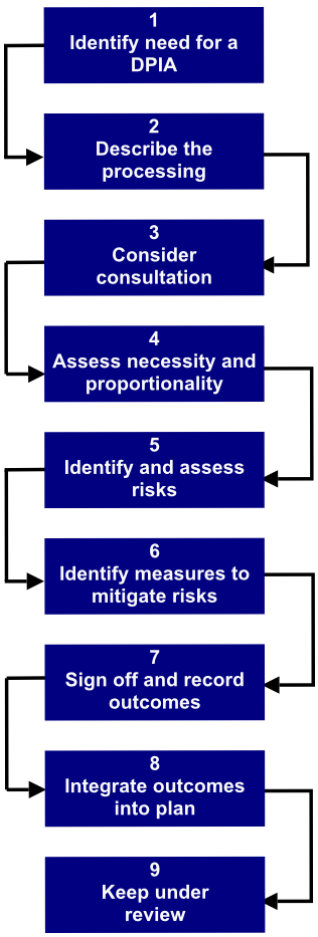
STAGE 6

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Before commencing an investigation a DPIA might be appropriate for specific high-risk projects. It could well be the investigator has in place a standing DPIA which applies to their business activities, particularly for multiple identical tasks for the same client.

Under the UK GDPR **Privacy by Design and Default** is a major requirement that is a legal obligation for everyone to design and implement policies and procedures that will protect data security. In other words privacy is built in from the start of every data processing situation. A key part of this is **Data Protection Impact Assessments**. This process will be different for all organisations and/or sole traders, that said there are basic elements applicable to everyone working to UK GDPR.

Depending on the complexity and nature of the investigation it is recommended that a Data Protection Impact Assessment is carried out prior to commencing. Even if there is no specific indication of likely high risk, the ICO state it is good practice to do a DPIA for any major new project involving the use of personal data. A DPIA should run alongside the planning and development process of the project, and include the following steps:



According to the ICO publishing a DPIA is not a requirement of UK GDPR, however there could be benefits in that it will demonstrate compliance and engender trust and confidence in one's business, especially if serious complaints result in a court appearance. The ICO therefore recommends that you publish a DPIA where possible removing sensitive details if necessary.

The process is designed to be flexible and scalable and to document the assessment one can utilise the ICO sample DPIA template or create one's own.

Further information

ICO – At a glance : Data Protection Impact Assessments and Checklists

ICO Detailed Guidance - Data Protection Impact Assessments (DPIAs)

STAGE 7

SPECIAL CATEGORY DATA

Article 9 of UK GDPR set outs an additional list of personal data which are collectively known as **Special Category data** (also referred to as sensitive data) :

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply (see ICO link below).

In addition to the lawful basis identified for processing you can only process special category data if you can meet one of the specific conditions in Article 9 of the UK GDPR. You need to consider the purposes of your processing and identify which of the following conditions are relevant:-

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated conditions in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If you are relying on the condition (g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

An investigator should have in place the highest security standards available at all times during and after processing, and also have in place a retention policy.

Further information

ICO – Special Category Data

ICO Criminal offence data

STAGE 8

DATA CONTROLLERS AND PROCESSORS

There have been lengthy discussions within the sector on the role of Controller and Processor, with reams of discourse on said subject.

The Data Controller role holds, without doubt, the higher burden and risk in UK GDPR. Get it wrong as a Controller and should you end up in court then there is a strong probability you will be convicted because GDPR places higher obligations on Controllers.

Data Controllers are the main decision makers who exercise overall control of the **purpose** and **means** of processing personal data (NB: an investigation can also have **Joint Controllers)** **e.g.** your client, say a Solicitor, decides that the purpose and means to process data to deal with a legal problem will be to pass the case to you to process personal data. This means the client is clearly the **Data Controller**, and as you will be processing said data you are clearly going to be the **Data Processor** and providing you don't commit any breaches of law during the course of your investigation there should be no problems arising. This situation is important to us all as investigators in that if we get sucked into being or assumed to be controllers the legal ramifications are seriously high risk.

