Let's talk GDPR:
Fair, transparent, lawful and accountable

UK Information Commissioner's Office

The Information Commissioner is the regulator of data protection law in the UK, as well as freedom of information laws in England, Wales, Northern Ireland and UK Government bodies. www.ico.org.uk

One unified law that applies directly to all EEA member states. Text of the Regulation - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
However, member states are left with derogations in certain areas which they must implement in national law.

The UK Government introduced a new Data Protection Bill on 13 September 2017. The Bill will exercise some areas of discretion left to member states in the GDPR.

It also confirms the Information Commissioner will be responsible for monitoring and enforcing compliance in the UK and gives her powers to do so.

You can find the latest details of the Bill on the UK Parliament website at https://services.parliament.uk/bills/2017-19/dataprotection.html.

Fair and transparent

ico.
Information Commissioner's Office

Right to be informed

- Your contact details
- The purposes and lawful basis
- Any recipients of the personal data
- Any international transfers
- Retention periods
- The data subject's rights

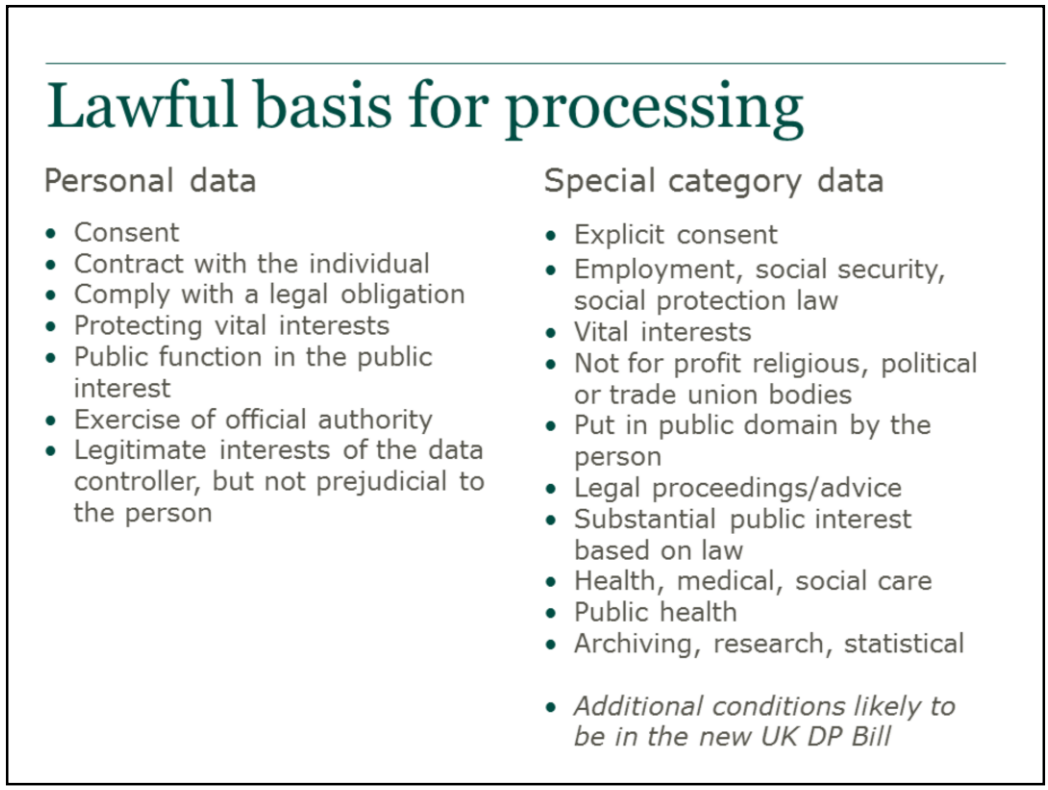
More information, including a link to our guidance on privacy notices, can be found in our guide to GDPR at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

How you inform

- Concise
- Transparent
- Intelligible
- Easily accessible
- Clear and plain language
- Consider the audience

Lawful

ico.
Information Commissioner's Office



In order to use personal data lawfully, you need to be able to have a lawful basis for processing. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Other than consent, the conditions require that the processing is **necessary**. Consent has its own particular requirements.

All conditions have equal weighting: one does not carry any more status than any other. It is for the data controller to be satisfied that they are relying on the appropriate condition and it is recommended that a record is kept of the basis on which the use is being made. This is especially important when not relying on consent.

Legitimate interests

- Direct marketing is a legitimate interest
- It must not override the rights and freedoms of the individual
- A legitimate interest must be within an individual's reasonable expectation

Recital 47, GDPR

We have published guidance on the legitimate interests basis for processing in our Guide to the GDPR at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

Consent must be:

- Able to be refused or withdrawn
- Freely given, specific, informed and unambiguous
- A clear, affirmative act
- Intelligible and easily accessible
- Requested in plain language
- Separate from other matters

The ICO published draft guidance on consent for consultation earlier in 2017. A finalised version is expected in early 2018.

