Bird & Bird

Privacy Unpacked – Episode 1

Podcast transcript – A spotlight on UK data protection legal reform

Featuring Ruth Boardman (Partner and Co-head of Bird & Bird's International Privacy & Data Protection practice), James Moss (Partner and former Director of Legal Services (Regulatory Enforcement) at the ICO), and Emma Drake (Legal Director, International Privacy & Data Protection practice)

April 2023

Click or tap here to enter text.

Ruth Boardman:

Welcome to Privacy Unpacked from Bird & Bird. I'm Ruth Boardman, co-head of Bird & Bird's international privacy and data protection practice. In this podcast series, our team from around the world will share their insights on key issues and topical debates in the privacy world. Today, we will be looking at the recently relaunched UK reform of data protection law. We will be looking at the key points privacy professionals need to note, we will also look at timing and what happens next, and I am joined by two colleagues from London to guide us through the reform, Emma Drake who is a legal director here in London.

Emma Drake:

Hello.

Ruth Boardman:

And James Moss, who recently joined us as a partner from the ICO, where he was legal director of enforcement.

James Moss:

Hello.

Ruth Boardman:

So, privacy professionals may feel a sense of deja vu with this bill, we've already seen this once before in summer of 2022, so James, how come we've ended up back where we started?

James Moss:

Keen followers of UK reform will probably recall that a Data Protection and Digital Identities Bill was launched in the summer of 2022, in the dying days of the Boris Johnson administration, although the idea of the Bill survived, a new secretary of state arrived over the summer of political turmoil, and in the October, she announced a radical new approach, the tearing up of the GDPR. However, following a winter of soft consultation with industry, what has eventually reappeared is actually a very similar set of amendments to the one we originally saw last summer.

Emma Drake:

For anyone wanting to see just quite how little has changed since bill number one, they can have a quick look at the Keeling Schedules we have recently published, so for those who aren't parliamentary process gurus, a Keeling Schedule is a redline of the bill's affect against the legislation it seeks to amend, so against the Data Protection Act, against the GDPR or, I should say the UK GDPR, and Pecker, and we've flagged where practical what's new since the summer, which in short, is not a lot.

Ruth Boardman:

So let's turn to what the Bill does promise. To my mind, the area where organisations will see the biggest change is in accountability. Emma, what are the highlights there?

Emma Drake:

Well, what we don't have is a complete replacement or removal of the accountability obligations of the UK GDPR that we have today, what we do have are some targeted changes which allow the Government to point to some burning of red tape. The requirement to maintain a record of processing has been deleted, but replaced with a very similar obligation that only applies to controllers carrying out high risk processing, so that's a substantial relaxation, although it should be noted that the obligation to create that record of processing is not limited to just the high risk bit that you do, so if you have a high risk part of your business, all of your processing is caught by that obligation still. Data protection impact assessments have also had a rebrand, so these become assessments of high-risk processing, and the required contents of these documents look much less like the DPIA's that we know, and much more like a legitimate interest assessment, so less of the systematic description of processing, and more of assessing need and necessity of your purpose. Gone too is the requirement to consult the ICO, so where you have outstanding high-risk processing, this becomes an optional requirement.

Ruth Boardman:

So, what should we expect on data protection officers Emma, should UK DPOs be polishing their CV's now?

Emma Drake:

Well, this is one of the biggest shifts in approach being made, so the Government proposes to abolish the requirement to have a DPO in the UK, the article has been entirely deleted. This doesn't mean that there should be no individual responsible for privacy, so what they are introducing instead is a new role of senior responsible individual, and the key difference in approach to the EU is the level of involvement that this senior responsible individual should have in taking decisions about the processing, so the role of DPO as we understand it under the EU GDPR and in the UK GDPR until now, is one of an independent privacy guide to the senior voices in the business, but as the Court of Justice in the EU has emphasised, this cannot be an individual who takes processing decisions, the UK Government's new senior responsible individual, although they are given very similar tasks and responsibilities and employment protections as a DPO, is required to be a member of senior management, and that is defined as being an individual who plays a significant role in the making of decisions about how the whole or a substantial part of activities are to be managed or organised which sounds a lot like taking a position in processing decisions. A DPO of course reports to senior level, but it does appear even if the primary aim of the Government is to avoid some particularly small organisations the technical cost of having a DPO then that might well be an outcome, is that there is a divergence on this point of independence, I know clients will ask well, can I still be a DPO in the EU and be the senior responsible person in the UK, and I don't know what others think but I don't think so, but the senior responsible person is entitled to secure that another person in their organisation fulfils their list of tasks, so maybe an EU DPO can be the senior responsible person's best friend, and rely on the EU GDPR for their employer protections but, there you go. I suppose DPO's aside, the Bill also tries to make things easier for multi-nationals, it recognises the legitimate interest in intergroup data sharing and it removes the needs for UK representatives for unestablished entities, and there are a number of changes to data transfer rules but, I know you've looked at data transfer rules

