OLIVIA WHITCROFT

"I often see jaws drop when I tell a business they need to speak about what they're planning to do"

The updated Bill covering data protection and digital information contains subtle changes that may have a big impact on how your firm does business

I've been holding off writing about the draft new data protection law in the expectation that it may be finalised soon. But I'm impatient, and it's been hanging around as a Bill for over a year now, so I can't wait any longer. Last year we had the "Data Protection and Digital Information Bill" (DPDI 1). This year, the "Data Protection and Digital Information (No. 2) Bill" (DPDI 2) appeared, largely copied across from DPDI 1.

The Bill makes amendments to the existing UK data protection regime under the UK GDPR and Data Protection Act 2018. Its aim (as stated in the Explanatory Notes) is to "update and simplify the UK's data protection framework with a view to reducing burdens on organisations while maintaining high data protection standards". Which I suppose can be interpreted as: "We want to put our Brexit stamp on UK data protection law, but we don't want to lose the adequacy status given to us by the EU."

Big changes afoot?

When I excitedly first read through DPDI 1 last year, I wanted to spot some headline changes to alert my clients about. It looked promising.

Article 30 – on "Records of processing activities" (commonly called ROPAs) – is being removed. This is a significant change. I have several smaller clients for whom maintaining ROPAs has slipped to the bottom of their to-do list; now they can remove it from their list completely. I read on. There will be a new Article 30A: "Records of processing of personal data." So ROPAs are to become ROPOPDs?

Undeterred, I moved on to the next proposal. Articles 37 to 39 are being deleted – no more data protection officers (DPOs). This is huge! What will become of all those people who have spent the last five years training and establishing themselves as DPOs? Not wanting to be caught out again, I checked for a new Article 37A. There was none. DPOs really are gone. But hang on: what are these new Articles 27A to 27C? A requirement for some organisations to appoint a "senior responsible individual". Oh.

I tried again to find my big news. Are data protection impact assessments (DPIAs, currently required for high risk processing activities) being scrapped? Nope, they're being renamed. And they didn't even bother to put in some new Articles. Instead, it's a find and replace: for "data protection impact assessment", substitute "assessment of high risk processing".

Come on, we must find something. Okay, this is definitely radical: the UK data protection regulator, the Information Commissioner's Office (ICO), is to be abolished! Will data protection law go unenforced? I wasn't convinced, and rightly so. There will be a new Information Commission (IC?) that will take on all the ICO's old responsibilities.

So my excitement quickly faded, as I sceptically pondered how long it took to come up with all this fancy relabelling.

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"I wanted to spot some changes to alert my clients about. It looked promising"

BELOW The UK is in the process of updating its data protection regime

Digging deeper

DPDI 2 is a 220-page Bill, and if you dig a little deeper there's lots more to get your teeth into. In fact, too much to fit into one *PC Pro* article, so I will be continuing my deliberations in a future issue.

The proposals picked out on my first read do make some changes to the substance of the rules. ROPOPDs and assessments of high risk processing are different to ROPAs and DPIAs, and the move from DPO to senior responsible individual makes a subtle change with a big impact. The structure of the IC will be different to that of the ICO, though the nature of the regulator's role remains fundamentally unchanged.

There are also refinements to the rules surrounding rights of data subjects. And specific examples of when you can rely on the "legitimate interests" lawful basis, and when use of data is "compatible" with the purposes of collection. The Bill also provides clarity over the interpretation of "scientific research", "historical research" and "statistical purposes", which are exceptions to many data protection rules. These updates could assist organisations in applying the relevant provisions.

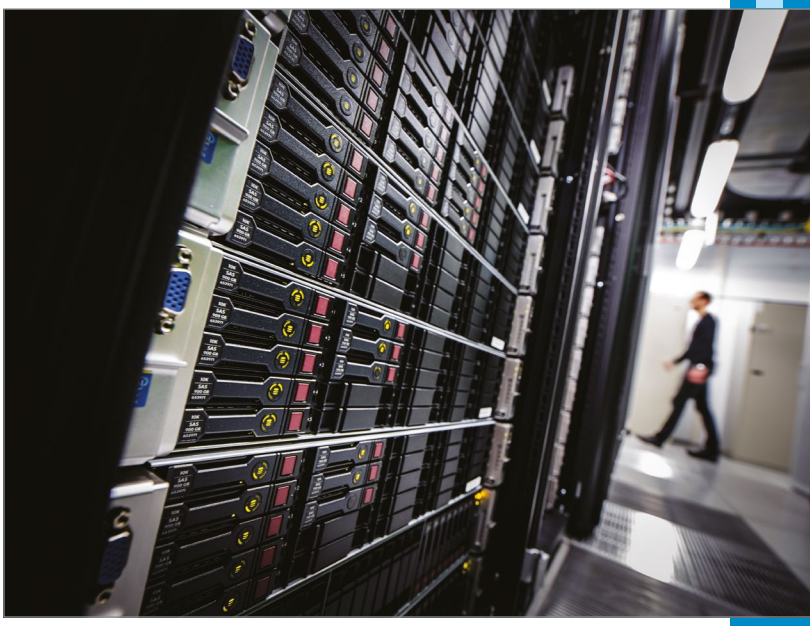
A new "data protection test" for international data transfers appears to embed transfer risk assessments. As well as standard contractual clauses (or other safeguards), organisations must ensure the transfer does not cause the protection of personal data to be materially lowered.

