PAUL | TICHER

Data Protection roundup: December 2017

GDPR progress

You may already have picked up on some of the recent developments, but lots has been going on. Bear in mind that things are still changing all the time, so some of this may even already be out of date!

Updated ICO GDPR guidance

The ICO has revised and expanded their guidance on GDPR. A lot of it is still very light on detail, but the section on consent is worth looking at, as it stresses that consent is just one of the possible legal bases for processing, and not always the most appropriate one.

The Data Protection Bill

This was introduced to the House of Lords (which is where the 1998 Act started too) on 13th September 2017.

Why will we need a Data Protection Act when we have GDPR? The bill sets out to do three things:

- There are various places in GDPR where national governments are allowed to make minor amendments and the Bill covers these.
- GDPR does not apply Data Protection to certain areas, including law enforcement and national security. These are subject to separate EU provisions, and the Bill contains the necessary UK legislation to implement these.
- The Bill ensures that our Data Protection regime will remain unchanged after the UK has left the EU.

The Bill is divided into a number of separate parts, and it is important to be clear which part you are reading. One of my clients was told that the Bill introduces a requirement for *all* organisations to have a qualified Data Protection Officer even though GDPR only requires this in very specific circumstances.

However, it turned out that this provision is in Part 3, which applies to law enforcement, not in Part 2 which has general application. Panic over!

The Bill has made steady progress through committee, and is now at the report stage.

Once we know for sure what is likely to be in the final version this will be the subject of a future update.

For more information see:

- The text of the Bill (as amended in Committee).
- The 'Keeling' version of GDPR, which shows how GDPR would read in the UK if everything in the original Bill went through unchanged.

- The ICO page on progress with the Bill.

ICO promises to play nice

Simon Entwisle from the ICO spoke reassuring words at an NCVO conference in November. He said that the ICO will be "proportionate" in how it enforces GDPR and will be pragmatic and "risk-based" if an organisation can show that it is actively working on GDPR and taking it seriously.

Meanwhile the Information Commissioner had already said that she is not intending to ramp up the level of fines for breaches, despite the new maximum being so much higher than at present.

Registration with the ICO

As you may be aware, GDPR says that: "While [the general obligation to notify the processing of personal data to (the ICO)] produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished".

However, a little-noticed provision in the UK's Digital Economy Act 2017 over-rides GDPR and reintroduces registration for the UK. The ICO has announced that there will be several levels of fee (amounts not yet publicised, but rumoured to be higher than the current £35), and that these will apply to any registration that has to be made or renewed from April 2018.

This suits both the ICO, which therefore retains an income independent of government funding, and the government itself, which avoids having to fund the ICO.

Further details, including any exemptions that will be available, are yet to be announced.

Legitimate interests

Many organisations are having to decide which of their processing should be based on consent, and which activities are more appropriately based on their 'legitimate interests'.

In many cases the arguments for legitimate interests (or other legal bases) are turning out to be convincing in more situations than people originally thought, leaving consent for those situations where it clearly should be optional whether you process people's data or not.

The Data Protection Network has issued a 30-page document setting out in detail how an organisation might establish that it can use legitimate interest as its basis for processing. Three questions have to be answered:

- Can we show that we have a legitimate interest?
- Is the processing necessary in order to achieve that interest?
- Does our interest outweigh the interests of the Data Subject?

The document includes a lengthy set of questions to help make these judgements. It's probably too detailed for relatively straightforward situations, but at least worth looking at for an overview of a well thought-through approach.

Profiling & automated decisions

GDPR introduces new restrictions on automated decision-making ("computer says no" situations) and profiling – trying to work out something about an individual from information you hold or acquire.

These concepts have been analysed in detail by an EU committee (the "Article 29 Data Protection Working Party").

Entirely automated decision-making does not appear to happen very often in the voluntary sector, but profiling does occur (and got the thumbs down from the ICO in their enforcement action against 13 charities a year ago because it took place without the Data Subjects' knowledge).

The Working Party report explains the issues in some detail. It does say that profiling may take place on the basis of legitimate interests if the impact on the individuals is slight, but it doesn't suggest that any exemption is available from the requirement to be transparent.

This is a complex area which I intend to write on in more detail before too long.

Data Processor contracts

GDPR says a lot about what has to be in contracts between Controllers and Processors. In September the ICO issued draft guidance on this for consultation (which no longer seems to be available on the ICO website – email me for a copy).