more closely Ruth, will they save us from death by DTIA?

Ruth Boardman:

Well, I think all organisations are struggling with the requirements around international data transfers now, and here the Bill will definitely be helpful, although I think you can probably describe the changes as useful nudges or editing around the edges, rather than anything that would be more revolutionary. So first, if we look at transfer risk assessments, so here the Bill states that organisations should undertake a risk based and proportionate assessment, and I suspect many who are listening to this podcast will think hallelujah, risk based and proportionate sounds good to them. The Bill makes clear that the nature and volume of the data transferred can be considered, and also it makes clear that what is required is a holistic approach where overall you say 'are the standards of protection going to be materially lower than those that apply in the UK', so it is intended to be easier to manage for organisations perhaps than the equivalent EU test, and certainly for organisations whose transfer present a low risk, then there could be considerable scope to simplify transfer risk assessments for UK data. Secondly, the Bill introduces a rule making power for the secretary of state in this area, and the secretary of state is able to introduce additional transfer clauses or other safeguards which of themselves will meet the data protection test that exporters have to carry out, so just to unpack what that means, if the measures themselves completely meet the test then that means that there is no need to consider other safe guards, and if there's no need to consider other safeguards, then there will be no need to undertake a transfer risk assessment. Now this does sound really useful if there are measures that organisations can adapt without needing to do a transfer risk assessment, that would be great, as I said though, this is the rule making power, the bill doesn't actually do this, and as yet we don't know what these additional magic measures might be, but let's watch and see. Lastly, the Bill also amends and restates the way the UK should carry out assessments of other countries. Gone is the rather paternalistic or condescending adequacy test, and instead we have a data protection test designed to facilitate free-flows of data, again, the requirement is for a holistic assessment where the key test is where the standards will be materially lower than those in the UK, and interestingly the secretary of state can also consider the desirability of transfers of data to and from the UK, so a definite change in emphasis, although I should stress that looking at the desirability of transfers can't replace the need to consider whether the data protection test is met, now I just mentioned powers for the secretary of state to introduce further rules down the lines, and there are a number of other places where that pops up, James, do you want to share any thoughts on that?

James Moss:

Yes that's right, the Bill includes (as does the original Data Protection Act) a number of powers for the secretary of state to make changes to the law, but as yet we've not really seen a lot of that exercised, so it's more of a question of waiting to see how these powers are used and whether we do see that sooner rather than later.

Ruth Boardman:

Thanks James. I want to take you back to your former role at the ICO and look at some changes proposed there, the last time the Bill was introduced in Parliament, there was a lot of comment on proposed changes to the ICO's structure and remit and there was some discussion about whether or not this might undermine ICO's independence, and as a result affect the UK's adequacy status. Can you talk us through the proposed changes there?

James Moss:

Yes, absolutely. So, the headline news is that the information commissioner, that role, is being abolished and being replaced by a new body called the Information Commission. Now on first hearing that may sound quite radical, but actually it's less so than you might think from hearing that in short summary. In my view it's a sensible modernisation of the