More information on consent, including a link to the draft guidance, is available in our Guide to GDPR at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Section 11(3), Data Protection Act 1998

Direct marketing

The communication (by whatever means) of any particular advertising or marketing material which is directed to particular individuals.

This includes material promoting the aims of not-for-profit organisations.

Children

"…specific protection should, in particular, apply to the use of personal data of children for the purposes of **marketing** or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."

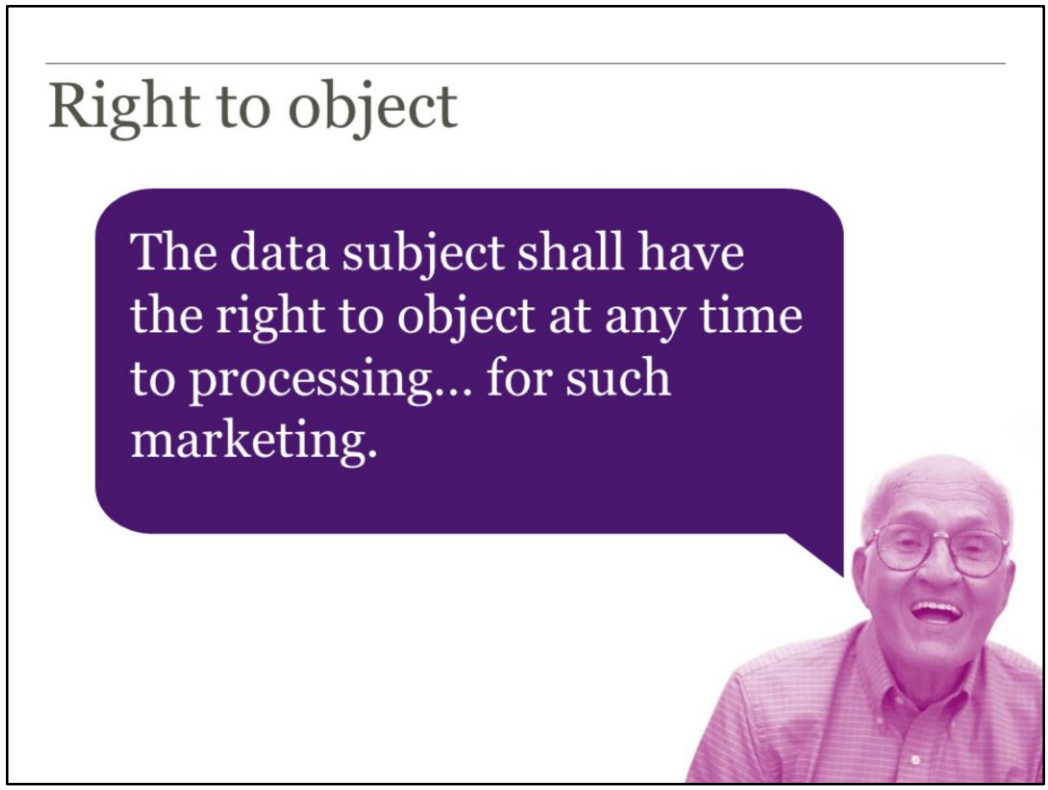
Recital 38, GDPR

The ICO expects to publish guidance on children and data protection in 2018.

Our Guide to PECR can be found on our website at: https://ico.org.uk/for-organisations/guide-to-pecr/

A new e-Privacy Regulation is being drafted by the EU which could change the rules for direct marketing by electronic methods.

This will eventually replace the UK's Privacy and Electronic Communications Regulations 2003.

