Key definitions

What is personal data?

ico.

Information Commissioner's Office

About this detailed guidance

These pages sit alongside our [Guide to the GDPR](#) and provide more detailed guidance for UK organisations on the definition of personal data under the GDPR.

This guidance will help you to understand when you are processing personal data and when your obligations to comply with the provisions of the GDPR apply.

In addition, it will help you to allow individuals to exercise their rights with regard to their personal data by assisting you in correctly identifying the personal data you are processing.

For an introduction to the key themes and provisions of the GDPR, you should refer back to the Guide to the GDPR. You can navigate back to the guide at any time using the link at the top of this page. Links to other relevant guidance and sources of further information are also provided throughout.

When downloading this guidance, the corresponding content from the Guide to the GDPR will also be included so you will have all the relevant information on this topic.

What is personal data?

In detail

What does the GDPR say?

Personal data is defined in the GDPR as:

> 66
>
> "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

This means personal data has to be information that relates to an individual. That individual must be identified either directly or indirectly from one or more identifiers or from factors specific to the individual.

The GDPR covers the processing of personal data in two ways:

- personal data processed wholly or partly by automated means (that is, information in electronic form); and
- personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

In most circumstances, it will be relatively straightforward to determine whether the information you process 'relates to' an 'identified' or an 'identifiable' individual. In others, it may be less clear and you will need to carefully consider the information you hold to determine whether it is personal data and whether the GDPR applies.

This guidance will explain the factors that you should consider to determine whether you are processing personal data. These are:

- identifiability and related factors;
- whether someone is directly identifiable;
- whether someone is indirectly identifiable;
- the meaning of 'relates to'; and
- when different organisations are using the same data for different purposes.

Further Reading

Relevant provisions in the GDPR - See Articles 2(1), 4(1) and Recitals 15, 26 and 30 ☑
External link

Are there categories of personal data?

Some of the personal data you process can be more sensitive in nature and therefore requires a higher level of protection. The GDPR refers to the processing of these data as 'special categories of personal data'. This means personal data about an individual's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

> **In more detail – ICO guidance**
>
> For more information please see our guidance on special category data and criminal offence data.

Further Reading

Relevant provisions in the GDPR - See Articles 9(1), 9(2) and 10 Recital 34, 35 and 51-54 ↗
External link

What about unstructured paper records?

The GDPR does not cover information which is not, or is not intended to be, part of a 'filing system'. However, under the Data Protection Act 2018 (DPA 2018) unstructured manual information processed only by public authorities constitutes personal data. This includes paper records that are not held as part of a filing system. While such information is personal data under the DPA 2018, it is exempted from most of the principles and obligations in the GDPR and is aimed at ensuring that it is appropriately protected for requests under the Freedom of Information Act 2000.

We intend to publish further guidance on the provisions of the DPA 2018 in due course.

Is pseudonymised data still personal data?

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.

The GDPR defines pseudonymisation as:

> 66
>
> "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to ensure that this additional information is held separately.

Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations.

However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data. Recital 26 makes it clear that pseudonymised personal data remains personal data and within the scope of the GDPR.

> 66
>
> "…Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person…"

Example

A courier firm processes personal data about its drivers' mileage, journeys and driving frequency. It holds this personal data for two purposes:

- to process expenses claims for mileage; and
- to charge their customers for the service.

For both of these, identifying the individual couriers is crucial.

However, a second team within the organisation also uses the data to optimise the efficiency of the courier fleet. For this, the identification of the individual is unnecessary.

Therefore, the firm ensures that the second team can only access the data in a form that makes it not possible to identify the individual couriers. It pseudonymises this data by replacing identifiers (names, job titles, location data and driving history) with a non-identifying equivalent such as a reference number which, on its own, has no meaning.

The members of this second team can only access this pseudonymised information.

Whilst the second team cannot identify any individual, the organisation itself can, as the controller, link that material back to the identified individuals.

This represents good practice under the GDPR.

Further Reading

What about anonymised data?