ICO's structure, and it moves away from the now somewhat archaic Corporation Sole Model to something more akin to comparable regulators such as the CMA, the FCA, and Ofcom. So, in terms of detail, the Information Commission as it is proposed to be will consist of non-executive members led by the Chair, and executive members led by a chief executive who will in turn be appointed by the non-executive members. In addition to the Chair, who will be a crown appointee, as is the current commissioner on the recommendation of the secretary of state, the secretary of state may appoint other non-executive members and the commission can appoint one of the non-executive members as deputy to the chair. Executive members of the commission are in turn appointed by the non-executive members, so everything fits together in that way. There are, it's worth pointing out, saving provisions to ensure that the current commissioner will automatically become the first Chair of the commission for the remainder of the period of tenure in which they were appointed, so that ensures a smooth transition between the old and new regimes, so in simple terms, John Edwards who is currently the Information Commissioner, will become Chair of the Commission. The main change I would say is the greater role for the non-executive members than currently, and it moves away from the present model where effectively all the legal authority rests with the Commissioner and is delegated down on the commissioner's discretion alone, so these structural changes do not in themselves appear likely to cause issue in respect of UK adequacy I'd suggest, however some of the changes which will permit Government to have a greater say in the content of ICO guidance and the setting of the ICO's priorities may cause some issues in that regard. In the round, I think our view collectively is that the Bill remains sufficiently closely aligned to GDPR for adequacy to be maintained.

Ruth Boardman:

I think we all have a collective sigh of relief if that is going to be the case. Now, James, the Bill also proposes to give the ICO more powers. Can you share what those extra powers are going to be?

James Moss:

Yes, this is an interesting area and something which is run alongside the changes to structure which we were just talking about. So, at the moment the ICO already has significant powers in terms of investigation and enforcement, one of those is that it can compel organisations to provide the commissioner with information by serving of an information notice, but these powers have extended under the Bill to permit in addition the commission to require production of specific documents in addition to simply information, and that's new and no doubt stems from previous issues in that regard and that distinction. So that's the first thing I'd call out. The second thing is again the power that the Information Commissioner already has which is to conduct on-site assessments by way of assessment notices, albeit they can also be done remotely, and that did happen during the pandemic. So these powers are going to be expanded to permit the ICO to order the preparation of a report by an approved person, and to provide that report to the commission, and the commission have very wide ranging powers to dictate content, form, the required date of completion of that report, and bear in mind which is I'm sure going to be of interest, that the controller or a processor who is ordered to prepare this report must pay for it, so perhaps most significantly the commission will have a new power which doesn't exist currently at all to issue interview notices, where an individual can be called for interview either in their capacity as a controller or processor, or a present or past employee or manager of a controller or processor. So, there are some exemptions from having to answer questions, but essentially this power is a mandatory one and the commission can enforce compliance. There are some relatively limited exemptions which mainly involve privilege, and there are some protections against self-incrimination backed into the drafting, however these also have limitations and apply, it's worth baring in mind, only to the individuals who are being interviewed rather than the organisations that they are there to represent, and failure to comply with an interview notice or complying but providing false information, they themselves are offences which are

punishable by significant financial penalties in line with the existing penalties already set out under the Data Protection Act, so very strong powers of compulsion to require wide-ranging categories of people and individuals to come and speak to the commissioner and answer questions.

Emma Drake:

Well, having scared the audience with visions of being grilled in the gloomiest offices Wilmslow has to offer, do we have any better news on the Bill for those in riskier privacy positions?

Ruth Boardman:

I think I'll pick up that question Emma, and there is some good news in relation to cookies and e-privacy, so what does the Bill propose here? Well first of all, the rules on cookies are going to be adjusted. Low risk cookies will no longer need consent, and that's primarily going to benefit those who use analytics cookies. Secondly, the rules relating to email marketing by charities and political parties may benefit from some relaxation. At the moment, charities need opt-in consent in order to undertake any email marketing or other forms of outreach, that is going to be changed so that charities can do email marketing on an opt out basis like other commercial organisations, and as far as political parties go, and there is one of these rule making powers that would allow the secretary of state to exempt marketing for purposes of democratic engagement from the email and phone marketing rules in their entirety, however it's not all good news. At the moment, the current maximum fine for breach of these new privacy rules is £500,000, and the Bill will increase this in line with GDPR penalties, so most of these provisions will now be linked to a fine of 4% of worldwide turnover. Now of course, having an ability to impose a fine that high does not mean that ICO will do. James, in your brains from your former life, do you think ICO is likely to substantially change its approach when it can impose higher fines?

