Lawful basis for processing

Special category data

ico.
Information Commissioner's Office

About this detailed guidance

This guidance discusses special category data in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding of the conditions for processing special category data to help you comply in practice. It is aimed at DPOs and those with specific data protection responsibilities in larger organisations.

If you haven't yet read the 'in brief' page on special category data in the Guide to Data Protection, you should read that first. It introduces the topic and sets out the key points you need to know, along with practical checklists to help you comply.

What is special category data?

What are the rules on special category data?

What are the conditions for processing?

- (h) Health or social care
- (i) Public health
- (j) Archiving, research and statistics

What are the substantial public interest conditions?

- What substantial public interest conditions are available?
- How do the substantial public interest conditions work?
- What are 'reasons of substantial public interest'?
- What is the role of consent?
- What is an appropriate policy document?

What is special category data?

In detail

What are the 'special categories of personal data'?

The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- 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**.

In this guidance we refer to this as 'special category data'.

The majority of the special categories are not defined and are fairly self-explanatory. However specific definitions are provided for genetic data, biometric data and health data.

Further Reading

> Key provisions in the legislation - See Article 9(1) and Recital 51
> External link

Why is this data special?

It's not just that this type of information might be seen as more sensitive or 'private'. The recitals to the GDPR explain that these types of personal data merit specific protection. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms. For example, the various categories are closely linked with:

- freedom of thought, conscience and religion;
- freedom of expression;
- freedom of assembly and association;
- the right to bodily integrity;
- the right to respect for private and family life; or
- freedom from discrimination.

The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination. This is part of the risk-based approach of the GDPR.

Whilst other data may also be sensitive, such as an individual's financial data, this does not raise the same fundamental issues and so does not constitute special category data for the purposes of the GDPR. And while data about criminal allegations or convictions may raise some similar issues, it does not constitute special category data as it is covered by separate rules. However, you always need to ensure that when you are processing other types of data, it is fair and meets other GDPR requirements (including the separate rules on criminal offence data).

These special categories of personal data are framed broadly and may also catch information that is not seen as particularly sensitive. For example, details about an individual's mental health are likely to be much more sensitive than whether they have a broken leg – but both are data concerning health. Given the potential risks to fundamental rights, it is important that you identify any special category data and approach it carefully, even if you don't think it is particularly sensitive.

Further Reading

> Key provisions in the legislation - See Recital 51
> External link

What is genetic data?

The GDPR defines genetic data in Article 4(13):

> "'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question".

Recital 34 says this includes chromosomal, DNA or RNA analysis, or any other type of analysis that enables you to obtain equivalent information. (Ribonucleic acid (RNA) plays an essential part in the coding, decoding, regulation and expression of genes).

Not all genetic information constitutes genetic data. The first question is always whether the genetic

information is personal data. A genetic sample itself is not personal data until you analyse it to produce some data. And genetic analysis data is only personal data (and so genetic data) if you can link it back to an identifiable individual.

In most cases, you process genetic information to learn something about a specific identified individual and to inform you about taking some action in relation to them. This is clearly personal data – and special category genetic data - for the purposes of the GDPR.

However, the definition of personal data also includes identification by reference to "one or more factors specific to the genetic identity of that natural person", even without their name or other identifier. So, in practice, genetic analysis which includes enough genetic markers to be unique to an individual is personal data and special category genetic data, even if you have removed other names or identifiers. And any genetic test results which are linked to a specific biological sample are usually personal data, even if the results themselves are not unique to the individual, because the sample is by its nature specific to an individual and provides the link back to their specific genetic identity.

However, there are cases where genetic information is not identifiable personal data. For example, where you have anonymised or aggregated partial genetic sequences or genetic test results (eg for statistical or research purposes), and they can no longer be linked back to a specific genetic identity, sample or profile; a patient record; or to any other identifier.

Further Reading

Key provisions in the GDPR - See Articles 4(1) and 4(13) and Recital 34
External link

Further reading – ICO guidance

What is personal data?

Further reading – European Data Protection Board (EDPB)

The EDPB, which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR. The EDPB has not yet adopted guidelines on genetic data under the GDPR, but you may find it useful to read the 2004 WP29 working document on genetic data (WP91) and WP29 Opinion 6/2000 on the Genome issue (WP35).

What is biometric data?

Article 9(1) includes in the list of special categories of data:

> “biometric data for the purpose of uniquely identifying a natural person”.

The 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 dactyloscopic data”.

The term ‘dactyloscopic data’ means fingerprint data.

Example

A gym introduces an electronic fingerprint scanning system. Members scan their fingerprint in order to get through the entrance turnstiles. This system is processing biometric data to identify individual members, so the gym needs a valid condition for processing that special category data.

Example

A school introduces an electronic fingerprint scanning system to charge students for their school meals. This system is processing biometric data to identify the individual students, so the school needs a valid condition for processing that special category data.

Facial imaging and fingerprint data are just two examples, but these are not exhaustive. Many other types of physical, physiological or behavioural ‘fingerprinting’ fall within the definition.

Examples of physical or physiological biometric identification techniques:

- facial recognition;
- fingerprint verification;
- iris scanning;
- retinal analysis;
- voice recognition; and
- ear shape recognition.

Examples of behavioural biometric identification techniques:

- keystroke analysis;
- handwritten signature analysis;
- gait analysis; and
- gaze analysis (eye tracking).

If you process digital photographs of individuals, this is not automatically biometric data even if you use it for identification purposes. Although a digital image may allow for identification using physical characteristics, it only becomes biometric data if you carry out "specific technical processing". Usually this involves using the image data to create an individual digital template or profile, which in turn you use for automated image matching and identification.

All biometric data is personal data, as it allows or confirms the identification of an individual. Biometric data is also special category data whenever you process it "for the purpose of uniquely identifying a natural person". This means that biometric data will be special category data in the vast majority of cases. If you use biometrics to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, you need to comply with Article 9.

Further Reading

Key provisions in the GDPR - See Articles 9(1) and 4(14), and Recital 51
External link

In more detail

We are planning to produce more detailed ICO guidance on processing biometric data.

We have published an Opinion on the use of live facial recognition technology by law enforcement in public places following the High Court judgment R (Bridges) v Chief Constable of South Wales Police & others [2019] EWHC 2341 (Admin).

The EDPB has not yet adopted guidelines on biometrics under the GDPR, but you may find it useful to read WP29 Opinion 03/2012 on developments in biometric technologies (WP 193) and WP29 Opinion 02/2012 on facial recognition in online and mobile services (WP 192).

What is health data?

The GDPR defines health data in Article 4(15):

> "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

Health data can be about an individual's past, current or future health status. It not only covers specific details of medical conditions, tests or treatment, but includes any related data which reveals anything about the state of someone's health.

Health data can therefore include a wide range of personal data, for example:

- any information on injury, disease, disability or disease risk, including medical history, medical opinions, diagnosis and clinical treatment;
- medical examination data, test results, data from medical devices, or data from fitness trackers;
- information collected from the individual when they register for health services or access treatment;
- appointment details, reminders and invoices which tell you something about the health of the individual. These fall under 'the provision of health care services' but must reveal something about a person's health status. For example, a GP or hospital appointment in isolation will not tell you anything about a person's health as it may be a check-up or screening appointment. However, you could reasonably infer health data from an individual's list of appointments at an osteopath clinic or from an invoice for a series of physiotherapy sessions; and
- a number, symbol or other identifier assigned to an individual to uniquely identify them for health purposes (eg an NHS number, or Community Health Index (CHI) number in Scotland), if combined with information revealing something about the state of their health.

Further Reading

Key provisions in the GDPR - see Article 4(15) and Recital 35
External link

What about criminal offence data?

Personal data about criminal allegations, proceedings or convictions is not special category data. However, there are similar rules and safeguards for processing this type of data, to deal with the particular risks associated with it. For more information, see our separate guidance on criminal offence data.

What about inferences and educated guesses?

The GDPR is clear that special category data includes not only personal data that specifies relevant details, but also personal data **revealing** or **concerning** these details.

It may be possible to infer or guess details about someone which fall within the special categories of data. Whether or not this counts as special category data and triggers Article 9 depends on how certain that inference is, and whether you are deliberately drawing that inference.

If you can infer relevant information with a reasonable degree of certainty then it's likely to be special category data even if it's not a cast-iron certainty. But if it is just a possible inference or an 'educated guess', it is not special category data (unless you are specifically processing to treat someone differently on the basis of that inference) - even if that guess turns out to be right.

Example

A job applicant lists on their CV that they are a trustee of a charity that supports deaf people. Other individuals associated with the charity are themselves deaf – but being a trustee does not necessarily mean that the individual is deaf. The company processing personal data contained in the CV would not need a special category condition to process that data, even if the individual in fact is deaf or hard of hearing.

However, if the company has other information which confirms that the individual is deaf, it will then need a condition to process this special category data.

You can often infer an individual's religion or ethnicity with varying degrees of certainty from names or images. For example, many surnames are associated with a particular ethnicity or religion. However, it is inappropriate to treat all such names as special category data in every instance, as this would mean you need a special category condition just to hold such names on a customer database, which is not the case.

However, if you process such names specifically because they indicate ethnicity or religion, for example to target services on this basis, then you are processing special category data.

This is likely to be a particular issue if you undertake any form of profiling which infers, for example, ethnicity, beliefs, politics, health risks, sexual orientation or relationship status. If you intend to create such inferences, you are processing special category data irrespective of the level of statistical confidence. The key question here is not whether the inferences are correct, but whether you are using an inference linked to one of the special categories to influence your activities in any way.

You must also take extra care to ensure you are not processing inaccurate, inadequate or irrelevant personal data (in line with the accuracy principle), and that you only draw such inferences where they are directly relevant and necessary for your purpose (in line with the data minimisation principle).

If you are concerned that someone might be able to infer special category data even if it is not relevant to your purpose, you may want to identify a condition to cover that possibility, to minimise the privacy risks. However, there is nothing in the GDPR that says a condition for processing is required, just in case it turns out that an unintended potential inference is in fact correct.

If you think the data carries a risk of inferences that might be considered sensitive or private, even if this falls short of revealing something about one of the special categories with any level of certainty, then you should also carefully consider fairness issues and whether there is anything more you can do to minimise privacy risks.

Further reading – ICO guidance

Data minimisation principle (adequacy)

Accuracy principle

Further reading – European Data Protection Board (EDPB)

The EDPB has endorsed guidelines on automated individual decision making and profiling, which includes a section on profiling and creating special category data by inference.

What are the rules on special category data?

In detail

What does the GDPR say?

Article 9 prohibits the processing of special category data. There are 10 exceptions to this general prohibition, usually referred to as 'conditions for processing special category data':

(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)

Five of the conditions only apply if your processing has an authorisation or basis in EU or member state law. In the UK, this authorisation or basis in law is set out in the DPA 2018.

The GDPR also says that member states can add further specific conditions for genetic, biometric or health data (although the UK has not done so).