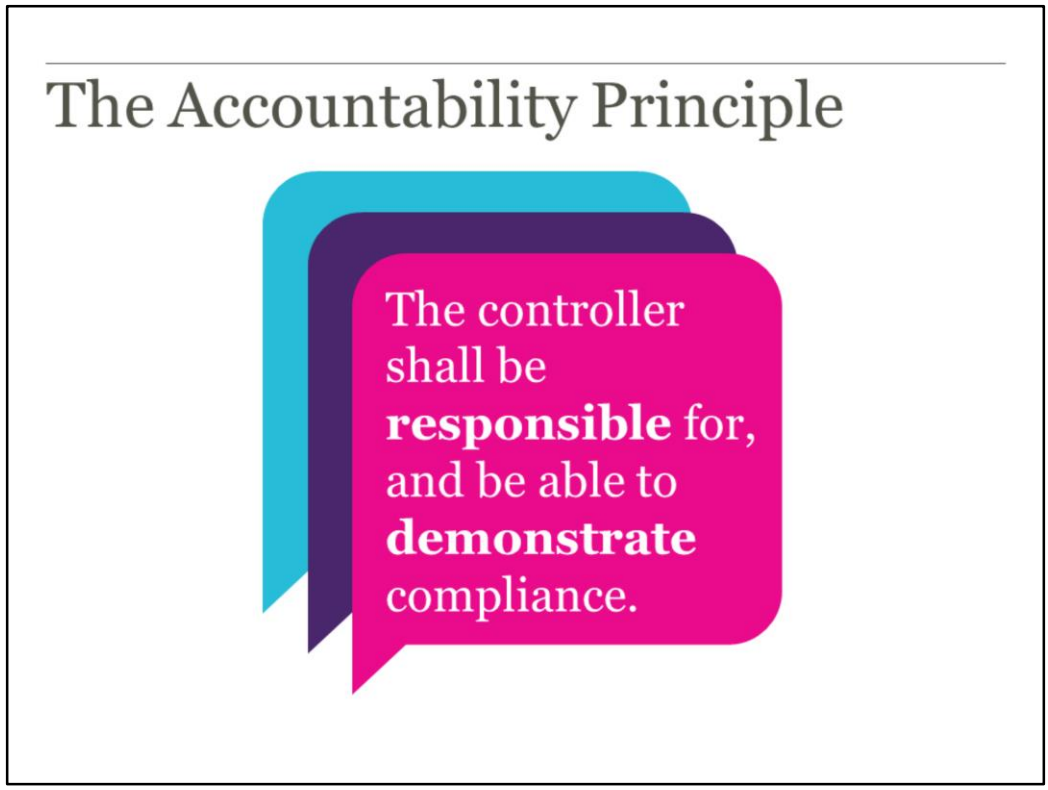


The right to object to processing of personal data for direct marketing purposes is absolute. Organisations must comply with an objection as quickly as possible.

More information on the right to object can be found in our Guide to the GDPR at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

Accountable

ico.
Information Commissioner's Office



https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

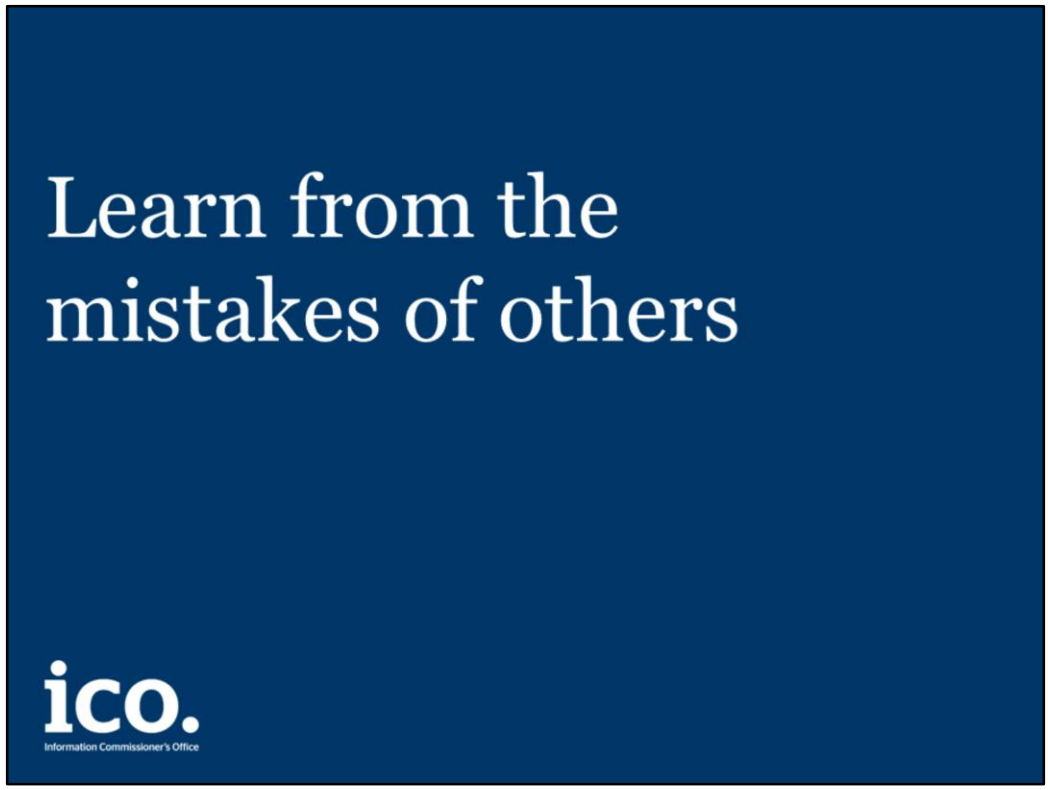
More information, including links to ICO and European guidelines, is available in our Guide to the GDPR at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Data processors

