

Appropriate Policy for processing Special Category Data (sensitive personal information)

Contents

Overview	2
Changes since Brexit.....	2
Policy Scope	2
Who is this policy for?	3
Purpose.....	3
What is personal data?.....	4
Special Category Data.....	4
Criminal Offence Data	4
Lawful Consent for Processing Data.....	4
Six lawful reasons.....	4
Conditions for processing special category data and criminal offence data	5
Schedule 1 condition for processing	6
UK GDPR Seven Principles	6
The UK GDPR sets out seven key principles:.....	6
Procedures for ensuring compliance with the principles.....	7
Principle: lawfulness, fairness, and transparency.....	7
Principle (b): purpose limitation	7
Principle: data minimisation	7
Principle: accuracy.....	7
Principle: storage limitation	8
Principle: integrity and confidentiality (security)	8
Retention and erasure policies	8
Data Security.....	8
How you can access your data.....	8
Contacting the regulator	9
Regulatory references	9
Appendix One-Article 5 UK GDPR	10
Appendix Two Personal Data.....	11

Overview

All our stakeholders should feel confident in Professional Assessment Limited (PAL's) handling of their personal data and how we use such data and be assured that we will only request and process essential data and that we strive to ensure data and information is collected, recorded, and compiled accurately and only used for stated purposes.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

All personnel involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

Professional Assessment Ltd (PAL) is committed to a policy of protecting the rights and privacy of individuals, staff, associates, consultants/TAs, and others in accordance with Data Protection Legislation¹. This policy applies to all personal data processed by PAL.

This policy provides information about the legal basis and safeguards that PAL has put in place for sensitive processing, the processing of special categories of personal data and criminal convictions data.

Our ICO registration number is ZA275792.

Changes since Brexit

The EU's GDPR has been lifted into a new UK-GDPR that took effect on January 31st, 2020. An adequacy decision for the UK and the Law Enforcement Directive (LED) was adopted on June 28, 2021, by the EU, securing unrestricted flows of personal data between the two blocs until June 2025.

Policy Scope

The policy includes processing relating to:

- PAL staff
- PAL Associates and Consultants/TAs
- Individuals external to PAL – for example, an apprentice, when a person applies for a role at PAL, when an organisation provides PAL with data or services to support our data collection and processing activities for our core work

This policy should be read in conjunction with PAL's Data Protection and Privacy Policy. PAL also includes privacy notices for our Whistleblowing, Maladministration and Malpractice, Complaints and Appeals and Enquiries policies.

Special Category personal data (as with all personal information) must be handled and dealt with appropriately however it is collected, recorded, and used, and whether it is on paper, in electronic records or recorded in other formats, on other media, or by any other means.

¹ From 1st January 2021, the law relating to data processing in the UK changed. Any processing of data prior to 1st January 2021 has been undertaken in accordance with EU General Data Protection Regulation (EU) 2016/679 ("the EU GDPR"). From 1st January 2021, the EU GDPR no longer applies to the UK. The UK has retained the EU GDPR under Section 3 of the European Union (Withdrawal) Act 2018 (EUWA). It has been renamed as the UK GDPR and tailored by the Data Protection Act 2018. From 1st January 2021, the UK data protection regime consists of the UK GDPR as incorporated under the EUWA and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC) and the Data protection Act 2018 as enacted in May 2018 and amended by the DPPEC Regulations.

Who is this policy for?

This policy is for both PAL personnel and all PAL's stakeholders, including contractors and suppliers. It includes information held on computers (including email), paper files, photographs, audio and video recordings and images.

Purpose

The purpose of this policy is to detail how PAL will handle and treat any special category data that we need to collect in order to meet our contractual and legal obligations.

This document provides information about the legal basis and safeguards that PAL has put in place for sensitive processing, the processing of special categories of personal data and criminal convictions data. The Data Protection Act 2018 (DPA 2018) outlines the requirement for an appropriate policy document when processing special category data and criminal offence data under certain specified conditions.