This describes the additional terms that now have to be in every contract, in order to cover compliance with all aspects of GDPR. There is a list of eight items that must be included, and the content under each item has to be specific. The terms commonly seen in current contracts to "comply with the Data Protection Act", or something like that, will no longer do.

Many existing Data Processor contracts don't even meet the requirements of the current Data Protection Act, so it is essential that every organisation:

- identifies all the Data Processors it uses;
- finds the relevant contracts – even those that were been entered into long ago;
- reviews the contracts; and
- negotiates improvements where necessary.

This process, in my experience, is unlikely to be quick or easy, but it must be done.

Some companies whose business is based on acting as a Data Processor might already have begun to issue revised contracts; however, it is the Data Controller's responsibility to ensure that a compliant contract is in place, so you should be prepared to take the initiative.

When reviewing your contracts, you might also find this detailed set of proposed model terms useful.

Fundraising: the debates continue

There have been several reports over the last couple of months relating to the consent vs legitimate interests debate:

- September: the RNLI reported that its individual fundraising income had gone down by about 10% (£5million) after it moved to opt-in only communications – a smaller decline than it had expected.
- October: Comic Relief announced that it would be relying on legitimate interests for its mailings in 2018.
- November: Cancer Research UK (CRUK) reported that responses from new supporters being asked to opt in were around 45% for email, 20% for postal mail and "single figures" for telephone.

Perhaps in response to figures such as those from CRUK, many commentators are now arguing that charities should not be feeling obliged to move to consent only for contact with supporters, but should use legitimate interests where it is appropriate – as long as supporters are fully informed, of course and offered the opt out that they are legally entitled to.

The Fundraising Regulator's existence hasn't stopped the press from finding fault. In November the *Daily Mail* claimed that charities are getting round the rules on direct mail by sending mail to 'the householder'. And the *Daily Telegraph* claimed that universities are still using the type of wealth screening that led to 13 charities being fined a year ago. Both stories were dismissed, by the Fundraising Regulator and the Institute of Fundraising respectively.

The British Heart Foundation's Head of Legal Services, meanwhile, criticised the ICO for imposing the fines a year ago – seemingly because of media and political pressure – when the charities had already responded to the ICO's concerns.

For a slightly different take on fundraising and Data Protection, it's worth a look at Tim Turner's guidance, from the point of view of a Data Protection expert well outside voluntary sector fundraising.

Transfers abroad

GDPR rules on data transfers to countries outside the European Data Protection framework are very similar to those currently in place. The ICO reported in October on a study that showed many organisations not providing adequate information about data transfers, or referring to the out-of-date US Safe Harbor arrangement.

Under GDPR you *must* know where your data is stored and you *must* tell people if it is outside the European framework.

Meanwhile Privacy Shield – the current arrangement with the USA – has passed its first annual review from the European Commission, so remains accepted as providing an adequate level of protection.

However, Privacy Shield and the EU's model clauses that are an alternative way to underpin data transfers abroad are being challenged legally by Max Schrems – who previously achieved the demise of Safe Harbor through a similar challenge.

Charity breaches

According to data from the ICO, charities reported 27 data security incidents in the first quarter of 2017 and 21 in the second quarter. The most frequent causes were loss or theft of paperwork, cyber incidents failure to use BCC and lost devices.

Don't forget that under GDPR it will for the first time be mandatory to report serious breaches – within 72 hours of becoming aware of them. Make sure that your staff (and volunteers) know how to report a breach internally so that you can decide quickly on remedial action, and whether it requires reporting to the ICO.

ICO hotline

I do try to provide good information, but if you want a second opinion you could always try the ICO's new hotline for smaller organisations (employing under 250 people): dial the normal support line 0303 123 1113 and select option 4.

And by the way: Don't steal your employer's data

A charity worker from Rochdale now has a criminal record after emailing personal data about 183 of his organisation's clients to himself. This is a breach of s.55 of the Data Protection Act. He also received a conditional discharge and had to pay £1,845.25 in costs. The ICO said, "Just because [someone] can access data that doesn't mean they should."

And a Leicester City Council employee was fined £160 plus £384.08 in costs and victim surcharge for a similar offence aimed at helping him to set up a new business.

I'm an independent specialist. Drawing on 25 years' experience of Data Protection in the voluntary sector I can deliver training, carry out audits, help to write policies and procedures, or give information on specific problems or questions.

However, I'm not a lawyer. The content of this paper may not be a complete or accurate statement of the law, and it is not intended to be legal advice.