Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'.
- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

What information does the GDPR apply to?

- **Personal data**

  The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

  This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

  The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

  Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

- **Sensitive personal data**

  The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

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

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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

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

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

- For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data.
- It is important that you determine your lawful basis for processing personal data and document this.
- Your lawful basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.

At a glance

- The GDPR sets a high standard for consent.
- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh consents if they don't meet the GDPR standard.
- Consent means offering individuals genuine choice and control.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of consent by default.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and granular. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent a precondition of a service.
- Public authorities and employers will find using consent difficult.
- Remember – you don't always need consent. If consent is too difficult, look at whether another lawful basis is more appropriate.

Checklists

Asking for consent

☐ We have checked that consent is the most appropriate lawful basis for processing.
☐ We have made the request for consent prominent and separate from our terms and conditions.
☐ We ask people to positively opt in.
☐ We don't use pre-ticked boxes, or any other type of consent by default.
☐ We use clear, plain language that is easy to understand.
☐ We specify why we want the data and what we're going to do with it.
☐ We give granular options to consent to independent processing operations.
☐ We have named our organisation and any third party controllers who will be relying on the consent.
☐ We tell individuals they can withdraw their consent.
☐ We ensure that the individual can refuse to consent without detriment.
☐ We don't make consent a precondition of a service.

4Recording consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Managing consent

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don't penalise individuals who wish to withdraw consent.

In brief

What's new?

- The GDPR sets a high standard for consent, but the biggest change is what this means in practice for your consent mechanisms.
- The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action.
- Consent should be separate from other terms and conditions. It should not generally be a precondition of signing up to a service.
- The GDPR specifically bans pre-ticked opt-in boxes.
- It requires granular consent for distinct processing operations.
- You must keep clear records to demonstrate consent.
- The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.
- Public authorities, employers and other organisations in a position of power are likely to find it more difficult to get valid consent.
- You need to review existing consents and your consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.
-

Why is consent important?

- Consent is one lawful basis for processing, and consent (or explicit consent) can also legitimise use of special category data, restricted processing, automated decision-making or overseas transfers.
- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Relying on inappropriate or invalid consent could destroy trust and harm your reputation – and may leave you open to substantial fines.
-

When is consent appropriate?

- Consent is one lawful basis for processing, but there are alternatives. If consent is difficult, you should consider using an alternative basis.
- Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate.
- If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

- If you make 'consent' a precondition of a service, consent is unlikely to be the most appropriate lawful basis.
- Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent as it is unlikely to be freely given.
-

What is valid consent?

- Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.
- Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.
- Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
- Consent should be obvious and require a positive action to opt in.
- Explicit consent must be expressly confirmed in words, rather than by any other positive action.
- There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.
-

How should you obtain, record and manage consent?

- Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand.
- Include the name of your organisation and any third party controllers who will be relying on the consent, why you want the data, what you will do with it, and the right to withdraw consent at any time.
- You must ask people to actively opt in. Don't use pre-ticked boxes, opt-out boxes or default settings.
- Wherever possible, give granular options to consent separately to different purposes and different types of processing.
- Keep records to evidence consent – who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose. Consider using preference-management tools.
- Keep consents under review and refresh them if anything changes. Build regular consent reviews into your business processes.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

What is the accountability principle?

The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

How can I demonstrate that I comply?

You must:

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default.

Measures could include:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing; and
- creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.