This was experienced by a Surrey Investigator who was deemed by the ICO to have been a Data Controller. This resulted in him being charged with a number of offences that were heard in the Crown Court. Fortunately he was able to convince the Court that he was in fact a Data Processor and not a Controller. The prosecution failed in their attempts to get a guilty result and the investigator won his day in Court.

Data Processors act on behalf of and only on the instructions of a Controller.

There now follows a summary of the definitions and obligations of these roles.

DATA CONTROLLER

Definition : the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data.**

Obligations
If you are a controller, you are responsible for ensuring your processing complies with the UK GDPR, including any processing carried out by a processor on your behalf. Your responsibilities include the following:

- Compliance with the data protection principles
- Individuals' rights
- Security
- Choosing an appropriate processor
- Processor contracts
- Notification of personal data breaches
- Accountability obligations
- International transfers
- Appointing a representative within the European Union
- Co-operation with supervisory authorities
- Data protection fee

(The above is a summary CLICK HERE to see ICO guidance for full details)

JOINT DATA CONTROLLER

Definition: Where two or more controllers jointly determine the purposes and means of processing, they shall be **joint controllers**.

If two or more separate organisations collate data and use it for a common purpose it is said they will be joint controllers. They do not need to be processing the data at the same time or regularly. For instance, a firm of Lawyers instructs a Private Investigator to trace a defendant in a court case and in doing so passes personal information relating to the data subject to assist the investigation. As the investigator is now in possession of the same data as the instructing lawyer, who is clearly the controller in such a case it seems, then the PI may become a joint controller. However once they embark on the investigation by a means they determine their role changes.

Obligations:

- **Obligations of controllers**: You need to decide with your fellow joint controllers who will carry out which controller obligation under the UK GDPR. However, regardless of those arrangements, each controller remains responsible for complying with all the obligations of controllers under the UK GDPR as set out in the Data Controller section above.
- **Transparent arrangement**: Joint controllers are not required to have a contract, but you must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the UK GDPR. The main points of this arrangement should be made available to individuals. It is recommended that you include this in your privacy information.
- **Individuals' rights**: In particular, you must decide (and be transparent about) how you will comply with transparency obligations and individuals' rights. You may choose to specify a central point of contact for individuals. However, individuals must remain able to exercise their rights against each controller.
  (The above is a summary CLICK HERE to see ICO guidance for full details)

DATA PROCESSORS

Definition: a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller.**

Obligations:

- Controller's instructions
- Processor contracts
- Sub-processors
- Security
- Notification of personal data breaches
- Notification of potential data protection infringements
- Accountability obligations
- International transfers
- Appointing a representative within the European Union
- Co-operation with supervisory authorities

(The above is a summary CLICK HERE to see ICO guidance for full details)

DUE DILIGENCE BY DATA CONTROLLERS IN RESPECT OF DATA PROCESSORS

Article 28(1) of UK GDPR relates to the obligations of a data controller to carry out enough due diligence on the data processor before instructing them for a processing activity. Attention by the controller should be applied to:

- Expert knowledge
- Reliability
- Resources
- Adherence to an approve code of conduct
- Approved certification

A data controller is responsible not just for its own compliance but also that of its data processor and any sub-processors used.

Further information

ICO at a glance ICO Controllers and Processors guidance

ICO detailed guidance on Controllers and Processors

ICO Small Business Web Hub

ICO - Controllers self-assessment checklist

ICO - Processors self-assessment checklist

STAGE 9

SUB-PROCESSORS

It is not uncommon for a private investigator to sub-contract part or all of an assignment to another agency. In such a situation the sub-contractor becomes a **sub-processor**. To comply with UK GDPR the investigator should have in place a contract with the Processor who is instructing them, and the Processor should have permission of the controller to sub-contract the assignment. See fuller description below.