Almost all the substantial public interest conditions in Schedule 1 part 2 of the DPA 2018 require an appropriate policy document to be in place to demonstrate compliance with the requirements of Article 5 UK GDPR.1. **The ICO notes that one collective document for the processing of sensitive information is sufficient.**

As part of PAL's statutory and corporate functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK GDPR and Schedule 1 of the Data Protection act 2018. In summary, we process data about our employees, and prospective employees, to fulfil our obligations as an employer. We also process this data, for reasons of legitimate business interest and substantial public interest, to perform our role as a regulated End-point Assessment Organisation, (EPAO) responsible for the **assessment** design, development, delivery, and award of publicly funded apprenticeships (qualifications).

DPA 2018

The DPA 2018 continues to set out the framework for data protection law in the UK. It was amended on 01/2021 by regulations under the European Union Withdrawal Act to reflect UK's status outside of the EU.

The main changes to the old regulations are:

- Transparency- more detailed and informative privacy notices are required
- The purpose of, and legal basis for processing data must be explained in clear and simple terms

The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing, but the way you interact with European data protection authorities has changed.

The EU Commission must monitor developments in the UK on an ongoing basis to ensure that the UK continues to provide an equivalent level of data protection. The Commission can amend, suspend, or repeal the decisions if issues cannot be resolved. Also, EU data subjects or an EU data protection authority can initiate a legal challenge to the decisions. The Court of Justice of the European Union would then have to decide whether the UK did provide essentially equivalent protection.

All PAL personnel are aware of the requirements of the UK GDPR. They appreciate the impact of this piece of legislation and the associated updates and of areas of work that could cause potential compliance problems under

the GDPR. The Business Operations Director and Director of Audit and Compliance will be responsible for staff training and compliance.

We are committed to ensuring that the principles of data protection that predicate GDPR are embedded into everything we do.

What is personal data?

The UK GDPR applies to the processing of personal data that is:

wholly or partly by automated means; or

the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.

Personal data only includes information relating to natural persons who:

- **can be identified or who are identifiable, directly from the information in question; or**
- **who can be indirectly identified from that information in combination with other information**

See Appendix Two for further amplification regarding personal data.

Special Category Data

Special category data is defined as data revealing or concerning:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- political opinions, sexual life, sexual orientation
- trade union membership
- biometric data². PAL does not process this category of data
- genetic data

Criminal Offence Data

Criminal offence data is defined as data revealing or concerning:

- offences (including alleged offences)
- criminal proceedings, outcomes, and sentences (regulated qualifications, including allegations of fraud and malpractice; relevant criminal convictions related to staff)

Lawful Consent for Processing Data

The UK GDPR³ lists six lawful conditions for processing personal data, and at least one condition must apply for an organisation to be able to collect, collate, process and store data that constitutes personal data.

Six lawful reasons

1. Consent is given to process data
2. Data collection and processing is necessary to perform and undertake business and forms part of the contract between two parties
3. Legal obligation
4. Protection of life
5. The processing of data meets the requirements for being in the public interest
6. Legitimate interests

² The UK GDPR defines biometric data in Article 4(14):

“‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data”.

³ See Article 6 of the UK GDPR

In most circumstances, PAL's legal basis for processing the personal data for the listed activities are Articles 6(1)(a), (b) and (f). These are:

- 6 (1)(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- 6 (1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- 6 (1) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Conditions for processing special category data and criminal offence data

The processing of special categories of personal data is only permitted where special conditions and the associated data are required to support PAL's contractual and legal obligations apply. In most circumstances, PAL's legal basis for processing special category personal data is covered by Articles:

- **Article 9(2)(b)** – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Processing under this condition would include the information we process for recording staff sickness absences, staff qualifications and training and information required to access benefits such as health insurance.
- **Article 9(2)(f)** – for the establishment, exercise, or defence of legal claims
- **Article 9(2)(g)** – processing is necessary for reasons of substantial public interest...which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interest of the data subject. In respect of this condition, PAL would process data for statutory and government purposes; to ensure equality of opportunity or treatment; regulatory requirements and support for individuals with a particular disability or medical condition and safeguarding of children and individuals at risk.

PAL is a regulated AO⁴ (end-point assessment organisation), delivering end-point assessment for a range of apprenticeship standards, working with many apprentices, employers, and providers. PAL also offers a commercial and independent audit and compliance function.