Now liable if they do not follow your instructions

- You must only use a processor providing sufficient guarantees that they can meet GDPR requirements
- Contract must govern data processing in detail
- Controller must provide documented instructions on what to do with the data
- Contract must specify whether or not a sub-processor can be engaged
- Processor must assist the controller as required to comply with GDPR and must allow audits of the processing

Further information on contracts with data processors can be found in our Guide to the GDPR at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/


Learn from the
mistakes of others
ico.
Information Commissioner's Office

MF

Further details of our enforcement action can be found at:
https://ico.org.uk/action-weve-taken/charity-fundraising-enforcement-action/

The full monetary penalty notice can be found at:
https://ico.org.uk/action-weve-taken/enforcement/flybe-limited/

MF

The full monetary penalty notice can be found at:
https://ico.org.uk/action-weve-taken/enforcement/honda-motor-europe-limited/

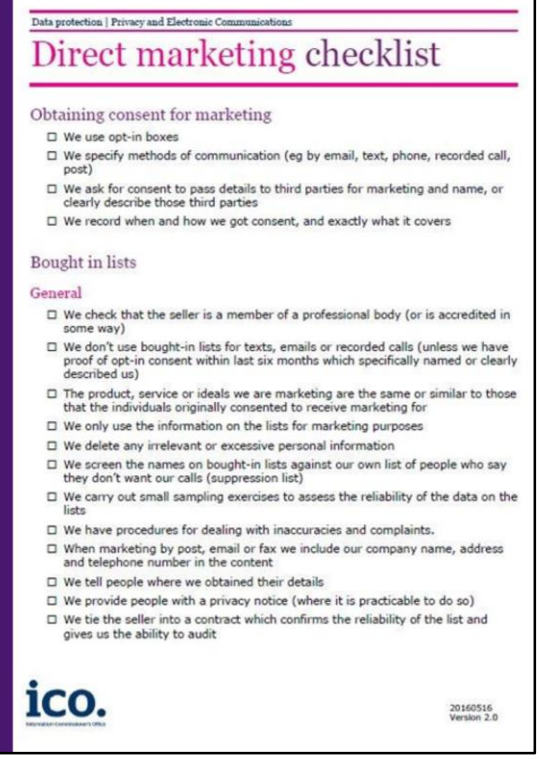
Support and resources

ico.
Information Commissioner's Office

https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/

Our sector page for charities: https://ico.org.uk/for-organisations/charity/

Existing ICO guidance



Data protection | Privacy and Electronic Communications

Direct marketing checklist

Obtaining consent for marketing

- ☐ We use opt-in boxes
- ☐ We specify methods of communication (eg by email, text, phone, recorded call, post)
- ☐ We ask for consent to pass details to third parties for marketing and name, or clearly describe those third parties
- ☐ We record when and how we got consent, and exactly what it covers

Bought in lists

General

- ☐ We check that the seller is a member of a professional body (or is accredited in some way)
- ☐ We don't use bought-in lists for texts, emails or recorded calls (unless we have proof of opt-in consent within last six months which specifically named or clearly described us)
- ☐ The product, service or ideals we are marketing are the same or similar to those that the individuals originally consented to receive marketing for
- ☐ We only use the information on the lists for marketing purposes
- ☐ We delete any irrelevant or excessive personal information
- ☐ We screen the names on bought-in lists against our own list of people who say they don't want our calls (suppression list)
- ☐ We carry out small sampling exercises to assess the reliability of the data on the lists
- ☐ We have procedures for dealing with inaccuracies and complaints.
- ☐ When marketing by post, email or fax we include our company name, address and telephone number in the content
- ☐ We tell people where we obtained their details
- ☐ We provide people with a privacy notice (where it is practicable to do so)
- ☐ We tie the seller into a contract which confirms the reliability of the list and gives us the ability to audit

ico.

20160516
Version 2.0

Checklist: https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf
Full guidance: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

We expect the new UK Data Protection Bill will enable us to publish a statutory code on direct marketing. This gives it a legal status and it can be submitted as evidence in legal proceedings.

Webinars

https://ico.org.uk/for-organisations/resources-and-support/webinars/

Including webinars on direct marketing for charities, and data protection for SMEs

www.ico.org.uk/enewsletter

Working with the third sector

OSCR/Panel

GDPR blogs and regulatory cooperation

SCVO

GDPR blogs and conference

TSIs/Reps

Workshops

Keep in touch

ICO Scotland
45 Melville Street
Edinburgh EH3 7HL
T: 0303 123 1115
E: Scotland@ico.org.uk

@iconews

How would you like to be treated?