Article 22(4) says that you cannot use special category data for solely automated decision-making (including profiling) that has legal or similarly significant effects, unless you have explicit consent or meet the substantial public interest condition. You also need suitable measures in place to safeguard the data subject's rights, freedoms and legitimate interests.

Use of special category data, particularly on a large scale, can also affect your other obligations and in particular the need for documentation, DPIAs, DPOs and EU representatives. See below for what else you need to do.

Further Reading

Key provisions in the GDPR - See Article 9 and Recital 51
External link

See also Articles 22(4), 27(2), 30(5), 35(3), 37(1)
External link

What does the DPA 2018 say?

The DPA 2018 supplements and tailors the GDPR conditions for processing special category data.

Section 10 says that if you are relying on a GDPR condition which requires authorisation by law or a basis in law, you must meet one of the additional conditions in Schedule 1.

Section 11(1) applies to the health or social care condition, and clarifies when the requirement for a professional obligation of secrecy will be met under UK law.

Schedule 1 Part 1 contains the first four conditions, which give a specific basis in UK law for relying on specific Article 9 conditions:

1. employment, social security and social protection - Article 9(2)(b);
2. health or social care - Article 9(2)(h);
3. public health - Article 9(2)(i); and
4. archiving, research or statistics - Article 9(2)(j).

Schedule 1 Part 2 then specifies a further 23 potential 'substantial public interest' conditions for the purposes of Article 9(2)(g).

Schedule 1 (at paragraphs 5 and 38 to 41) also includes additional requirements for you to keep an appropriate policy document and records of processing in relation to special category data.

The DPA 2018 does not add any more specific conditions for genetic, biometric or health data, although there is the power for the Secretary of State to make regulations to add or amend conditions.

Further Reading

Key provisions in the DPA 2018 - See sections 10 and 11, and Schedule 1
External link

What is the combined effect of these rules?

You must always ensure that your processing is generally lawful, fair and transparent, and complies with all of the other principles and requirements of the GDPR.

Remember that in order for your processing to be lawful, you always need to identify an Article 6 basis for processing.

In addition, you can only process special category data if you can meet one of the conditions in Article 9 of the GDPR, together with any associated DPA Schedule 1 conditions where required. This table summarises when you need a Schedule 1 condition:

(a) explicit consent	-
(b) employment, social security and social protection	+ condition 1
(c) vital interests	-
(d) not-for-profit bodies	-
(e) manifestly made public	-
(f) legal claims or judicial acts	-
(g) substantial public interest	+ one of conditions 6 - 28
(h) health or social care	+ condition 2
(i) public health	+ condition 3
(j) archiving, research or archiving	+ condition 4

You need to be able to demonstrate that your processing meets the specific requirements of the relevant conditions. For more detail on each condition, see What are the conditions for processing?

If you plan to make solely automated decisions (including profiling) on the basis of special category data, the rules are stricter. If this might have a significant effect on the individual, you can only go ahead with either explicit consent, or a substantial public interest condition. You should also read our separate guidance on rights related to automated processing.

How do the conditions work?

First you need to be clear about why you need special category data, as most of the conditions are based on the specific purpose for the processing. You can then identify the most relevant condition.

Given the potential risks to individuals' rights, the conditions are narrowly drawn and often require you to meet detailed criteria and put in place specific safeguards and accountability measures. Some conditions are also limited to specific types of controllers, and some only apply to particular types of special category data.

For some of the conditions, you need to justify why you cannot give individuals a choice and get explicit consent for your processing. This is different to the separate rules on having a lawful basis for processing personal data, where there is no preference for consent. Given the risks to individuals, there is more emphasis on explicit consent for special category data. However, this justification is not required for all conditions, and even where it is required the law acknowledges there may be good reasons why you can't get valid consent in some cases.

If you're not sure which condition is appropriate, it can be useful to start by considering whether you could reasonably get explicit consent for your processing. However, consent won't always be appropriate, particularly in the public sector. If there are good reasons why consent won't work, you can then consider the other Article 9 conditions. You should focus on your purpose for processing, ensuring that the special category data is actually necessary for that purpose. If the only relevant condition is

substantial public interest, you should go on to consider the specific substantial public interest conditions in the DPA 2018.

If your purpose is not covered by any of the conditions, and you cannot obtain valid explicit consent, you cannot process the special category data. It doesn't matter how good your reason for processing might be. In practice, you need to change your plans to either avoid using special category data, or else obtain valid explicit consent.

The only potential exemption from Article 9 is the public interest exemption for journalism, academia, art or literature. There are no other exemptions from Article 9.

The ICO cannot authorise the use of special category data in the absence of a condition. Adding further conditions is a matter for government and would require new legislation.

What does 'necessary' mean?

Most of the conditions depend on you being able to demonstrate that the processing is 'necessary' for a specific purpose. This does not mean that processing has to be absolutely essential. However, it must be more than just useful or habitual. It must be a targeted and proportionate way of achieving that purpose.

The condition does not apply if you can reasonably achieve the same purpose by some other less intrusive means – and in particular if you could do so by using non-special category data. There is a link here to the data minimisation principle, which you should consider carefully for special category data.

It is not enough to argue that processing is necessary because it is part of your particular business model, processes or procedures, or because it is standard practice. The question is whether the processing of the special category data is a targeted and proportionate way of achieving the purpose described in the condition.

Further reading – ICO guidance

Data minimisation principle

How does this affect our lawful basis?

It doesn't. These conditions do not replace or override the usual rules on having a lawful basis for processing. Instead, they operate as an additional layer of conditions on top of the usual rules.