As an EPA we are subject to regulation by the qualifications regulator Ofqual, we are also bound by the terms and conditions of the approved providers and endpoint assessment register (APAR), overseen by the ESFA and must comply with the apprentice standards and accompanying assessment plans as published by IfATE. Examples of data we may process under special category data, include the application and approval of reasonable adjustments in assessments and in specific cases, depending on the circumstances this may extend to the processing of special considerations applications.

Additionally in addressing any disclosures regarding an individual's well-being and safety, from either PAL personnel or others, this condition would be applied in any processing of data and sharing of information with relevant

⁴ Ofqual refers to all regulated awarding organisations as Aos, PAL uses the term EPAO and/or AO

authorities and bodies. Our processing of data in this context is for the purpose of substantial public interest and necessary for the carrying out of our role.

Article 9(2)(a) – the data subject has given explicit consent to the processing of those personal data. Circumstances in which PAL might rely on consent include where we process information about dietary requirements for an event or conference, or where we request or are provided with information to enable us to make reasonable adjustments for individuals regarding how they receive our materials or access our services. For EPA work we are obliged to seek the consent of the individual apprentice to request an apprenticeship certificate, we request this consent during the assessment planning meeting, and we ask the apprentice to opt in and their decision is recorded on the assessment planning document.

Article 9(2)(c) – processing is necessary to protect the vital interests of the data subject or of another natural person. This would include circumstances where we might disclose medical information about an employee in an emergency.

We process criminal offence data in accordance with Article 10 UK GDPR

Schedule 1 condition for processing

Schedule 1 of the DPA 2018 identifies that to rely on certain conditions for processing data, an appropriate policy document must be in place. We process personal data for the following purposes:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security, or social protection (Sch 1, Part 1, Paragraph 1)
- The processing is necessary for reasons of substantial public interest (Sch 1, Part 2)
- The processing is necessary for statutory or government purposes (Sch 1, Part 2, Paragraph 6)
- The processing is necessary for the purposes of equality of opportunity or treatment in identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained (Sch 1, Part 2, Paragraph 8)
- The processing is necessary for racial and ethnic diversity at senior levels of organisations (Sch 1, Part 2, Paragraph 9)
- The processing is necessary for the purposes of complying with a regulatory requirement which involves taking steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice, or other seriously improper conduct (Sch 1, Part 2, Paragraph 12)
- The processing is necessary for the purposes of (i) protecting an individual from neglect or physical, mental, or emotional harm, or (ii) protecting the physical, mental, or emotional well-being of an individual (Sch 1, Part 2, Paragraph 18)
- The processing is necessary for the purposes of obtaining legal advice, establishing, exercising, or defending legal rights or in connection with, any legal proceedings (including prospective legal proceedings) (Sch 1, Part 3, Paragraph 33)

UK GDPR Seven Principles

The UK GDPR sets out seven key principles:

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

7. Accountability

These principles inform PAL's approach to data collection, management, and processing.

See Appendix One for further details regarding the GDPR principles

Procedures for ensuring compliance with the principles

1. Accountability principle
2. We maintain documentation of our processing activities
3. We adopt and implement data protection policies and have written contracts in place with data processors. We also implement information sharing agreements with other data controllers where appropriate
4. We routinely carry out data protection impact assessments, as part of our risk management and self-evaluation reviews
5. We implement appropriate security measures in relation to the personal data we process
6. We adopt a 'data protection by design and default' approach
7. We have appointed a data protection officer who is the Director of Audit and Compliance

Principle: lawfulness, fairness, and transparency

- We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices, policy documents which we make publicly available (including this policy document).
- Our processing for purposes of substantial public interest is necessary for the exercise of designing, developing, delivering assessment instruments, and requesting certification for apprenticeship standards, which are regulated qualifications, with the regulatory body being Ofqual.
- Our processing for the purposes of employment relates to our obligations as an employer.
- We also process special category personal data to comply with other obligations imposed on PAL in its capacity as a regulated body bound by conditions set by Ofqual and the Conditions for being on the End-Point approved register, overseen by the ESFA, so for example we will monitor data for equality opportunity reasons