Definition: In circumstances where a processor sub-contracts part or all of the processing to a third party then this party becomes a sub-processor. Note: this title is not taken from the UK GDPR itself but is a shorthand term used for the description in Article 28(4) GDPR which simply refers to this role as *"where a processor engages another processor".*

Obligations:

- As a sub-processor you must comply with the obligations imposed on processors as listed in the section above.
- You will be liable for any damage caused by your processing if you have not complied with said obligations or you have acted contrary to the controller's lawful instructions, relayed by the processor, regarding the processing.
- A sub-processor may also be contractually liable to the processor for any failure to meet the terms of their agreed contract. This will of course depend on the exact terms of that contract.

AUTHORISATION REQUIRED TO APPOINT A SUB-PROCESSOR:

If you wish to use a sub-processor, you **must obtain the controller's written authorisation**. The authorisation can be specific or general.

Specific authorisation means the controller must approve the particular sub-processor for the particular processing operation in question.

General authorisation means:

- the controller pre-approves a list of potential sub-processors; or
- the controller approves a list of criteria that you can use to select and appoint a sub-processor.

If you have general authorisation, you must inform the controller if you wish to make any changes to the list of possible sub-processors or criteria for choosing a sub-processor, and give the controller a chance to object. You must send the controller any proposed changes in writing, setting out the date by which the controller should raise any objections. The controller should also respond in writing and explain the reasons for any objections.

Note: The fact that you may sub-contract some or all of the processing activities you have been engaged to perform does not make you a controller in your own right, as overall control of the processing remains with the original controller.

If you use a sub-processor to carry out processing on your behalf, you will be fully liable to the controller for the sub-processor's compliance. This means that, under Article 82(5), if a sub-processor is at fault, the controller may claim back compensation from you for the failings of the sub-processor. You may then claim compensation back from the sub-processor.

Further information

ICO at a glance ICO Controllers and Processors guidance

ICO guidance on Controllers and Processors

ICO - Who is liable if a sub-processor is used?

STAGE 10

Following the conclusion of an assignment all personal data - electronic or hard copy - should be securely held in accordance with UK GDPR. When the information is no longer required it should be erased or disposed of in a secure manner as recommended by the ICO

Further information on Security and Retention

ICO Security, including cyber security

ICO - Data storage, sharing and security - Small Businesses

ICO – FAQs on Data storage, sharing and security – Small Businesses

ICO - Retention and destruction of information

STAGE 11

SUBJECT ACCESS REQUESTS (SAR) including EXEMPTIONS and DATA SUBJECT'S RIGHTS

Important : Throughout the investigation the processing of a data subject's personal information should be in accordance with UK GDPR and the Data Protection Act 2018. An investigator should be aware that at any time during, or after, the investigation a data subject has a number of legal rights including the right to submit a Subject Access Request (SAR) requesting the release of data that is being held on file about the individual the investigator is legally required to respond within 30 days.

Details of data subjects' rights and subject access requests are as follows:

Every Data Subject has rights and if you as an investigator abuse, or ignore them consequences will almost certainly prevail in the form of large fines, prosecution and/or both. These rights are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the right to be forgotten)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

RIGHT TO ACCESS

Under the **right to access** a Data Subject has the legal right to request access to any personal data being held or processed about them by any business or official department. This is done by way of a **Subject Access Request**, which is usually submitted in writing, but can be done verbally – note: the ICO recommend any verbal submission should be followed up in writing.

Further information

ICO Individual's Rights guidance

DEALING WITH A SUBJECT ACCESS REQUEST (SAR)

1. Check the ID and contact details of the individual. You need to be satisfied that you know the identity of the requester (or the person the request is made on behalf of). If you are unsure, you can ask for information to verify an individual's identity. The timescale for responding to an SAR does not begin until you have received the requested information. However, you should request ID documents promptly.

2. You must comply with a SAR without undue delay and at the latest within one month of receiving the request. You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual, eg other types of requests relating to individuals' rights.

3. Consider if an exception may be appropriate, for example is it vexatious or a fishing expedition during an ongoing court case.