If you are processing special category data this means you must still identify a lawful basis for your processing, in exactly the same way as for any other personal data. In other words, you must identify both a lawful basis under Article 6 and a condition for processing special category data under Article 9.

However, if you are relying on legitimate interests as your lawful basis, you need to take into account the particular risks associated with special category data in your legitimate interests assessment. You may need to put in place more robust safeguards to mitigate any impact or risks to the individual to demonstrate that the legitimate interests basis applies.

Your choice of lawful basis under Article 6 does not dictate which condition you must apply, and vice versa. You can choose whichever condition best fits the circumstances, irrespective of your lawful basis.

Of course, in some cases there may be an obvious link between the lawful basis and a particular condition. For example if your lawful basis is vital interests, the special category condition for vital interests may well also be appropriate. And if your lawful basis is consent, it is likely to make sense to use explicit consent for special category data.

However, some of the lawful bases do not have a direct link with a particular condition, for example, contract or legitimate interests. This is because the conditions for special category data are designed to be more restrictive and specific. This does not mean that you will never have a condition – just that you need to look at all of them to see if you can identify one that fits the circumstances and justifies that element of your processing.

In particular, even if you are not using consent as your lawful basis for all the data, you can still consider explicit consent as your condition for processing any special category data.

Further Reading

> Key provisions in the GDPR See Article 6
> External link

Further reading – ICO guidance

Lawful basis for processing
Legitimate interests
Consent

Do we need to do a DPIA?

You must do a data protection impact assessment (DPIA) for any type of processing which is likely to be high risk. This means you are more likely to need to do a DPIA for special category data, and be aware of the likely risks.

In particular, you must carry out a DPIA if you plan to process special category data:

- on a large scale;
- to determine access to a product, service, opportunity or benefit; or
- which includes genetic or biometric data (if in combination with any other criteria in European DPIA guidelines).

If in doubt, we recommend you carry out a DPIA. This will make it easier to ensure you have appropriate safeguards in place and can demonstrate your compliance.

Further reading

ICO guidance on DPIAs
European guidelines on DPIAs

What else do we need to do?

You must always ensure that your processing is generally lawful, fair and transparent, and complies with all the other principles and requirements of the GDPR. Be aware that the particular risks associated with special category data might affect what is considered fair, or what you need to do to comply.

In particular, you may need to consider:

- **Data minimisation:** it is particularly important to make sure you collect and retain only the minimum amount of special category data - and can justify why you need this specific type of data.
- **Security measures:** one of the considerations for determining the appropriate level of security is the sensitivity of the personal data. You may need to consider whether you need additional security measures for special category data.
- **Transparency:** you need to include information about categories of data in your privacy notice and other privacy information for individuals. If you are processing special category data, you should make this clear and specify which categories of data. You don't have to say which condition you are relying on.
- **Rights related to automated decision-making:** if you are carrying out automated decision-making (including profiling) using special category data and this might have a 'legal or similarly significant effect' on the individual, you can only go ahead if you get the individual's explicit consent, or if you identify a substantial public interest condition.
- **Documentation:** if you process special category data you must keep records, including documenting the categories of data. You must also identify whether you need an 'appropriate policy document' under the DPA 2018. If so, your general documentation must include your condition for processing the data, how you satisfy a lawful basis for that processing, and specific details about whether you have followed your retention and deletion policies – and if not, why not.
- **Data Protection Officer (DPO):** you must appoint a DPO if your core activities (in other words, your primary business objectives) require large scale processing of special category data.
- **EU representative:** if you are not established in the EU but you offer services to, or monitor, individuals in the UK or other EU member states, and you process special category data on a large scale, you need to designate a representative in the EU. You may need a representative even for occasional small-scale processing of special category data, unless you can show that it is low risk. You may also need to seek your own legal advice on the law in other relevant member states.

Further Reading

See GDPR Articles 5, 13, 14, 22(4), 27(2), 30(5), 32, 35(3), 37(1)
External link

See DPA 2018 section 10 and Schedule 1
External link

Further reading – ICO guidance

Lawfulness, fairness and transparency
Data minimisation
Security
Right to be informed
Rights related to automated decision-making including profiling

Documentation
Data protection officers

What are the conditions for processing?

In detail

(a) Explicit consent

Article 9(2)(a) permits you to process special category if:

> "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes".

'Explicit consent' is not defined in the GDPR, but must meet the usual GDPR standard for consent. In particular, it must be freely given, specific, affirmative (opt-in) and unambiguous, and able to be withdrawn at any time. In practice, the extra requirements for consent to be 'explicit' are likely to be:

- explicit consent must be confirmed in a clear statement (whether oral or written), rather than by any other type of affirmative action;
- it must specify the nature of the special category data; and
- it should be separate from any other consents you are seeking.

Explicit consent is the only condition that can apply to a wide range of circumstances, and in some cases may be your only option. If so, you need to make sure that you offer people genuine choice over whether and how you use their data.

You need to be particularly careful if you ask for consent as a condition of your services, or if you are in a position of power over the individual, for example, if you are a public authority or their employer.

If you need to process special category data to provide a service to the individual, explicit consent may be available as your condition for processing that data even if it is a condition of service. However, you must be confident that you can demonstrate consent is still freely given. In particular, that the

processing is actually objectively necessary to perform the contractual service, and not just included in your terms for broader business purposes.

Example

A gym introduces a facial recognition system to allow members access to the facilities. It requires all members to agree to facial recognition as a condition of entry – there is no other way to access the gym. This is not valid consent as the members are not being given a real choice – if they do not consent, they cannot access the gym. Although facial recognition might have some security and convenience benefits, it is not objectively necessary in order to provide access to gym facilities, so consent is not freely given.