Principle (b): purpose limitation

- We process personal data for purposes of substantial public interest when the processing is necessary for us to fulfil our statutory functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts
- We only collect data necessary to deliver our services to our clients and to meet the requirements of the qualifications regulatory body and the ESFA who are responsible for the issuing of apprenticeship certificates. We are explicit about to whom and how and why we share data with other bona-fide third parties
- We will not process personal data for purposes incompatible with the original purpose it was collected for

Principle: data minimisation

- We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it in line with our retention schedule

Principle: accuracy

- Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay, during any period of checking we will suppress processing in respect of the individual or individuals concerned. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision

Principle: storage limitation

- All special category data processed by us for the purpose of employment or substantial public interest, for example to ensure equality of access to assessment opportunities and to avoid disadvantaging any individual or groups of individuals in achieving their apprenticeships. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs
- Our retention schedule is reviewed regularly by the DPO and updated when necessary

Principle: integrity and confidentiality (security)

- Electronic information is processed within our secure networks. Hard copy information is processed in line with our security procedures
- Our electronic systems and physical storage have appropriate access controls applied. The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate

Retention and erasure policies

- Our retention and erasure practices are set out in our data, archiving and anonymisation statement

Data Security

We recognise the importance of data security and take a number of measures to ensure the security of personal data. These include training all staff on data protection and cyber security via in-house training.

Access to your personal data is password-protected, and only those with permission are granted access. Any misuse of personal data by our employees, is considered a disciplinary offence and a full investigation is automatically initiated. Any misuse of data by any of our associates and consultants/technical advisors will result in an investigation and the potential termination of their service level agreements.

All personnel associated with PAL are required to sign confidentiality agreements, which makes reference to data protection.

Any breach of data security is recorded in PAL's governance reporting system, data as required, and our Business Operations and Director of Audit and Compliance review our data collection and storage protocols, to ensure we only collect the data we require to discharge our services.

We conduct randomised checks on employees, associates, and consultants/technical advisors equipment as part of our ongoing and continual improvement of organisational and technical security measures, alongside reviewing our IT security.

How you can access your data

We try to be as open as we can be regarding giving people access to their personal information. Individuals can find out if we hold any personal data by making a '**Subject Access Request**' (SAR). There is no charge for such a request, and we will respond within 30 days of a verified request.

Regarding information we hold on you, we will:

- Give you a description of it
- Tell you why we are keeping it
- Tell you who it could be disclosed to
- Let you have a copy of the information in an intelligible form

To make a SAR to us for any personal information we may hold you need to put the request in writing addressing it to either:

- email: info@professionalassessment.co.uk- subject SAR
- Or by posting to: Connect House, Kingston Road, Leatherhead, Surrey, England, KT22 7LT

To protect the confidentiality of your information, we will ask you to verify your identity before we proceed with any request you make under this Privacy Policy. If you have authorised a third party to submit a request on your behalf, we will ask them to prove they have your permission to act. From the date, we receive this information we will respond within 30 days.

We will try to deal with your request informally if you agree this is the best way to proceed, for example by providing you with the specific information you need over the telephone or by email. If we do hold information about you, you can ask us to correct any mistakes by using the same email or postal address above.

If we choose not to action your request, we will explain to you the reasons for our refusal. If we feel your application isn't covered under the definition of a SAR, we shall endeavour to assist you to the best of our ability.

Contacting the regulator

If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, you have the right to complain with the Information Commissioner's Office (ICO). You can contact them by calling [0303 123 1113](tel:03031231113). Or go online to www.ico.org.uk/concerns (opens in a new window; please note we can't be responsible for the content of external websites).