The GDPR does not apply to personal data that has been anonymised. Recital 26 explains that:

> 66
>
> "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

This means that personal data that has been anonymised is not subject to the GDPR. Anonymisation can therefore be a method of limiting your risk and a benefit to data subjects too. Anonymising data wherever possible is therefore encouraged.

However, you should exercise caution when attempting to anonymise personal data. Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. You should therefore ensure that any treatments or approaches you take truly anonymise personal data. There is a clear risk that you may disregard the terms of the GDPR in the mistaken belief that you are not processing personal data.

In order to be truly anonymised under the GDPR, you must strip personal data of sufficient elements that mean the individual can no longer be identified. However, if you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised. This means that despite your attempt at anonymisation you will continue to be processing personal data.

You should also note that when you do anonymise personal data, you are still processing the data at that point.

Further Reading

Relevant provisions in the GDPR - Recital 26 ⤤

External link

Is information about deceased individuals personal data?

The GDPR only applies to information which relates to an identifiable living individual. Information relating to a deceased person does not constitute personal data and therefore is not subject to the GDPR.

Further Reading

Relevant provisions in the GDPR - Recital 27 ⤤

External link

What about information about companies?

Information concerning a 'legal' rather than a 'natural' person is not personal data. Consequently, information about a limited company or another legal entity, which might have a legal personality separate to its owners or directors, does not constitute personal data and does not fall within the scope of the GDPR. Similarly, information about a public authority is not personal data.

However, the GDPR does apply to personal data relating to individuals acting as sole traders, employees, partners, and company directors wherever they are individually identifiable and the information relates to them as an individual rather than as the representative of a legal person. A name and a corporate email address clearly relates to a particular individual and is therefore personal data. However, the content of any email using those details will not automatically be personal data unless it includes information which reveals something about that individual, or has an impact on them (see the chapters on the meaning of 'relates to' and indirectly identifying individuals, below).

What are identifiers and related factors?

In detail

What is identifiability?

If you can distinguish an individual from other individuals, then that person is 'identified' or is 'identifiable'. Often an individual's name together with some other information will be sufficient to identify them.

A name is perhaps the most common means of identifying someone. However, whether any potential identifier, including a name, actually identifies an individual depends on the context.

By itself, the name 'John Smith' may not always be personal data because there are many individuals with that name. However, if the name is combined with other information (such as an address, a place of work, or a telephone number) this is often sufficient to clearly identify one individual.

Example

'John Smith, who works at the Post Office in Wilmslow.'

This may normally be enough information to directly identify an individual. However, if it is a common name and there is more than one John Smith who work at this organisation, you would need further details to directly identify them, such as:

'John Smith with blonde hair and green eyes with a tattoo on his right arm, who works at the Post Office in Wilmslow.'

This additional information helps to single out that particular individual.

What information can be an identifier?

The GDPR provides a non-exhaustive list of common identifiers that, when used, may allow the identification of the individual to whom the information in question may relate. These identifiers include:

- name;
- identification number;
- location data; and
- an online identifier.

What are online identifiers?

The GDPR specifically includes the term 'online identifiers' within the definition of what constitutes personal data.

These may include information relating to the device that an individual is using, applications, tools or protocols. A non-exhaustive list is included in Recital 30:

- internet protocol (IP) addresses;
- cookie identifiers; and
- other identifiers such as radio frequency identification (RFID) tags.

Other examples of online identifiers that may be personal data include:

- MAC addresses;
- advertising IDs;
- pixel tags;
- account handles; and
- device fingerprints.

The use of these may leave traces which, when combined with unique identifiers and other information received by servers, may be used to create profiles of individuals and identify them.

When assessing if an individual is identifiable, you must consider whether online identifiers, on their own or in combination with other information that may be available to those processing the data, may be used to distinguish one user from another, possibly by the creation of profiles of the individuals to identify them.

This may be either as a named individual or simply as a unique user of electronic communications and other internet services who may be distinguished from other users.

Example

Using cookies or similar technologies to track an individual across websites involves the processing of personal data if this tracking involves online identifiers that are used to create a profile of the individual.