However, if the gym provides an alternative, such as a choice between access via facial recognition and access via a membership card, consent could be considered freely given. The gym could rely on explicit consent for processing the biometric facial scans of the members who indicate that they prefer that option.

We have produced separate detailed guidance on how to obtain, record and manage valid consent, including explicit consent.

Further reading – ICO guidance

Consent

(b) Employment, social security and social protection law

Article 9(2)(b) permits you to process special category data if:

> "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".

The relevant legal authorisation is set out in the DPA 2018, in Schedule 1 condition 1. This condition also requires you to have an appropriate policy document in place.

This condition is particularly relevant for employers, for example where you are:

- checking if individuals are entitled to work in the UK;
- ensuring health, safety and welfare of employees;

- maintaining records of statutory sick pay and maternity pay; or
- deducting trade union subscriptions from payroll.

It also applies to public authorities involved in providing social services and benefits. Social security and social protection covers benefits, social support or other interventions designed to assist individuals with:

- sickness;
- maternity and paternity;
- invalidity or disability;
- old-age;
- death and survivorship;
- accidents at work or occupational diseases;
- unemployment;
- housing;
- family life and children; or
- other forms of social exclusion.

Your purpose must be to comply with employment law, or social security and social protection law. You need to be able to identify the legal obligation or right in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable employment obligations or rights.

If you are providing social care, or managing social care services, you may find that the condition for health or social care is more appropriate.

This condition does not cover processing to meet purely contractual employment rights or obligations.

You must be able to justify why processing of this specific data is 'necessary' - it must be a reasonable and proportionate way of meeting specific rights or obligations, and you must not have more data than you need.

Example

A coach company wants to undertake random drug and alcohol testing of its drivers. As an employer, it has a health and safety obligation to ensure that its drivers are not under the influence of alcohol or drugs while working. It relies on the employment, social security and social protection condition for this processing.

If the company widens the test to include those staff that don't have a safety-critical role, it will not be able to justify that the processing of these individuals' data is necessary.

(c) Vital interests

Article 9(2)(c) permits you to process special category data if:

> “processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent”.

You don’t need a DPA Schedule 1 condition to rely on vital interests or an appropriate policy document.

Recital 46 provides some further guidance:

> “The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person…”

Vital interests are intended to cover only interests that are essential for someone’s life. So this condition is very limited in its scope, and generally only applies to matters of life and death.

This condition only applies if the individual is physically or legally incapable of giving consent. This means you should ask for explicit consent if possible. If a data subject refuses consent, you cannot rely on vital interests as a fallback condition, unless they are not legally competent to make that decision.

This condition is likely to be most relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is unconscious or otherwise incapable of giving consent.

Example

A medical team in a hospital want to provide emergency care to an unconscious patient. They cannot obtain consent to process the individual’s medical records and so rely on the vital interests condition for processing.

Further reading – ICO guidance

Lawful basis - vital interests

(d) Not-for-profit bodies

Article 9(2)(d) permits you to process special category data if:

> “processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects”.

You don’t need a DPA Schedule 1 condition to rely on this condition or an appropriate policy document.

This condition is one of the few that is not purpose-based. Instead, it applies to some specified activities of not-for-profit bodies. Because it is not purpose-based, there is no necessity test. However, this does not mean it is a blanket condition for all processing by not-for-profit bodies. You must still demonstrate how you meet the specific requirements of the condition, and you must still consider your data minimisation obligations.

You can only rely on this condition if you:

- are a not-for-profit body, for example charities, clubs, political parties, churches, trade unions and other associations if they have a political, philosophical, or religious aim;
- are processing special category data as part of your legitimate activities. This is fairly broad, and covers most of what you do, as long as it does not stray outside the purposes and powers set out in your constitution or governing documents, and is not unlawful or unethical in any way;
- are only processing the data of members, former members, or other individuals in regular contact with you ‘in connection with your purposes’, eg partners, supporters or beneficiaries. This condition does not therefore apply to processing employee data, or to prospective members or other individuals who have not had any prior contact with your organisation;
- have appropriate safeguards in place, for example restricting access to the data, applying shorter retention periods, or providing individuals with an opt-out; and
- do not disclose this data to a third party without the individual’s consent. You must get explicit consent for any disclosures. If you need to disclose the data to a third party without consent, you need to rely on a different condition for the disclosure.

Example

A church processes personal data of its members and supporters in order to run church activities and provide pastoral care. The church can rely on the not-for-profit condition to process the data which reveals their religious belief.

The church publishes an annual report which is available to third parties. The church must seek explicit consent before naming any of its members in the annual report.

You may find it useful to conduct a legitimate interests assessment (LIA) to assess appropriate

safeguards and document your reliance on this basis. There is no requirement to do so, but it can help you demonstrate your compliance in line with the accountability principle. More information on how to conduct an LIA is set out in our legitimate interests guidance.

(e) Made public by the data subject

Article 9(2)(e) permits you to process special category data if:

> "processing relates to personal data which are manifestly made public by the data subject".

You don't need a DPA Schedule 1 condition to rely on this condition or an appropriate policy document.

This condition does not cover all special category data in the public domain. It only covers personal data that the individual themselves has made public.

The term 'manifestly made public' is not defined by the GDPR. But it clearly assumes a deliberate act by the individual. It's not enough that it's already in the public domain – it must be the person concerned who took the steps that made it public.

Example

A security breach means that information about an individual's health condition is publicly available from an organisation's website. Clearly, making their special category data public was not a deliberate act on the part of the individual. Therefore this condition would not apply to any processing of health data obtained from the website.