4. If you are satisfied it is a bonafide request carefully prepare your response and remember the applicant is only entitled to their data, however she/he may ask how you obtained the information and if it was obtained legally. In this writer's opinion a data subject is not entitled to copy documents such as reports to clients and witness statements which will in any event be disclosed in accordance with Disclosure Rules.

5. In most cases you cannot charge a fee to comply with a SAR. However, you can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

6. Data subjects may request the following items from a Data Controller:

   a. Confirmation that you're processing or have processed their personal data.

   b. Copy of their personal data, but no data of other people.

   c. Other mandatory information as specified in Article 15(1) – *note: you may already be providing this information in a privacy notice.*

      - the purposes of your processing;
      - the categories of personal data concerned;
      - the recipients or categories of recipient you disclose the personal data to;
      - your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
      - the existence of their right to request rectification, erasure or restriction or to object to such processing;
      - the right to lodge a complaint with the ICO or another supervisory authority;
      - information about the source of the data, where it was not obtained directly from the individual;
      - the existence of automated decision-making (including profiling); and
      - the safeguards you provide if you transfer personal data to a third country or international organisation.

   d. In the event you have recorded incorrect data you can be requested to delete and or amend mistakes.

EXEMPTIONS TO DATA BEING PROVIDED AS PART OF AN SAR

There are certain exemptions to the data you are being requested to disclose in response to an SAR, as set out in Schedules 2 and 3 of the UK's Data Protection Act 2018 as follows:

- Crime and taxation: general
- Crime and taxation: risk assessment
- Legal professional privilege
- Functions designed to protect the public
- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Judicial appointments, independence and proceedings
- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Other exemptions ***CLICK HERE for ICO details on SAR Exemptions***

Further information

ICO Subject Access Requests guidance

ICO How to deal with a request for information: a step-by-step guide

ICO Subject access request template for small businesses

THE RIGHT TO ERASURE - ALSO KNOWN AS THE RIGHT TO BE FORGOTTEN

Under Article 17 a data subject can write and request that they want to exercise their right to be forgotten. When the right applies you have an obligation to forget the data subject and erase the vast majority of personal data you hold on them. This right is different from an opt-out where consent has been relied upon as a lawful basis.

WHEN DOES THE RIGHT TO ERASURE (TO BE FORGOTTEN) APPLY?

- When personal data is no longer necessary for the reason the data was collected and/or processed in the first place.
- When the data subject withdraws consent on which basis the processing was based and this is no other legal ground for processing.
- When the personal data is processed on the grounds of legitimate interests or public interest and the data subject objects and there is no overriding legitimate interest to continue processing.
- When data has been unlawfully processed.
- When data has to be deleted to comply with a legal obligation.

- When the data was collected in relation to processing for the offer of online services to a child.

WHEN THE RIGHT TO ERASURE (TO BE FORGOTTEN) DOES NOT APPLY

- For exercising the right of freedom of expression and information.
- For compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority.
- For reasons of public interest in health and safety situations.
- For archiving purposes in the public interest.

CHILDREN'S DATA

Beware if you are collecting or processing personal data relating to children. This is an area of operation where one should utilise the guidance from the ICO on the current UK GDPR regulations before processing such information. *ICO - Children and the UK GDPR*

ARE PHOTOGRAPHS PERSONAL DATA?

It all depends on the purpose of a photograph as to whether or not it will be classified as personal data according to UK GDPR. Therefore if an investigator takes a covert photograph of a specific data subject then this clearly must be classified as personal data and will need to be handled in the same way as written data. The photograph should only be taken if a lawful basis exists.

STAGE 12

ACCOUNTABILITY & DOCUMENTATION

Under the **Accountability Principle** and Article 30 of the UK GDPR organisations are required to have in place specific documentation to demonstrate compliance.