Example

Using facial recognition for the purpose of uniquely identifying an individual involves processing special categories of personal data.

In this context, facial recognition techniques record the unique features of an individual's face in order to distinguish one person from another. This is then linked to a specific individual and stored for reference for future comparison in identification, authentication and/or verification.

Example

An individual's social media 'handle' or username, which may seem anonymous or nonsensical, is still sufficient to identify them as it uniquely identifies that individual. The username is personal data if it distinguishes one individual from another regardless of whether it is possible to link the 'online' identity with a 'real world' named individual.

What else can identify an individual?

The GDPR makes it clear that other factors can identify an individual. These include:

> "
>
> "…one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

These sorts of characteristics can help to uniquely identify a particular individual as they tell you something about them.

What if we are still unsure if information is personal data?

There will be circumstances where it remains uncertain whether particular data is personal data. If this is the case we consider that, as a matter of good practice, you should still treat the information collected as though it is personal data. You still need to protect information because of the risk that otherwise someone may, with greater or lesser certainty, be able to infer something about a particular individual. For example if it was published and combined with information held by other organisations. In some cases the information will be personal data and the GDPR will apply to it. In particular you should:

- keep the information secure;
- protect it from inappropriate disclosure;
- be open about how you are collecting the information ; and
- ensure that you are justified in any processing.

Further Reading

🔗 **Relevant provisions in the GDPR - Article 4(1) and Recitals 26 and 30** 🔗
External link

Further reading

Article 29 Working Party Opinion 4/2007 on the concept of personal data WP136

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

In detail

How do we directly identify someone?

If you are able to identify an individual solely from the information that you are processing, the information may be personal data. In some instances, it will be clear that an individual is directly identifiable.

Example

It will be obvious that an individual is directly identifiable, for example if you hold their name and address.

Mr Isaac Wright
Information Avenue
Nowhere
DP9 8UK

A corporate email address can directly identify the individual (as it is a unique identifier), as well as providing further information about the individual (ie where they work).

Example

johnsmith@example.com

From this, you can learn that an individual named John Smith works at the company 'Example'.

What if we don't know the individual's name?

You do not need to hold an individual's name in order to identify them. If you hold any identifier, or combination of identifiers, this can be sufficient to identify a single individual. An individual is also identifiable if you are able to distinguish that individual from other members of a group.

Example

The elderly man who lives at number 15 Purple Street and drives a Porsche Cayenne.

Example

A description of an individual may be personal data if it is processed in connection with a neighbourhood watch scheme, for the purpose of identifying an individual as a potential witness to an incident.

Example

Megan Smith's foster mum, from Year 4 at Broomfield Junior School.

Further Reading

📑 [Relevant provisions in the GDPR - Article 4(1) and Recital 26](#) ⧉
External link

Further reading

[Article 29 Working Party Opinion 4/2007 on the concept of personal data WP136](#)

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

In detail

How do we identify someone indirectly?

It's important to be aware that information you hold may indirectly identify an individual and therefore can still be personal data. If so, this means that the information is subject to the GDPR.

If you cannot identify an individual directly from the information that you are processing (for example where all identifiers have been removed) an individual may still be identifiable by other means. This may be from information you already hold, or information that you need to obtain from another source. Similarly, a third party could use information you process and combine it with other information available to them.

You must carefully consider all of the means that any party is reasonably likely to use to identify that individual. This is important because you could inadvertently release or disclose information that could be linked with other information and (inappropriately) identify an individual.

What kind of information could allow an individual to be indirectly identified?

The following is a non-exhaustive list of information that could constitute personal data on the basis that it allows for an individual to be singled out from others:

- car registration number and/or VIN;
- national insurance number;
- passport number; or
- a combination of significant criteria (eg age, occupation, place of residence).

The key point of indirect identifiability is when information is combined with other information that then distinguishes and allows for the identification of an individual.

Example

A vehicle's registration number can be linked to other information held about the registration (eg by the DVLA) to indirectly identify the owner of that vehicle.

Example

If an individual is not known to the operators of an out-of-town shopping centre CCTV system, but they are able to distinguish that individual on the basis of physical characteristics, that individual is identified. Therefore, if the operators are tracking a particular individual that they have singled out in some way (perhaps using such physical characteristics) they will be processing 'personal data'.

Can we identify someone from other information we hold?

You may process information that, by itself, does not permit the direct identification of an individual. However, within your organisation you may also process other information that, when combined, allows a particular individual to be indirectly identified. If the information relates to that identified individual it constitutes personal data. It's important to recognise this, so that you can comply with your obligations under the GDPR.

Example

An individual submits an application for a job.

On receiving the application, the organisation's HR department removes the first page, which contains the individual's name, contact details, etc and saves the remainder of the form in 'Folder 1'. The application form is saved with a randomly generated application number and sent on to the recruiting manager.

In a restricted-access folder, 'Folder 2', the HR department stores the first page of the application, alongside the application number.

The information in Folder 1 does not allow for the identification of any individual. However, when it is combined with the information in Folder 2, the applicant can be identified.

Example

A business uses Wi-Fi analytics data to count the number of visitors per hour across different retail outlets. It is not necessary to know whether an individual has visited an individual store (or multiple stores) before.

This involves the business processing the Media Access Control (MAC) addresses of mobile devices that broadcast probe requests to its public Wi-Fi hotspots. MAC addresses are intended to be unique to the device (although they can be modified or spoofed using software).

If an individual can be identified from that MAC address, or other information in the possession of the network operator (the business, in this example), then the data is personal data. Additionally, even if the business does not know the name of the individual, using a MAC address (or other unique identifier) to track a device with the purpose of singling out that individual or treating them

differently means the data is also personal data.

Can we or someone else identify an individual from information we hold and they hold?

Sometimes, whether someone can be identified may depend on who may have access to the information and any other information that can be combined with it.

It's important to be aware that you may hold information, which when combined with other information held outside of your organisation, could lead to an individual being indirectly identified or identifiable.

Example

An online platform release statistical data sets about the use of its services for research purposes. This information does not contain the names of the services users, but instead profile data showing usage patterns. However, a number of those individuals have made public comments about their use of the platform. The information released by the platform can be matched to the public comments to identify those individuals.

Example

A public authority releases information about complaints in response to a request under Freedom of Information Act 2000. It does not reveal the names or addresses of the complainants, but other information is in the public domain that can easily be used to match the identity of those complainants.

If there is only a very slight possibility that an individual could be indirectly identified, is it still personal data?

Sometimes it is not immediately obvious whether an individual can be identified or not, for example, when someone holds information where the names and other identifiers have been removed or where you process a 'non-obvious' identifier. In these cases, Recital 26 of the GDPR states that, to determine whether or not the individual is identifiable you should take into account 'all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly'.

Therefore, the fact that there is a very slight hypothetical possibility that someone might be able to reconstruct the data in such a way that the individual is identified is not necessarily sufficient to make the individual identifiable. You must consider all the factors at stake.

What factors should we consider when assessing the possibility of identification?

You should consider what means are reasonably likely to be used to identify the individual taking into account all objective factors, such as:

- the costs and amount of time required for identification;
- the available technology at the time of the processing; and
- likely technological developments.

You should also document this assessment.

Your starting point might be to look at what means are available to identify an individual and the extent to which these are readily available. For example, if searching a public register or reverse directory would enable you to identify an individual from an address or telephone number, and you are likely to use this resource for this purpose, you should consider that the address or telephone number data is capable of identifying an individual.

You should assume that you are not looking just at the means reasonably likely to be used by an ordinary person, but also by a determined person with a particular reason to want to identify individuals. For example, investigative journalists, estranged partners, stalkers, or industrial spies.

Means of identifying individuals that are feasible and cost-effective, and are therefore likely to be used, will change over time. If you decide that the data you hold does not allow the identification of individuals, you should review that decision regularly in light of new technology or security developments or changes to the public availability of certain records.

The measures reasonably likely to be taken to identify an individual may vary depending upon the perceived value of the information. For example, if the information is thought to be about a high profile public figure, it is likely that there will be some who are willing to use extreme measures to identify that individual.

Further Reading

> ↗ **Relevant provisions in the GDPR - Article 4(1) and Recital 26 and 30** ↗
> External link

Further reading

We are working to update existing Data Protection Act 1998 guidance to reflect GDPR provisions. In the meantime, this existing guidance is a good starting point:

Anonymisation

Wi-Fi Location analytics

What is the meaning of 'relates to'?

In detail

Does the data 'relate to' an identifiable data subject?

It will often be clear where data 'relates to' a particular individual. However, sometimes this is not so clear and it may be helpful to consider in more detail what 'relates to' means.

Data which identifies an individual, even without a name associated with it, may be personal data if you are processing it to learn or record something about that individual, or where the processing has an impact on that individual. Therefore, data may 'relate to' an individual in several different ways, the most common of which are considered in this section.

Is the content about an individual?

Information may be obviously about a particular individual or about their activities. This information is personal data regardless of the purpose for which you are processing the data.

In many cases data may be personal data simply because its content is 'obviously about' an individual. Alternatively, data may be personal data because it is clearly 'linked to' an individual as it is about his or her activities and you are processing it for the purpose of determining or influencing the way in which that individual is treated. Data may also be personal data if it is biographically significant or has a particular individual as the focus.

There are many examples of data that 'relates to' an individual because the content of the information is clearly about that individual. For example:

- medical history;
- criminal record;
- a record of an individual's performance at work; or
- a record of an individual's sporting achievements.

There are also many examples of records which will clearly be personal data where the content of the information is about their activities not about the individual themselves. For example:

- personal bank statements; or
- itemised telephone bills.

There will also be many cases where data is not in itself personal data but, in certain circumstances, it will become personal data where it can be linked to an individual to provide particular information about that individual.

Example

If data about a job salary is included in a vacancy advertisement, it will not, in those circumstances,

be personal data. However, if the same salary details are linked to a name (for example, when the vacancy has been filled and there is a single named individual in post), the salary information about the job is personal data 'relating to' that employee.

Example

An organisation has a number of employees with the same job title. This constitutes personal data when a particular individual can be identified from the job title information and additional information.

Does the purpose of the processing make information personal data?

If the data is used, or is likely to be used, to learn, evaluate, treat in a certain way, make a decision about, or influence the status or behaviour of an individual, then it is personal data.

Example

A company uses call logs from a desk phone to help identify when the person who sits at that desk was in the office.

Whilst the fact that a telephone was in use is not necessarily information relating to an individual in its own right, when associated with the individual who is allocated to that desk and used to assess performance, it is clearly information which relates to an identifiable individual.

There are many other examples of data which 'relate to' a particular individual because it is linked to that individual and informs or influences actions or decisions which affect an individual.

For example, an individual's data about their phone or electricity account clearly determines what the individual will be charged. However, data about a house is not, by itself, personal data.

Context is important here. Information about a house is often linked to an owner or resident and consequently the data about the house will be personal data about that individual.

Example

Information about the market value of a particular house may be used for statistical purposes to identify trends in the house values in a geographical area. The house is not selected because the data controller wishes to know anything about the occupants, but because it is a four bedroom detached house in a medium-sized town. As soon as data about a house is either:

- linked to a particular individual, for example, to provide particular information about that individual (for example, his address); or

- used in deliberations and decisions concerning an individual (even without a link to the individual's name, for example, the amount of electricity used at the house is used to determine the bill the individual householder is required to pay),

then that data will be personal data.

Example

An individual carries out unauthorised alterations to their house. The data about the unauthorised alterations is processed by reference to the house address. However, if the data is processed in order to decide whether to prosecute the house owner, the date clearly relates to the individual who carried out alterations.

Example

The value of a house is used to determine an individual's liability for Council Tax, or to determine their assets or in proceedings following divorce. This is then personal data because the data about the house is clearly linked to the individual or individuals concerned.

Does the data impact, or have the potential to impact, on an individual?

