CITY OF LONDON LAW SOCIETY DATA LAW COMMITTEE (THE "COMMITTEE")

Minutes of the Committee meeting held at 8.30am on 5 February 2019 at the offices of White & Case LLP, 5 Old Broad Street, London, EC2N 1DW (the "Meeting")

Present:	Jon Bartley, RPC LLP, Chair
	Elizabeth Robertson, Skadden, Arps, Slate, Meagher & Flom LLP
	Kevin Hart, City of London Law Society
	Tim Hickman, White & Case LLP
	Kate Brimsted, Bryan Cave Leighton Paisner LLP
	Ross McKean, DLA Piper (UK) LLP
	Jonathan Kirsop, Stephenson Harwood LLP
	Giles Pratt, Freshfields Bruckhaus Deringer LLP (by dial in)
	Rhiannon Webster, DAC Beachcroft LLP
	Miriam Everett, Herbert Smith Freehills
	Luke Dixon, Addleshaw Goddard
	Rebecca Cousin, Slaughter and May
	Barry Fishley, Weil, Gotshal & Manges (London) LLP
Apologies:	Sam De Silva, CMS Cameron McKenna Nabarro Olswang LLP
	Cynthia O'Donoghue, Reed Smith LLP
	Jonathan McDonald, Charles Russell Speechly LLP

---

1. Welcome

The Chair welcomed all in attendance to the fourth meeting of the Committee.

2. Apologies

Formal apologies were received from Sam De Silva, Cynthia O'Donoghue and Jonathan McDonald.

3. Minutes approved – no comments

The minutes from the previous meeting of the Committee were tabled and approved.

4. Discussion of Committee's first two submissions

4.1 The Chair thanked Rebecca Cousin for coordinating the previous submissions to the ICO and asked members of the Committee for comments on the process and suggestions for improvements. Ross McKean suggested that going forward, it would be useful to include a section of 'Key Highlights' as a summary of the suggestions put forward.

5. Follow up points arising from previous meeting

5.1 The Chair reminded the Committee of the proposal to appoint a Committee Secretary that could be an associate of a Committee member. The Chair suggested that Committee members send names of any associates to be considered for this role to him.

5.2 The Chair asked Tim Hickman if he had heard of any interest from the Cabinet Office to engage with the Committee. Tim Hickman said he had followed up with the Cabinet Office who had said that their priorities lay elsewhere at present, due to Brexit.

6. Fines under the GDPR

6.1 Miriam Everett explained that she had spoken to a representative of the Belgian DPA about the calculation of fines and was told there was still no clear system in place. Ross McKean pointed out that there was some interesting commentary from Germany on fines, which said it would be unlawful for DPAs to look at group revenue when assessing fines. Instead, only the revenue of the entity in question is relevant. Ross McKean suggested that given the current dearth of policy, this Committee could share ideas and produce guidance instead of waiting for a regulator to do so. There was general support for this proposal.

7. One stop shop under the GDPR

7.1 Miriam Everett noted that the one-stop-shop ("**OSS**") is a big concern for many of her clients. Tim Hickman pointed out that CNIL's recent imposition of a €50 million fine showed that US technology companies that have established themselves in Ireland are concerned about the risk that the OSS offers no real protection against the risk that a DPA in another Member State (in this case France) decides to take enforcement action on the basis that it does not believe that real decision-making power sits in Ireland. He also said that a significant outstanding question is whether the OSS principles will be applied in practice, or whether DPAs will ride roughshod over those principles when it suits them.

7.2 Jonathan Kirsop noted that the CNIL's approach could mean that any DPA could impose fines against a company with operations across the EU. Tim Hickman added that it was also likely that multiple DPAs could impose fines on such a company once a breach was established. Miriam Everett commented that if large companies felt they were under attack from multiple regulators, they might decide to start focusing on the OSS principle.

