Implications for organisations

Obtaining consent

The GDPR requires **explicit** consent to capture, store and process personal data. This can be achieved by:

- **Using positive opt-ins**
  Websites and digital advertising requesting personal data must include a positive opt-in box so individuals are aware what they are signing up to. Pre-filled tick boxes and implied consent is no longer acceptable.

- **Displaying clearly worded privacy notices**
  Websites must display links to clear and concise statements written in plain English, outlining how personal data collected is stored, shared and processed.

- **Being specific and granular**
  Only request the personal data that is required, and use it for the purposes specified in the privacy notice.

Consent case study

Bad practice	Best practice
A company outsource their email campaign to a PR agency who create a website form for individuals to subscribe to an email newsletter. The form captures the following data: • Full name • Email address • Phone number • Postcode Captured data is retained indefinitely with the email addresses also used for Facebook advertising.	The same campaign would meet GDPR requirements with the following changes. The form captures only the personal data required for the campaign: • First name • Email address The form includes a prominent tick box for individuals to opt-in to receive regular email updates. A clear link to the privacy notice is included, with an explanation of how the personal data is to be used. Personal data is not held indefinitely, and individuals are notified on a regular basis by email if they wish to still remain on the lists.

Why this is wrong • Individuals were not clearly informed what they were signing up for. • The email campaign only required a name and email address, but other personal data was requested. • Personal data was processed and used for another purpose (Facebook advertising) not originally outlined. • Personal data was held indefinitely and individuals were not notified.	**Why this is correct** This fulfils the requirements by: • Providing a positive opt-in option on the form. • Displaying a clear privacy notice. • Being specific about how personal data will be used. • Processing the data responsibly within a given time period. • Keeping individuals updated and actively managing consent.

Data processing overview
This refers to any use of personal or sensitive data done in-house or outsourced to a third-party.

Examples include:

- Registering individuals at an event or conference using an app.
- An HR department dealing with a job application.
- Using personal data from a contact form on a website to arrange research trials.
- Using personal data to send out email and direct marketing campaigns.
- Using personal data to deliver targeted social media advertising (Facebook, Twitter, Instagram and LinkedIn).
- A medical professional using sensitive medical data to safeguard at-risk individuals.
- Setting up appointments for individuals who have provided personal data to a chatbot (eg Facebook Messenger).
- Providing a sales quote based on personal data provided to voice assistants (eg Amazon Alexa or Google Home).
- Automated systems using artificial intelligence and algorithms to make decisions based on personal and sensitive data (eg health insurance premiums).

To simplify data processing, the GDPR helpfully defines specific roles and responsibilities. Let's explore these…

Roles and responsibilities
GDPR defines two roles for companies and organisations:

- **Data Controller**
  Person(s) who define the policy, processes and manner in which personal data is handled within an organisation.

  They are ultimately responsible for all personal and sensitive data.

- **Data Processor**
  Any person(s) other than a direct employee of the Data Controller who process personal data for the Data Controller (eg a PR / digital agency or financial services company).

Public authorities must also appoint a **Data Protection Officer (DPO)** to safeguard sensitive data. The criteria are as follows:

- are a public authority (except for courts acting in their judicial capacity);

- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or

- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.