If data is occasionally processed to learn something about an individual, even though it was not the controller's primarily purpose for processing the data, this data will be personal data as the processing does, or is likely to, impact on the individual (see next question, below).

Example

A biscuit factory records information about the operation of a piece of machinery. If the information is recorded to monitor the efficiency of the machine, it is unlikely to be personal data.

However, if the information is recorded to monitor the productivity of the employee who operates the machine (and his annual bonus depends on achieving a certain level of productivity), the information will be personal data about the individual employee who operates it.

When considering data about objects, if the data is processed to provide information about an individual

(for example, productivity) then the data is personal data. If the data about objects is not currently processed to provide information about an individual, but could be, then the data is likely to be personal data.

It depends on whether the processing of the information has or could have a resulting impact upon the individual even though the content of the data is not directly about that individual, nor is there any intention to process the data for the purpose of determining or influencing the way that person is treated.

Is data that refers to an identifiable individual, but does not relate to them, personal data?

Data can contain references to an identifiable individual, or be linked to them, but not 'relate to' them as it is not about that individual but is about another topic entirely. Depending on the circumstances, this data may or may not be personal data.

Example

Emails written by a lawyer to their client about their client's matter all contain references to the lawyer's name and place of work, which will be the lawyer's personal data. However, the content of the emails are not about the individual lawyer, but about the client's instructions. The content of the email is not, therefore, personal data where it concerns legal advice about the client's legal query.

If a complaint was then made about the lawyer's performance or advice and the emails were then used to investigate this, the legal advice given in them would become personal data.

Is inaccurate information about an individual still personal data?

If information seemingly relating to a particular individual is inaccurate (ie it is factually incorrect or it is information about a different individual), the information is still personal data, as it relates to that individual.

Example

Two people live in an apartment block who wear glasses. John lives on the ground floor and William lives on the top floor.

The landlord receives a complaint that the man wearing glasses who lives on the ground floor has engaged in anti-social behaviour. However, the complaint actually relates to activity conducted by William, who lives on the top floor.

The landlord records the information about the anti-social behaviour relating to John. This is inaccurate information but it is nevertheless personal data relating to John, which the landlord should correct if required to do so.

At the same time, this is also personal data about William, even though it's been recorded about

John.

If the information is inaccurate so that no individual can be identified from that information on its own or in conjunction with additional information, then the information is not personal data.

Example

The landlord then receives a further complaint that a tenant with a dachshund is also engaging in the anti-social behaviour.

There is nobody with a dachshund living in the apartments and, in fact, no tenants own a dog. This information does not relate to an identifiable data subject. This information is therefore not personal data.

An opinion relating to an individual is also capable of constituting personal data, irrespective of the accuracy of that opinion.

Further Reading

🔗 Relevant provisions in the GDPR - See Articles 5(1)(d) and Articles 16 and 19 🔗
External link

Further reading

See the following sections of The Guide to the GDPR:

Principles

Right to rectification

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

In detail

The same piece of data may be personal data in the hands of one organisation, while it may not be personal data in another organisation's hands. This depends on the purpose the organisation is processing the information for.

Example

A journalist takes a photograph of the beach on a sunny day to publish in a local newspaper alongside a story about record-breaking temperatures. The photograph includes some individuals who are relaxing on the beach and is of sufficient quality that some of the individuals may be identifiable.

The journalist is not processing the photograph to learn anything about any of the individuals whose images were captured, nor is it likely that the journalist would ever process the photograph for that purpose. Whilst processed by the photographer, the photograph would not be personal data as it is not used to record, learn or decide something about the individuals.

One of the individuals photographed on the beach had told their employer they needed to attend a funeral and had taken compassionate leave from work on that day.

Their colleague sees the photograph published in the newspaper, scans a copy and e-mails it to the manager of the individual photographed. The photograph is added to the individual's personnel file in order to start disciplinary proceedings for taking compassionate leave under false pretences.

When being processed by the individual's employer, the photograph is being used to record, learn or decide something about the individual. For this reason, it would be personal data when processed by the employer.

It is therefore necessary to consider carefully the purpose for which the controller is using the data in order to decide whether it relates to an individual.