Slaughter and May Podcast

Investigations and enforcement outlook 2021: Data breach and ICO

Jonathan Cotton	Welcome to the first instalment in the Slaughter and May podcast series, discussing the outlook for data breach enforcement in 2021. I'm Jonny Cotton, a partner in the disputes and investigations group here and co-head of our global investigations group.
Richard Jeens	I'm Richard Jeens, also a partner in our disputes and investigations group but with a particular focus on contentious data matters, including cyber or other data breaches and the regulatory enforcement and claims that so often follow.
Rebecca Cousin	I'm Rebecca Cousin, a partner in our corporate and commercial group and co-head of our data privacy practice and part of our cyber advisory team.
Jonathan Cotton	So today we'll be focussing on the increased enforcement risks associated with data breaches of all kinds, data protection legislation and privacy legislation, including the developing area of follow on civil litigation for damages. Rebecca and Richard, could you spend a minute setting the scene for us, in terms of the recent changes to the applicable regulatory regime?
Rebecca Cousin	Of course. From a global perspective, a key change is the increase in jurisdictions that have comprehensive data privacy legislation, with many adopting the approaches taken in the EU's General Data Protection Regulation, the GDPR, and a significant number of those regimes have real teeth in terms of the sanctions that can be imposed. Turning a bit closer to home, and the implications of Brexit, the EU GDPR was written into UK law with effect from the start of this year, effectively creating a UK GDPR, which is nearly identical in substance and form to the EU version that we are all used to.
Richard Jeens	And that of course means that as well as the usual eye on the global risk, some businesses will become subject to both GDPRs because they will have establishments in the EU and UK or because they are established in one and caught by the extra-territorial provisions of the other. So for instance, a UK company that offers goods to consumers in France will be subject to both regimes. Additionally, the EU GDPR will continue to apply to personal data of non-UK persons that was processed during the Brexit transition period unless and until the EU concludes that the UK's regime provides an adequate level of protection. There is therefore a risk of being fined twice - by the Information Commissioner's Office in the UK and the relevant EU enforcement authority for the same breach of the relevant data privacy rules.
Jonathan Cotton	Ok that's interesting, but I suppose it's no different from those dual risks that many businesses already face, where they could be fined or investigated at least for misconduct by both US or UK authorities or UK or EU authorities for the same conduct. So as with other regulatory issues, data privacy risks need to account for both the 'local' regulatory concerns and the relevant organisation's 'global' footprint.

Jonathan Cotton	Given that, can you talk to us about what you've learned from the past couple years of GDPR enforcement, that what impact that might have on the direction of travel for 2021 and beyond?
Rebecca Cousin	Sure. The first thing one notices when looking at enforcement trends across the EU is the divergence in the number of fines with regulators in Spain, Romania, Italy, Hungry and Germany topping the list. I saw a headline a few months back suggesting that companies in these countries were therefore less compliant but that's of course, a misinterpretation. It's just that the regulators in these countries have a strategy of taking formal enforcement action in more circumstances. Some other regulators carrying out a significant number of investigations but prefer not to always issue fines, whilst some regulators are genuinely less active. To illustrate the different approaches, we recently advised on the impact of a data incident that came to light in due diligence on a potential acquisition of a Swedish company. If that incident had taken place in a different country we would have expected an investigation and potentially enforcement action. However, the Swedish data protection authority doesn't undertake many investigations and it closed the case without asking any questions at all.
Richard Jeens	Interesting. By comparison, two of the ongoing ICO investigations on which we are engaged on have given rise to extensive questioning and in one case, there were real tensions between what our clients are being asked to provide to the ICO and what they feel comfortable providing to M&A bidders or other key contractual counterparts. One point here that has helped is the growing ability to anticipate the sort of questions the ICO may raise and so we can therefore help clients prioritise their response to an incident or, better, their pre-incident preparation.
Rebecca Cousin	Yes that makes sense. There's also a real divergence in the level of fines between regulators and you'll recall the GDPR allows regulators to impose fines of up to the higher of €20 million or 4% of annual worldwide turnover. The highest fine is still France's fine of Google for €50 million for transparency failings and not having a legal processing ground. However, last October there was another sizeable fine, this time from the Hamburg data protection authority, one of the German state regulators. This was a fine of €35 million of H&M Germany for the monitoring of hundreds of employees.
Richard Jeens	And I think it's fair to say that the UK data protection authority is also up there in terms of the quantum of its recent fines. British Airways were fined £20 million and Marriott International £18.4 million, in both cases for security breaches involving third party hacks rather than for the actual activities that they were taking as data controllers. However what has been striking and well reported is that in both those cases the final fines were significantly lower than the initial fines suggested by the ICO (in part as a result of the pandemic) – where the ICO had initially issued an intention to fine BA £183 million and Marriott £99 million.
Rebecca Cousin	I think given all of this, looking ahead, one of the hardest things to predict is the likely level of fine for a particular breach given the inconsistency between regulators to date. The enforcement decisions don't provide specific details and it is not always possible to work out which financial data has been used in terms of the percentage. But if you look at the larger fines, then you can see that the percentage of turnover is