An investigator should therefore be paying attention to best business practice and be incorporating UK GDPR into its overall working practices as a matter of course. This can be evidenced by formally documenting the following, which includes the required information under the UK GDPR, and can be shared publicly on a company web site and/or shared with clients offline:-

1. Data Protection Policy – this should be a detailed document.
2. Privacy Notice displayed on web site.
3. Retention policy – separate or included in Data Protection Policy.
4. Data Breaches handling process – separate or included in Data Protection Policy.
5. Subject Access Requests – separate or included in Data Protection Policy.
6. Data Inventory/Mapping.
7. Terms of Business.
8. Documented business standards.
9. Training programme and records.
10. Complaints procedure – separate or included in business standards.
11. Have appropriate insurance in place.
12. How and when documents are reviewed.

DATA INVENTORY ALSO KNOWN AS DATA MAPPING

An aspect of documentation under UK GDPR relevant to an investigator is a **Data Inventory**, also known and **Data Mapping**, which can show all sources of data, where they have come from, what is being processed, where they are held, why they are used, how they are shared and how long they are kept.

Whilst this information should be included in a Privacy Policy, it can be useful to document it by way of a data inventory or map. Deciding if and how a data inventory should be completed will depend on factors such as the size of your organisation, the volume of personal data processed, and the complexity of the processing operations. The ICO has produced templates which may be too complex for a micro organisation or sole traders, hence **their use is not mandatory** and the ICO advises that basic forms can be used. However the templates can be a good starting point and can be adapted accordingly.

For investigators the sources of data may come from:

- Forms on website
- Open Source Intelligence – OSINT
- Employee application form
- Direct from client
- Director for event attendees
- From suppliers
- Paid for database websites, tracing, credit search etc
- Third parties – i.e. benefit providers
- Third parties treated witnesses or sources of intelligence
- Cookies on your web site

In addition below are examples of what data may be processed by an investigator:

- Financial and lifestyle
- Medical in personal injury cases
- Family and domestic
- Contact information such as emails, addresses, phone numbers, websites, Facebook, LinkedIn
- Property ownership
- Employment history
- Human resources
- CCTV images
- Photographs

Further information

ICO Documentation guidance

ICO Accountability guidance

STAGE 13

DATA BREACHES

Under UK GDPR there is a legal requirement to report to the ICO within 72 hours of becoming aware of any breach that is likely to result in a risk to a person's rights and freedoms.

The ICO states : *"When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you do not have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it."*

Attached at Annex '6' is an example breach of personal data report form, to be completed and retained regardless of whether a report is made to the ICO.

Further information

ICO Data Breaches Guide
ICO Data Breach examples
ICO Self Assessment for data breaches
ICO How to report a Data Breach

STAGE 14

LEGISLATION RELEVANT TO PROFESSIONAL INVESTIGATORS

Investigators keen to demonstrate best business practice should also have a working knowledge of the following legislation which is considered essential in terms of the provision of investigative services.

- The Data Protection Act 2018 and UK General Data Protection Regulations (GDPR)
- Regulation of Investigatory Powers Act 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000
- The Human Rights Act 1998.
- The Protection from Harassment Act 1997
- The Computer Misuse Act 1990
- The Private Security Industry Act 2001
- The Criminal Procedure and Investigations Act 1996 or the Criminal Procedure (Scotland) Act 1995.
- The Civil Procedure Rules 1998 Part 31 (Disclosure).
- The Laws of Trespass and Stalking.

In addition knowledge of the following legislation is considered desirable in terms of investigative service, subject to the nature and scope of the services provided.

- The Consumer Credit Act 2006
- The Police and Criminal Evidence Act 1984 (PACE) and the PACE codes of practice; and the Criminal Procedure Rules 2020
- The Public Interest Disclosure Act 1998
- The Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002
- The Protection of Freedoms Act 2012
- The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022
- The Bribery Act 2010
- The Fraud Act 2006
- The Theft Act 1968
- The Consumer Insurance (Disclosure and Representations) Act 2012
- The Equality Act 2010

Annex '1'