Example

The political affiliations of a member of parliament are technically special category data (these are 'political beliefs'). However these are clearly a matter of public knowledge and the individual has actively chosen to make these public by standing for election as a member of parliament.

You need to be confident that it was the individual themselves who actively chose to make their special category data public and that this was unmistakably a deliberate act on their part. There is a difference between assenting to or being aware of publication, and an individual actively making information available. For example, by blogging or giving a media interview about their health condition or political views. You might also find it hard to show that someone has manifestly made information public if, for example, they made a social media post for family and friends but default audience settings made this public. You should therefore be very cautious about using this condition to justify your use of special

category data obtained from social media posts.

To be manifestly made public, the data must also be realistically accessible to a member of the general public. The question is not whether it is theoretically in the public domain (eg in a publication in a specialist library, or mentioned in court), but whether it is actually publicly available in practice. Disclosures to a limited audience are not necessarily 'manifestly public' for these purposes. In particular, information is not necessarily public just because you have access to it. The question is whether any hypothetical interested member of the public could access this information.

You cannot use this condition to justify publication of previously unpublished data. It only applies to information which is already public.

So to use this condition, you should consider some specific questions:

- Is the special category data already in the public domain – can a member of the public realistically access it in practice?
- Who made the data public – was it the individual themselves or was it someone else? In what context was it made public – for example was it due to them giving an interview, standing for public office, or writing a book, blog or social media post?
- Did the individual deliberately take the steps which made this special category data public, or was it accidental or unintentional? Did they make a clear decision? Is the individual likely to have understood that their action means that their special category data is in the public domain?

For accountability purposes, you should keep a record of the source of the data, to help you demonstrate it was manifestly made public by the individual.

It is important to remember that once you start processing this data, you become the controller for the data and this condition does not exempt you from your other obligations under the GDPR. You must always be able to demonstrate that your processing is more generally lawful, fair and transparent, and in particular that you have a valid lawful basis. You need to consider the individual's reasonable expectations for further use of the data, in order to ensure your processing is fair.

You also need to respect the individual's rights and ensure you tell individuals that you are processing their data. There is no automatic exemption from transparency obligations just because information is in the public domain.

Further reading – ICO guidance

Lawfulness, fairness and transparency
Lawful basis for processing
Right to be informed

More explanation on what counts as 'in the public domain' is available as part of our freedom of information guidance on Information in the public domain.

(f) Legal claims and judicial acts

Article 9(2)(f) permits you to process special category data if:

> “processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity”.

You don’t need a DPA Schedule 1 condition to rely on this condition or an appropriate policy document.

Legal claims

You must show that the purpose of the processing is to establish, exercise or defend legal claims. ‘Legal claims’ in this context is not limited to current legal proceedings. It includes processing necessary for:

- actual or prospective court proceedings;
- obtaining legal advice; or
- establishing, exercising or defending legal rights in any other way.

Example

An employer is being sued by one of its employees following an accident at work. The employer wants to pass the details of the accident to its solicitors to obtain legal advice on its position and potentially to defend the claim. The information about the accident includes details of the individual’s injuries, which qualify as health data. The purpose of the disclosure is to establish its legal position and to defend the claim.

Example

A professional trust and estate practitioner advises a client on setting up a trust to provide for a disabled family member. The adviser processes health data of the beneficiary for this purpose. Although there is no active legal claim before the courts, this is still for the purpose of establishing the legal claims of the trust beneficiary for the purposes of this condition.

Example

A hairdresser conducts a patch test on a client to check that they will not have an allergic reaction to a hair dye. The hairdresser records when the test was taken and the results. The hairdresser is therefore processing health data about the client's allergies. Although there is no actual or expected court claim, the purpose is to establish that the hairdresser is fulfilling their duty of care to the client, and to defend against any potential personal injury claims in the event of an adverse reaction.

You must be able to justify why processing of this specific data is 'necessary' to establish, exercise or defend the legal claim. The use of this data must be relevant and proportionate, and you must not have more data than you need.

Judicial acts

This condition also applies whenever a court (or tribunal) is acting in its judicial capacity.

If you are a court then you can apply this condition whenever you are processing special category data in your judicial capacity. If the processing is not part of your judicial duties then this condition does not apply and you need to look for an alternative condition in order to be able to process special category data.

(g) Substantial public interest

Article 9(2)(g) permits you to process special category data if:

> "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law 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 the interests of the data subject".

The relevant basis in UK law is set out in section 10(3) of the DPA 2018. This means that you need to meet one of the 23 specific substantial public interest conditions set out in Schedule 1 (at paragraphs 6 to 28). You must also have an 'appropriate policy document' in place for almost all of these conditions.

For more information, see What are the substantial public interest conditions?

(h) Health or social care

Article 9(2)(h) permits you to process special category data if:

> "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

The relevant basis in UK law is set out in the DPA 2018, in Schedule 1 condition 2. This condition covers the following purposes:

- preventive or occupational medicine;
- the assessment of an employee's working capacity;
- medical diagnosis;
- the provision of health care or treatment;
- the provision of social care (this is likely to include social work, personal care and social support services); or
- the management of health care systems or services or social care systems or services.

You must be able to justify why processing of this specific data is 'necessary' - it must be a reasonable and proportionate way of achieving one of these purposes, and you must not have more data than you need.