	tiny – for BA its 0.15% and for Google an even smaller 0.13%., with the highest reported percentage having been 2% against a small Danish taxi firm. However, the Norwegian regulator has recently announced an intention to fine Grindr a fine equating to 10% of its turnover in respect of data sharing with advertisers. Now this is not a final decision, so it will be interesting to see whether the ultimate fine is reduced just as Richard mentioned happened with BA and Marriot in the UK.
Richard Jeens	So taking together that makes it pretty tricky for organisations to know where to start. In the UK at least, the starting point in calculating the percentage fine is set out in a matrix reflecting on the one hand the seriousness of the breach and on the other the degree of culpability of the relevant organisation. That's then adjusted to reflect any aggravating or mitigating factors for the particular incident or behaviour. This will then be compared with the company's financial means and the impact that fine might have on it, as well as reflecting from a sort of policy perspective how effective, proportionate and dissuasive the fine would be. Looking ahead though, there is growing debate in the UK as to whether this % of turnover is (or should be) the starting point for fines or should apply as a cap, with the actual fine set by the facts of the particular incident. At the moment, the ICO seems set to go with the former but I think this is likely to be an area for further disputes, particularly where fines would have a disproportionate impact on a business or their operations or indeed act as a deterrent for other businesses in the same sector. I think that's particularly going to be the case where you're a low margin business or a low margin sector where the percentage of fine may wipe out your profits for many years, or indeed just drive up costs so in an outsourcing business would the data risk premium be passed on to customers?
Rebecca Cousin	There is actually a similar debate in Germany since the regulators there also have a fining model that has the businesses' revenue as its starting point. This appears to have led to higher fines being imposed which in turn has led to more court challenges on the level of the fines, some of which have been successful. If the ICO's criteria does lead to higher fines, we can also expect there to be greater challenge to these in future.
Jonathan Cotton	Fantastic, thank you. I mentioned at the beginning the risk of civil litigation follow-on claims, could I ask you to conclude the session by briefly giving us your thoughts on those matters?
Richard Jeens	Sure, I mean look, you are absolutely right because I think that there has certainly been a rise in civil litigation and as with the increased regulatory fines that absolutely is something that businesses take account of in their risk profile. I think there are three key themes driving this increase in civil litigation. First, is that there are clearer rights to bring civil claims under relevant data privacy rules and coupled with that is an awareness of those rights and that applies particularly where there is an absence of enforcement action being brought by a data protection authority. I think in that regard we can all remember those consent emails that came round when GDPR, which is effectively one of the most brilliant advertising campaigns for 'you must know your rights' from a data privacy claims perspective.
Rebecca Cousin	And just to add to that, we're definitely seeing an increasing number of claims being brought as collective actions, where a whole class or group of affected individuals are

	part of the claim – so increasing the amount of overall damages that is being claimed. The ability to bring mass claims varies among the EU states, with most still only having ‘opt in’ claims (where the group of claimants needs to be built up by the funders or claimant firms) but changes in both the Netherlands and United Kingdom mean that ‘opt out’ claims (where whole groups of claimants are automatically ‘in’) are increasingly available.
Richard Jeens	And I think that leads neatly to the third key theme here in the rise of civil litigation, which is litigation funding. Whilst familiar in many jurisdictions, not least for the follow on claims we see for other regulatory enforcement action (e.g. anti-trust cartels or similar), these are the organisations who will pay the cost of the litigation on the basis that they will then get a sizeable portion of the awarded damages, often 30% or more. Subject only to the increased risk for funders arising from a loser-pays cost-shifting rules, the increasing quantum available in data-related claims (which is often established in ‘one-off’ cases, such as the UK phone-hacking scandals or a particularly salacious celebrity gossip case) it means there is a veritable wall of money out there waiting to fund data-related civil claims.
Jonathan Cotton	Thank you, Rebecca and Richard, for the interesting discussion. For those of you who are listening, if you have any questions or would think you’d benefit from further discussion, please do not hesitate to contact any of today’s participants. We hope to see you again for our next session in this series, where we’ll be discussing 2021’s outlook for corporate crime.

End of podcast