7.3 Tim Hickman noted that it would be interesting to see how quickly DPAs would begin to take enforcement action against companies outside the technology sector, as currently many companies in other sectors do not seem to believe that the GDPR will ever be enforced against them.

8. Cookies

8.1 The Chair raised the issue of cookie notices on websites achieving the right balance between intrusiveness and necessity. He mentioned it would be helpful to have guidance on cookie policies.

8.2 Ross McKean noted that he had seen larger cookie banners and opt-out notices, but not a fundamental shift towards granular cookie controls. He also raised the point that inadvertent antitrust issues might arise out of privacy requirements, due to the limited

number of companies that exercise significant control over a large portion of the online advertising market.

8.3 Tim Hickman noted that there is a tension between: (i) the existing WP29 guidance[1] which permits website operators to obtain consent as a prior condition to the provision of a website or other service; and (ii) Article 7(4) GDPR, which indicates that any consent obtained in this manner may not be "freely given" (and may therefore be invalid). This tension appears to stem from the fact that the consents cover different activities (setting of cookies versus processing of personal data) but is not helped by the fact that the ePrivacy Directive imports the standard of consent in the GDPR.[2] Ross McKean discussed the fact that there are reasonable arguments for overcoming the presumption in Article 7(4) that such consent is not freely given. It was generally agreed that clarity from DPAs on this point would be helpful.

8.4 The Chair suggested that one possible approach could be to provide a cookie-category choice instead of a cookie-by-cookie choice for users to opt-into or switch off on a 'dashboard'. However, Miriam Everett noted that this would make the notice too technical and difficult for a lay person to comprehend. Rebecca Cousin also agreed the conflict between transparency and comprehensibility of cookie notices was a challenge.

8.5 Tim Hickman added that clients are increasingly experiencing attacks on social media (often from individuals seeking to make a name for themselves in data protection) alleging that clients have failed to implement proper data protection or cookie compliance mechanisms. These attacks can be very difficult to resolve positively.

9. Codes of conduct

9.1 Kevin Hart suggested reaching out to the Institute of Government and working with them on questions around codes of conduct. Tim Hickman noted that there is a gap between Article 40 GDPR (which sets out the rules for codes of conduct) and Article 41 GDPR (which states that codes of conduct "may" – not "must" – be monitored by an accredited body). Tim Hickman reported that the Irish DPA has said the objective of Article 41 was to reduce the work of DPAs, and therefore there must be an accredited body, regardless of the wording of the GDPR. However, the Belgian DPA has given a preliminary view that the GDPR cannot be read in this way, and that Article 41(1) does not create an obligation to appoint an accredited body. The preparation of EDPB guidance on codes of conduct is being led by the Irish DPA, but at present there is no indication on timing.

9.2 The Committee also discussed how it would be possible to satisfy the requirement in Article 41 of an accredited body being independent, while being funded by the organisations that sign up to the code of conduct. One of the main concerns discussed was that if the monitoring body fails to ensure compliance with codes of conduct, it will potentially be subject to fines under the GDPR, which may be difficult to insure. Ross McKean suggested appointing one person on the Committee who is independent.

9.3 The Chair observed that some clients are seeing codes of conduct as a silver bullet.

[1] See WP208, which states that, provided that users are "fully informed", their consent can be inferred from the user's "active behaviour" that indicates consent, such as dismissing a cookie banner.

[2] See Article 2(f) of Directive 2002/58/EC, and Article 94(2) of Regulation (EU) 2016/679.

10. Artificial intelligence

10.1 Rhiannon Webster informed the Committee that the ICO had commissioned a citizens jury asking them how to explain AI. The Committee discussed the difficulty of explaining AI to the public and the further challenge of regulating bias in AI. The Committee also discussed whether it would be better for the public to explain AI or ask individuals who have an interest to provide explanations. Ross McKean and the Chair raised the point that one of the fundamental challenges of this exercise was difficulty in providing explanations as to how an algorithm worked and made decisions in an AI context.