The Bill also provides long-awaited updates to laws on cookies and direct marketing (under the Privacy and Electronic Communications (EC Directive) Regulations 2003). These include new circumstances in which consent to the use of cookies is not required. There are also provisions on digital verification and smart data.

This article focuses on ROPOPDs, assessments of high risk processing and the role of senior responsible individuals, but I'll pick up again on some of the other points in a future article.

ROPOPDs

ROPOPDs will only be required for organisations carrying out high risk processing activities. I am unclear whether those organisations need to record all their activities, or just the high risk ones. The latter may not add much, if high



risk activities will be documented anyway as part of high risk assessments (as discussed below).

The required content for ROPOPDs is reduced, though some of this seems trivial. For example, you still need to record details of why and where you use data, and how you keep it secure, but you don't need to include the name of your organisation or the categories of data subjects.

Neither of these limitations – on who needs to have ROPOPDs and what needs to be in them – means that matters previously addressed within ROPAs disappear. As an example, the lawful basis for processing has never needed to be included in ROPAs. But organisations still need to identify and assess a basis (for example, whether the use of someone's data is *necessary* to perform a contract with them). The outcome should be recorded somewhere, and where's a good place to do this? You've got it: the ROPA.

As I raised earlier, I do have clients where formal ROPAs have not been a top priority. And this makes sense; surely individuals are more likely to suffer damage as a result of security failures in a system, than where the failure is that excellent security measures have not been recorded in a formal list? But, whether you conduct high risk processing or not, some record-keeping will be needed to keep track of your activities and compliance measures.

Assessments of high risk processing

Assessments of high risk processing are required in the same circumstances as DPIAs currently are: where the use of personal data is likely to result in a high risk for individuals. The IC must (continue to) publish a list of examples of high risk activities.

High risk assessments retain the fundamental elements of a DPIA, namely the need to assess and mitigate risks. But the list of defined steps has been cut back. Requirements to: (a) prepare a description of the processing; and (b) carry out an assessment of "necessity and proportionality", are being reduced to recording: (a) a summary of the purposes of the processing; and (b) an assessment of whether the processing is necessary for those purposes.

In practice, I think the broader DPIA steps will continue. As I often say to my clients (even pre-GDPR), it's impossible to assess and address the risks of an activity without an understanding of what that activity is. A summary of the purposes is unlikely to be enough; you need to map out what you're going to do with data throughout its lifecycle. The "necessity and proportionality" step has always been interpreted as linked to the data protection principles, and you still need to comply with these principles.

Another change is to remove the obligation to consult with data subjects. I often see jaws drop when I tell a business they actually need to speak with affected individuals about what they're planning to do. So this removal may be met with some relief. But it remains the case that data subjects can be an incredibly useful source of information. For example, if you want to know whether customers will understand what they are signing up to, is it better to sit alone in your office and guess, or might it be helpful to ask a selection of customers?

Senior responsible individuals

An organisation will need to have a senior responsible individual (SRI) if it's public sector, or carrying out high risk activities. This is clearer, though potentially wider, than for a DPO. The list of the SRI's tasks appears as you would expect: monitoring and overseeing compliance, organising training, dealing with breaches, and cooperating with the IC.

But here's something interesting, nestled in a new Article 27A(3)(a): the designated individual *must* be part of the organisation's senior management. Under current law, other tasks and duties of a DPO must not conflict with its DPO role, and EU guidance provides: "As a rule of thumb, conflicting positions within the organisation may include senior management positions…" So we're moving from "must *not* be senior management" to "*must* be senior management". I've talked to companies who struggle with this "no conflict" requirement, particularly SMEs who have limited choice in their selection of DPO. Some have looked to external independent DPOs to reduce the conflict risk. Under the Bill, organisations may need to change the person or the status of the person who takes on this role.

As a knock-on effect, for businesses with both UK and EU operations, the UK SRI may need to be a different person to the EU DPO.

ABOVE Companies will still need to record details of how data is kept secure

"Is it better to sit alone in your office and guess, or might it be helpful to ask?"

BELOW Under the new Bill, consent to the use of cookies is not always required

Are they big changes or not?

For organisations with a DPO, the move to an SRI needs careful thought, to meet seniority requirements and address conflict situations. And some companies that didn't need a DPO may now need to appoint an SRI.

I can see that the changes to ROPAs and DPIAs may provide some flexibility in approach. However, I'm not convinced these differences will (or should) lead to huge practical changes in a lot of cases. I have a concern that, with fewer formal documentation requirements, smaller organisations may revert back to thinking that data protection compliance is just about having a privacy notice, which can be prepared using a bog-standard template, or by copying what a competitor uses on its website. External-facing privacy notices incorporate a lot of behind-the-scenes assessments on all sorts of compliance matters. These should be recorded in line with principles of accountability and data protection by design. So if organisations already have well-established ROPA and DPIA procedures, they could choose to continue their existing approach.

Finally, an important question. I've been trying out the new acronym ROPOPDs throughout this article; do you think it will catch on?

olivia.whitcroft@obep.uk