EXAMPLE POTENTIAL CLIENT DUE DILIGENCE REPORT FORM

Full Name of client _____

Address _____

_____

_____

Telephone _____

Fax _____

E-mail _____

Website _____

Type of Business _____

Who recommended or how did client know of company? _____

Nature of Assignment _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Feasibility

1 Can this assignment be completed legally? Yes ☐ No ☐

2 Can we plan and implement this operation in accordance with our normal terms of business and method of operation, also in accordance with current Legislation and Best Practice? Yes ☐ No ☐

3 Describe any legal or Health and Safety Risks :

_____

_____

_____

4 Is there any known Conflict of Interest? Yes ☐ No ☐

_____

_____

5 Is there a lawful basis to process data if assignment accepted? Yes ☐ No ☐

_____

_____

_____

Contact and ID details confirmed Yes ☐ No ☐ Partial ☐

Method Companies House ☐ Open Source Search ☐

Previous client ☐ Current client ☐

Report

Can we accept? Yes ☐ No ☐ *Refer to report*

I the undersigned confirm this Assignment is acceptable/not acceptable as indicted

Name ..... Date .....

Annex '2'

EXAMPLE UK GDPR PRINCIPLES CHECK LIST

REMEMBER
PERSONAL DATA MUST BE:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with a person's rights;
- Kept Secure; and
- Not transferred to other countries without adequate protection
- Accountability

Annex '3'

EXAMPLE LEGITIMATE INTERESTS ASSESSMENT (LIA) TEMPLATE

In accordance with the UK GDPR & Data Protection Act 2018 [company name] relies upon "Legitimate Interests" as its legal basis for lawfully processing data for this assignment. In accordance with ICO guidance and the UK GDPR this LIA has been conducted and recorded to demonstrate compliance in line with [company name] accountability obligations under Articles 5(2) and 24 of GDPR.

Purpose Test

Why do you want to process the data?	
What benefit do you expect to get from the processing?	
Do any third parties benefit from the processing?	
Are there any wider public benefits to the processing?	
How important are the benefits that you have identified?	
What would the impact be if you couldn't go ahead with the processing?	
Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?	
Are you complying with other relevant laws?	
Are you complying with industry guidelines or codes of practice?	
Are there any other ethical issues with the processing?	

Necessity Test

Will this processing actually help you achieve your purpose?	
Is the processing proportionate to that purpose?	
Can you achieve the same purpose without the processing?	
Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?	

Balancing Test

Nature of the personal data	
Is it 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?	
Reasonable Expectations	
Do you have an existing relationship with the individual?	
What's the nature of the relationship and how have you used data in the past?	
Did you collect the data directly from the individual? What did you tell them at the time?	
If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?	
How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?	
Is your intended purpose and method widely understood?	
Are you intending to do anything new or innovative?	
Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?	
Are there any other factors in the particular circumstances that mean they would or would not expect the processing?	
Likely Impact	
What are the possible impacts of the processing on people?	
Will individuals lose any control over the use of their personal data?	
What is the likelihood and severity of any potential impact?	
Are some people likely to object to the processing or find it intrusive?	
Would you be happy to explain the processing to individuals?	
Can you adopt any safeguards to minimise the impact?	
Can you offer individuals an opt-out	

Decision: Can you rely on legitimate interests for this processing? : [YES/NO] Based upon the above three part test [company name] is satisfied that "Legitimate Interests" under UK GDPR is an appropriate legal basis in respect of the investigatory services it will be providing to this client. Other considerations: Under legitimate interests an individual's right to data portability does not apply.

Review: This LIA was carried out on [date] in accordance with ICO guidance. It will be reviewed if there is a significant change in the purpose, nature or context of the processing.

Signed ..... Date .....

Annex '4'

EXAMPLE BREACH OF PERSONAL DATA REPORT

Date of Breach	
Who discovered the breach?	
Details of Data	
Identity of Data Subject(s)	
Potential damage to Data Subject(s)	

Action take to rectify	
Notify ICO?	**YES** ☐ **NO** ☐
Other actions implemented	

Report completed by : Name: …….

Signed : ……..

Date : ……..……..