Article 9(3) of the GDPR contains the additional safeguard that you can only rely on this condition if the personal data is being processed by (or under the responsibility of) a professional who is subject to an obligation of professional secrecy. Section 11 of the DPA 2018 makes it clear that in the UK this includes:

(a) a health professional or a social work professional; or
(b) another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

Section 204 of the DPA 2018 defines the terms "health professional" and "social work professional". You should check the full details of section 204 where relevant, but as a guide this includes:

- doctors;
- nurses or midwives;
- dentists;
- opticians or optometrists;
- osteopaths;
- chiropractors;
- arts therapists;
- chiropodists;
- clinical scientists;
- dietitians;
- medical laboratory technicians;
- occupational therapists;

- orthoptists;
- paramedics;
- physiotherapists;
- prosthetists or orthotists;
- radiographers;
- speech and language therapists;
- pharmacists or pharmacy technicians;
- child psychotherapists; and
- social workers.

If you are not subject to a duty of confidentiality to the individual, but you are under a legal obligation in connection with the provision of social services, the condition for employment, social security and social protection law may be more appropriate.

You don't need to have an appropriate policy document in place.

Where this condition applies, the individual does not have a right to erasure.

(i) Public health

Article 9(2)(i) permits you to process special category data if:

> "processing is necessary for **reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".

The relevant basis in UK law is set out in the DPA 2018, in Schedule 1 condition 3. In order to rely on this condition the processing must be carried out either:

- by, or under the responsibility of, a health professional; or
- by someone else who in the circumstances owes a legal duty of confidentiality.

Recital 54 of the GDPR gives more guidance on what is meant by 'public health':

> "all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality."

You must be able to demonstrate that the processing is necessary for reasons of **public interest** in the area of public health. The term 'public interest' is not defined, but you need to point to a benefit to the wider public or society as a whole, rather than to your own interests or the interests of the particular individual. In particular, recital 54 makes clear this condition should not enable processing for other purposes by employers, or by insurance or banking companies.

This condition may for example apply where the processing is necessary for:

- public health monitoring and statistics;
- NHS resource planning;
- public vaccination programmes;
- responding to new threats to public health (eg epidemics, pandemics or new research findings);
- clinical trials of drugs or medical devices;
- regulatory approval of drugs or medical devices; or
- reviewing standards of clinical practice.

Example

A number of GP surgeries wish to use a workforce and workload planning tool for their practices. The tool requires the analysis of patients' health data to supply information on current activity, and identifies opportunities to improve effectiveness and efficiency of health provision. The GP surgeries can justify that this is necessary for public interest reasons in the area of public health.

You don't need to have an appropriate policy document in place.

Where this condition applies, the individual does not have a right to erasure.

(j) Archiving, research and statistics

Article 9(2)(j) permits you to process special category data if:

> "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

The relevant basis in UK law is set out in the DPA 2018, in Schedule 1 condition 4. This condition requires you to:

- demonstrate that the processing is necessary for archiving, research or statistical purposes - it must be a reasonable and proportionate way of achieving one of these purposes, and you must not have

more data than you need;

- comply with the safeguards and restrictions set out in Article 89(1) of the GDPR and section 19 of the DPA 2018 (see below); and
- demonstrate that the processing is in the public interest. The term 'public interest' is not defined, but you need to point to a benefit to the wider public or society as a whole, rather than to your own interests or the interests of the particular individual.

Not all research is covered by this condition. You need to demonstrate that your research is either scientific or historical in nature, and in the public interest. This applies to both public-sector and private-sector research. It can include, for example, technological development and demonstration, fundamental research, applied research and privately funded research. Commercial scientific research may therefore be covered, but you need to demonstrate that it uses rigorous scientific methods and furthers a general public interest. However, commercial market research is unlikely to be covered, unless you meet this requirement.

Article 89(1) says that you must have appropriate safeguards in place to protect individuals, and in particular technological and organisational measures to ensure data minimisation. Section 19 of the DPA 2018 contains further safeguards and restrictions. In particular, this means you must:

- be able to demonstrate why you cannot use anonymised data;
- consider whether you could use pseudonymisation to make it more difficult to link the personal data back to specific individuals;
- be able to demonstrate that the processing is not likely to cause substantial damage or distress to individuals;
- not use the data to take any action or make decisions in relation to the individuals concerned (unless you are carrying out approved medical research as defined in section 19(4) of the DPA 2018); and
- consider other appropriate safeguards and security measures.

You don't need to have an appropriate policy document in place.

Example

A hospital asks a number of patients for their informed consent to take part in a series of clinical trials for a new medication, in line with clinical trials regulations.

However, for the purposes of the GDPR, the hospital does not wish to rely upon explicit consent as its condition for processing the participants' health data. The hospital needs to continue to process the research data already collected even if the patient withdraws their consent and drops out of the trial. It also considers that in the context of a clinical trial, consent does not match the 'freely given' standard of the GDPR, given the imbalance of power between the patient and the hospital clinicians.

Instead the hospital relies upon Article 9(2)(j) - processing for scientific research purposes - as its condition for processing the special category data of the participants. It ensures it has addressed the safeguards set out in Article 89(1) of the GDPR and in section 19 of the DPA 2018.

The hospital's Article 6 basis for processing is Article 6(1)(e) - the performance of a task carried out in the public interest.

Further reading – European Data Protection Board (EDPB)

The EDPB has adopted an opinion on the interplay between the CTR and the GDPR.

What are the substantial public interest conditions?

In detail:

What substantial public interest conditions are available?

The 23 conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements
13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk
19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

You should identify which of these conditions appears to most closely reflect your purpose. This guidance gives you some general advice on how the conditions generally work, but you always need to refer to the detailed provisions of each condition in the legislation itself to make sure you can demonstrate it applies.

How do the substantial public interest conditions work?

The substantial public interest conditions give you the basis in UK law for relying on Article 9(2)(g).