Regulatory references

PAL is required to establish and maintain compliance with regulatory conditions and criteria. This policy relates to Ofqual General Conditions of Recognition: availability of adequate resources A5 - retention of data; - arrangements with third parties C1

Date Created: 15th April 2022

Last Review: 15th March 2023

Next Review: 15th March 2024

Person Responsible for review: Director of Audit and Compliance

This Policy has been agreed by Linda Martin, Managing Director

Appendix One-Article 5 UK GDPR

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’)

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’)

(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay (‘accuracy’)

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’)

(f) 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 (‘integrity and confidentiality’)

Article 5(2) adds that:

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”

For more detail on each principle, please visit the ico. website <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

Appendix Two Personal Data

- The UK GDPR applies to the processing of personal data that is:
 - wholly or partly by automated means; or
 - the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
 - can be identified or who are identifiable, directly from the information in question; or
 - who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive, and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- **If personal data can be truly anonymised, then the anonymised data is not subject to the UK GDPR.** It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.
- **Information about companies or public authorities is not personal data.**
- However, information about individuals acting as sole traders, employees, partners, and company directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

What are identifiers and related factors?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.
- The UK GDPR provides a non-exhaustive list of identifiers, including:
 - name
 - identification number
 - location data; and
 - an online identifier
- 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.
- Other factors can identify an individual.

Can we identify an individual directly from the information we have?

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

Can we identify an individual indirectly from the information we have (together with other available information)?

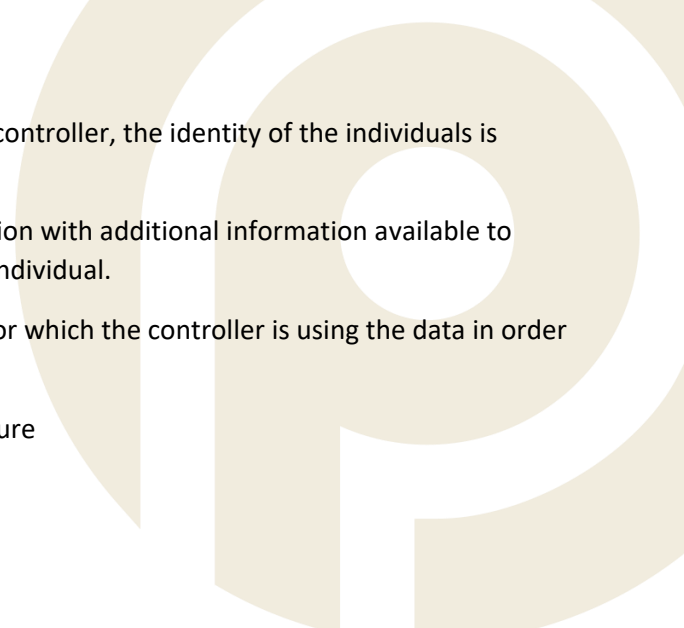
- It is important to be aware that information you hold may indirectly identify an individual and therefore could constitute personal data.
- Even if you may need additional information to be able to identify someone, they may still be identifiable.
- That additional information may be information you already hold, or it may be information that you need to obtain from another source.
- In some circumstances there may be a slight hypothetical possibility that someone might be able to reconstruct the data in such a way that identifies the individual. However, this is not necessarily sufficient to make the individual identifiable in terms of UK GDPR. You must consider all the factors at stake.
- When considering whether individuals can be identified, you may have to assess the means that could be used by an interested and sufficiently determined person.
- You have a continuing obligation to consider whether the likelihood of identification has changed over time (for example as a result of technological developments).

What is the meaning of 'relates to'?

- Information must 'relate to' the identifiable individual to be personal data.
- This means that it does more than simply identifying them – it must concern the individual in some way.
- To decide whether or not data relates to an individual, you may need to consider:
 - the content of the data – is it directly about the individual or their activities?
 - the purpose you will process the data for; and
 - the results of or effects on the individual from processing the data.
- Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.
- There will be circumstances where it may be difficult to determine whether data is personal data. If this is the case, as a matter of good practice, you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.
- Inaccurate information may still be personal data if it relates to an identifiable individual.

What happens when different organisations process the same data for different purposes?

- It is possible that although data does not relate to an identifiable individual for one controller, in the hands of another controller it does.

- 
- This is particularly the case where, for the purposes of one controller, the identity of the individuals is irrelevant, and the data therefore does not relate to them.
 - However, when used for a different purpose, or in conjunction with additional information available to another controller, the data does relate to the identifiable individual.
 - It is therefore necessary to carefully consider the purpose for which the controller is using the data in order to decide whether it relates to an individual.
 - You should take care when you make an analysis of this nature