James Moss:

Well I think my instinct is yes, I think they will, and one of the reasons I say that is listeners may well recall we've been here before in fairly recent memory, when the maximum penalty for infringements of, at the time, GDPR and the Data Protection Act increased from $500,000 to that same 4% of global turnover or £17.5 million figure that the ICO is currently working with, and again, listeners may well recall that the ICO moved fairly swiftly from imposing penalties in the region of £500,000, to the region of tens of millions of pounds, so I would expect a similar trajectory for these types of matters, which is not to say that I'd expect fines in the magnitudes of tens of millions given the generally lower level of seriousness and the penalties we've seen to date in this area, but I do think there will be a substantial jump from the outset. The ICO will however be cautious of the likely increased pushback against higher fines, because the economic priorities of companies on the receiving end will inevitably shift, in any event the first few cases under this new regime will be very interesting, and we'll have to see how they play out.

Ruth Boardman:

Thanks James, I'm conscious that we're nearly at the end of the time we've allowed for this podcast. Before we wrap up, Emma, could you share your main takeaways from the Bill?

Emma Drake:

I guess we couldn't really ever expect there to be radical rewrites for the benefit of business in this Bill, not least for the adequacy reasons we've discussed but there does feel like there's a sense of missed opportunity. The initial consultation document which came out a couple of years ago now proposed some bigger changes, and has made a bit more of a difference, like cost caps on subject access requests, which in the UK really do create quite a problem for businesses, or raising the data breach reporting threshold. Neither of those have been taken up, someone taking a look at the redlines would assume there's quite a lot of change being proposed, but if

you look at them in detail in practice, the UK regime will feel mostly unchanged for most businesses, I think if anything there's a bit of a risk of some grumbling from some privacy lawyers about the amount of redline which will make it a little more tricky to navigate, although I'm sure they'll adjust. James, are you a bit more upbeat?

James Moss:

I think a bit, yes. I mean my main take away is that this is a relatively minor evolution rather than a revolution, and the political force has seemed at times to push towards a more radical shift away from the European position have not ultimately won out, and in my view that's certainly a good thing given the inevitable difficulties for business that significant regulatory divergence would have produced, leaving aside the potential jeopardy to the UK's adequacy position. That being said, some of the points we've picked out today do suggest a newly refreshed regulator with greater flexibility and with provisions supportive of the UK's pragmatic in this space approach, allowing them to focus more on the greatest harms rather than technical minutia, and of course greater investigatory powers, as I spoke to earlier, so that might also suggest greater appetite for enforcement.

Ruth Boardman:

That's super interesting, thank you both. That's all we have time for on the content of the Bill itself. Emma, can you get your crystal ball out and let us know what we can expect to happen next?

Emma Drake:

Assuming you pick up this podcast shortly after we publish it, then you will have just missed the second reading of the Bill. This took place on 17 April and it was the Bill's first proper parliamentary outing so, no major challenges raised from opposition parties, and frankly, we shouldn't really expect much challenge while the Bill is in the House of Commons, the Government have a large majority there and we'd expect few amendments to be accepted unless of course the Government introduces them itself. There may be more change when the Bill gets to the House of Lords, after all, the Age-appropriate Design Code which was held up is a shining light of the existing Data Protection Act by various MPs at second reading, was born in the Lords back in 2017, with the activism of the Independent Baroness Kidron, but we shouldn't expect the Bill to get to the Lords this parliamentary session. The Bill is scheduled, so it might finish it's common stages before the summer recess, so committee is required to complete by late June. The Bill Team have secured permission to hold the Bill over to the new session in the Autumn, and we should expect that so happen so, with a good wind, the Lord's stage is then ping pong, which is a genuine technical term for the battle between houses on any amendment, might be done by the end of the year. But delay in the Lords or difficulty slotting into the busy parliamentary schedule and we all might be held up until 2024.

Ruth Boardman:

Thanks Emma. And thanks for joining us today, in this quick run through the UK's data protection reform. If you want to know more about the points that we've discussed, we've prepared a detailed article on the changes introduced by the Bill. You can find this in the IAPP's Privacy Advisor, or, on the Two Birds Website or LinkedIn page. This also covers changes that we've not discussed today, so changes to purpose limitation, to the rules on the use of data for research, on solely automated decision making, and some edits to processing with the purposes of legitimate interests. We hope you've found this episode of Privacy Unpacked useful. If you have a question for any of our team, or a suggestion for a future episode, please do get in touch. We look forward to you joining us again soon.

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw