ALAN CALDER

A NEW AGE OF CONSENT

What is the lawful basis for processing personal data and retaining it under the GDPR?

Under the General Data Protection Regulation (GDPR), every organisation that processes personal information needs to ensure it does so lawfully, fairly and transparently. Documenting your processes is essential. If you cannot demonstrate a lawful basis for processing before you start, any processing you carry out will necessarily be unlawful and you will be subject to the higher level of fines (up to €20m or 4% of annual global turnover – whichever is greater).

LAWFUL PROCESSING

Article 6 of the Regulation (Lawfulness of processing) states that processing is lawful only if and to the extent that one of the following conditions applies.

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3. Processing is necessary for compliance with a legal obligation to which the controller is subject.
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (this basis doesn't apply to processing carried out by public authorities in the performance of their tasks).

Consent, unsurprisingly, tends to get most attention. However, it's arguably the weakest basis because it can be withdrawn, so it's worth considering whether another lawful basis applies or can apply. For example, when you process staff data for payroll purposes, point 2 will apply as they will have signed a contract of employment – you will not need to obtain their consent.

Determining your lawful basis for processing personal data ought to be obvious given the processing you carry out, but a data protection impact assessment could prove helpful. It's also worth remembering that your decision will have an effect on data subjects' rights and your obligations as a data processor, especially if you rely on consent.

TICK THE BOXES

The GDPR is more specific than the Data Protection Act 1998 (DPA) when it comes to consent, especially in terms of how it should be given. Article 7 of the Regulation sets out the conditions for consent, but more detail is provided in Recital 32, which stipulates that "consent should be given by a clear affirmative act" and that "silence, pre-ticked boxes or inactivity should not therefore constitute consent".

If you have relied on consent under the DPA, you cannot assume it is still lawful under the GDPR. You will need to ensure it meets the regulation's requirements and if it does not, you will need to change your consent mechanisms and obtain fresh consent – or find an alternative lawful basis for processing.

It's essential that you keep records of consent, as stipulated by Article 7. This is particularly important because, under the GDPR, data subjects have the right to withdraw their consent at any time – and it must be as easy to do so as it was to provide it in the first place. You will then be obliged to erase their data "without undue delay" – not a simple proposition, especially if it has been shared or made public – so it is essential to ensure that you have appropriate processes in place.

If you haven't started your GDPR compliance project, the clock is ticking. You have until 25 May 2018 to bring your personal data processing into line with the new law.

Visit the IT Faculty's hub at icaew.com/gdpr for more information. ●

Alan Calder, CEO, IT Governance