These conditions allow you to process special category data for a variety of specific purposes. If you are clear on your purpose for processing, it should be relatively straightforward to identify the most relevant condition(s). You then need to consider the detail of that condition carefully, and ensure you can demonstrate that it applies. The conditions are narrowly drawn and generally require you to meet a number of specific criteria.

For some of these conditions, the substantial public interest element is built in. For others, you need to be able to demonstrate that your specific processing is "necessary for reasons of substantial public interest", on a case-by-case basis.

For some of the conditions, you also need to justify why you cannot give individuals a choice and get explicit consent for your processing.

In most cases, you must have an 'appropriate policy document' in place.

6. Statutory and government purposes	Y	N	Y
7. Administration of justice and parliamentary purposes	N	N	Y
8. Equality of opportunity or treatment	N	N	Y
9. Racial and ethnic diversity at senior levels	N	Y	Y
10. Preventing or detecting unlawful acts	Y	Y	Y/N*
11. Protecting the public	Y	Y	Y
12. Regulatory requirements	Y	Y	Y
13. Journalism, academia, art and literature	Y	N	N
14. Preventing fraud	N	N	Y
15. Suspicion of terrorist financing or money laundering	N	N	Y
16. Support for individuals with a particular disability or medical condition	Y	Y	Y
17. Counselling	Y	Y	Y
18. Safeguarding of children and individuals at risk	Y	Y	Y

19. Safeguarding of economic well-being of certain individuals	Y	Y	Y
20. Insurance	Y	Y	Y
21. Occupational pensions	N	Y	Y
22. Political parties	N	N	Y
23. Elected representatives responding to requests	N	Y	Y
24. Disclosure to elected representatives	N	Y	Y
25. Informing elected representatives about prisoners	N	N	Y
26. Publication of legal judgement	N	N	Y
27. Anti-doping in sport	N	N	Y/N*
28. Standards of behaviour in sport	Y	Y	Y

*Under conditions 10 and 27, you don't need an appropriate policy document to disclose data to the relevant authorities (or prepare to disclose it). You still need an appropriate policy document for other processing activities.

What are 'reasons of substantial public interest'?

The term 'substantial public interest' is not defined in the DPA 2018 or the GDPR.

Some of the conditions assume that processing under that condition is always in the substantial public interest, eg ensuring equality, or preventing fraud. However, some only apply to the extent that the processing is "necessary for reasons of substantial public interest".

The public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. Commercial or private interests are not the same as a public interest, and if you need to point to reasons of substantial public interest it is not enough to point to your own interests. Of course, you can still have a private interest - you just need to make sure that you can also point to a wider public benefit.

Substantial public interest means the public interest needs to be real and of substance. Given the inherent risks of special category data, it is not enough to make a vague or generic public interest argument – you should be able to make specific arguments about the concrete wider benefits of your processing. For example, you may wish to consider how your processing benefits the public in terms of both depth (ie the amount of benefit experienced from the processing, even if by a small number of people) and breadth (the volume of people benefiting from the processing).

You should focus on showing that your overall purpose for processing has substantial public interest benefits. You do not need to make separate public interest arguments or show specific benefits each time you undertake that processing, or for each separate item of special category data, as long as your overall purpose for processing special category data is of substantial public interest. However, you must

always be able to demonstrate that all your processing under the relevant condition is actually necessary for that purpose and complies with the data minimisation principle.

What is the role of consent?

Many of the substantial public interest conditions only apply if there is a good reason why you cannot get valid explicit consent.

As a general rule, for these conditions you should consider first whether you could give individuals a choice and only process their special category data with their explicit consent. However, there may be a good reason why you should not give individuals an upfront choice. For example, you might not want to ask for consent if you were investigating someone and tipping them off might prejudice your investigation. Alternatively, you may be able to show that you cannot technically get valid consent in the circumstances, but there is a good reason to go ahead anyway. For example, public authorities, employers and other organisations in a position of power may not be able to demonstrate that consent would be freely given.

The details of the conditions vary, so if you do have a reason for not getting explicit consent, or you think it wouldn't be valid, you must always check the detail of the relevant condition to see exactly what justification you need.

Further reading – ICO guidance

Consent

What is an appropriate policy document?

An appropriate policy document is a short document outlining your compliance measures and retention policies for special category data. The DPA 2018 says you must have one in place for almost all of the substantial public interest conditions (and also for the employment, social security and social protection condition), as a specific accountability and documentation measure.

It doesn't have to take any particular form, as long as it briefly outlines:

- the Schedule 1 condition (or conditions) you are relying on;
- your procedures for complying with each of the principles;
- your retention and deletion policies; and
- an indication of the retention period for the specific data.

If you process special category data for a number of different purposes you don't need a separate policy document for each condition or processing activity – one document can cover them all. You should provide the data subject with sufficient information to understand how you are processing their special category data and how long you will retain it for.

We have developed an appropriate policy document template to help you meet this requirement.

If you have carried out a DPIA, you should be able to reuse Part 4 of your DPIA (necessity and proportionality) to inform your appropriate policy document.

You need to retain your appropriate policy document until six months after the date you stop the relevant processing. You must keep it under review. You do not have to publish it, although it is good practice to do so. If we ask to see it, you must provide it to us free of charge.

You also need to include some further details in your general GDPR documentation:

- how the processing satisfies a lawful basis;
- your condition for processing special category data; and
- whether you have followed your retention and deletion policies - and if not, why not.

Further Reading

> See DPA 2018, Schedule 1 paragraphs 5 and 38-41
> External link

Further reading – ICO guidance

Documentation