11. Data breaches

11.1 Tim Hickman asked whether anyone had heard from the ICO regarding data breaches. The Chair said that the ICO had on some occasions, responded within a week. Ross McKean said that often the ICO responded asking his clients for more information on the data breach. Rhiannon Webster confirmed that she too had had a few relatively quick responses from the ICO.

11.2 Ross McKean pointed out that a long wait for a response from the ICO did not necessarily mean the client was in the clear. The ICO could take months to respond before asking for further information. He also noted the ICO was keen to close files especially if the breaches do not relate to companies which handle large volumes of personal data.

11.3 Rhiannon Webster further commented that in cases relating to doctors and other professions which are subject to confidentiality requirements, the ICO had mentioned certain breaches were not notifiable. Miriam Everett said that she had attended a seminar recently where the ICO mentioned there was a significant level of over-notification.

11.4 Ross McKean said DLA Piper had published a report on data breach notifications, which showed that the highest level of reporting was in the Netherlands, but other Member States have seen markedly lower levels of reporting.

11.5 The Chair noted that data breach notifications were mainly made online but a small proportion were also made over the telephone. Miriam Everett added that telephone conversations should not be treated as informal communications and would be treated by the ICO as a formal notification.

11.6 Ross McKean suggested that the 72-hour notification requirement was not as important as getting the information right when reporting and the incremental harm of waiting a week to have a better understanding of the data breach rather than notifying within 72 hours was likely to be marginal. He also pointed to the US, where the introduction of reporting obligations in some states had seen a spike in notifications followed by a gradual tailing off, as organisations became increasingly wary of over-notification. Miriam Everett agreed that it was likely the high volume of notifications would eventually fall.

11.7 The Chair pointed out that notifying data subjects is a challenge for many clients because of the risk of causing distress. He said individuals tend to panic and are likely to assume any future issues could be traced back to a breach notification.

11.8 The Chair raised the fact that an increasing number of ambulance chasing law firms have emerged, and are encouraging individuals to sue for data breaches. Miriam

Everett said it would be interesting to understand if individuals were getting more or less distressed in light of the increasing notifications. Ross McKean said that his firm have begun offering credit monitoring and fraud monitoring services and noted that the take up was very low.

12. Insurability against fines

12.1 The Committee briefly discussed the potential for the insurability and recoverability of fines. Miriam Everett said that organisations in the EU appear to believe that they are not able to insure against a fine by a regulatory authority. Ross McKean pointed to commentary in the US, where some analysis on the insurability and recoverability of direct liability and vicarious liability has been carried out, with an indication that it may be easier in some cases to obtain insurance coverage for vicarious liability. It remains to be seen how this will play out in Europe.

13. Brexit developments

13.1 Jonathan Kirsop mentioned that his firm was debating incorporating Standard Contractual Clauses ("**SCCs**") in its template engagement letter as part of preparations for Brexit and asked if anyone in the Committee had undertaken something similar. Rebecca Cousin confirmed that her firm had incorporated proactive terms in its engagement letters. Ross McKean said that banks were beginning to do this reactively. The Committee also discussed the possibility of a hard Brexit. If the UK did not pay the "divorce bill", it was possible that there could be an increase in fines or measures put in place by DPAs to make it difficult for information to flow from the EU to the UK. Miriam Everett pointed out that it would not take too long to put SCCs in place to ensure smooth information flow, where needed.

14. General discussion and other developments

14.1 The Chair asked if there was anything else Committee members had seen from the ICO to which the Committee could make a contribution.

14.2 Rhiannon Webster mentioned that Committee members are welcome to send through comments to the ICO regarding joint controllership. The Committee discussed this topic briefly. Rhiannon Webster explained the ICO's view that it is not possible to be a processor and controller of the same data unless the organisation separated its systems. It was agreed that further clarity on this topic would be welcomed.

15. AOB

15.1 There was no other business to be discussed by the Committee and the Meeting was closed.