

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

**Meeting Date** 9 February 2023 at 9.30am

**Location** Ashurst Office and Virtual Meeting Room

**Present** Jon Bartley (RPC)  
Cynthia O'Donoghue (Reed Smith LLP)  
Kate Brimsted (Bryan Cave Leighton Paisner LLP)  
Rebecca Cousin, (Slaughter and May)  
Luke Dixon (Freeths LLP)  
Barry Fishley (Weil, Gotshal & Manges LLP)  
Kevin Hart (CLLS)  
Tim Hickman (White & Case LLP)  
Jonathan Kirsop (Pinsent Masons)  
Jade Kowalski (DAC Beachcroft LLP) (left at 10am)  
Ross McKean, (DLA Piper LLP)  
Jonathan McDonald (Charles Russel Speechlys)  
Rhiannon Webster (Ashurst LLP)  
Eve-Christie Vermynck (Skadden, Arps, Slate, Meagher & Flom LLP)

Guest minute taker: Shehana Cameron-Perera (Ashurst)

**1. Apologies**

Sam De Silva and Giles Pratt sent apologies ahead of the meeting.

**2. Welcome**

The Chair welcomed all those in attendance at the meeting, acknowledging this was the second in person meeting since Covid.

**3. Previous minutes and agenda**

It was reported that draft minutes from the previous meeting held on 23 September had been circulated and would be published. No agenda had been circulated for this meeting.

**4. Update on event with the Information Commissioner**

4.1 The Committee discussed the event with John Edwards (UK Information Commissioner) that CMS hosted at their London office on 18 January 2023 and which c. 170 people attended. CMS was thanked for organising and everyone was in agreement that it was a great event. A note of the event (which had been approved by the Information Commissioner's private secretary) would be circulated in due course.

4.2 The Committee agreed that the Information Commissioner was forthcoming and pragmatic and focused on (i) producing more guidance; and (ii) key harms rather than penalising organisations for technical breaches of accountability (e.g., lack of a ROPA). It was agreed that this would be a welcome message for the Committee's clients and was helpful to understand the ICO's focus.

4.3 It was noted that only 43% of organisations/people had been using the TRA Tool – the Information Commissioner was surprised by lack of take-up.

4.4 The Committee discussed the ICO proposal of "submitting a request for a binding decision"; which would in essence enable an organisation to rely on a letter of comfort about an approach on a matter of data protection. This was the model in New Zealand and the Committee agreed that it would be helpful in theory but would depend on the ICO's resource and how the publication of comments from the ICO's review of such requests would work in practice. The

Committee could anticipate such a model being inundated by SMEs and discussed the impact of associated delays on organisations.

- 4.5 The Committee agreed that this event had successfully built engagement with the ICO and that it should look to build on such momentum by considering future events or opportunities for future engagement. The Committee was invited to identify such opportunities, in particular any groups that it could introduce to the ICO such as the Federation of small businesses. It was finally noted that ICO stakeholders could be booked to speak at future corporate events.

## **5. Future events**

Following the event with the Information Commissioner, the Committee agreed that future annual events with external speakers should be arranged, particularly to give juniors the opportunity to network. It was agreed that this should be scheduled for Data Privacy Day in 2024 on 1 February 2024. Rhiannon offered to organise this at Ashurst London offices.

## **6. ICO's approach to data breaches**

- 6.1 The Committee discussed its experience with the ICO in respect of data breaches. The Committee Members discussed the challenges with assessment of likelihood of harm and the consideration of whether unduly worrying data subjects by notifying them could cause more alarm and distress. Some Committee Members were of the view that this was not a factor that was taken into consideration by the ICO (who seemed to take the view that any risk of harm should be notified) and that the ICO was becoming more conservative and aggressive in its approach to data breaches; perhaps due to cross-regulatory co-operation with bodies such as the NCIS and ENISA which predominantly focussed on severity.
- 6.2 A need for further guidance on likelihood of harms was expressed; in particular for (i) examples of circumstances which were considered to be a grey area for notification; and (ii) more guidance on how organisations can make a judgment of whether to notify. It was agreed that it would be most helpful if this guidance could be obtained from a forensic specialist who could advise on likely consequences of breach and likely exploitation of such data. Such insight would be useful in making a more informed assessment of harm and risk to individuals.
- 6.3 It was noted that notwithstanding the above, that there would be (i) more reason to notify data subjects if they could take a proactive step to protect themselves e.g., change a password; and (ii) as per EDPB guidance, less of a reason to notify either regulators or data subjects if the data had been sent to a trusted person (as the data had been contained).
- 6.4 It was acknowledged that in light of the ICO's recent decision to publish data breach notifications, this would likely increase potential mass claims, and this would likely factor, in some form, into consideration for breach notification.

## **7. DSIT**

A new government Department for Science, Innovation and Technology (DSIT) was established in February 2023 and it appeared to have a wide scope. It was assumed that previous individuals in government who had been dedicated to data protection policy would move across to DSIT for continuity purposes but that it would inevitably have some impact/disruption. The Committee hoped that the creation of DSIT would mean that data protection would gain more prominence.

## **8. Data Protection and Digital Information Bill (the "Bill")**

- 8.1 A new version of the Bill was intended to be published before Summer. It would not go through another consultation as various bodies had already been involved and provided feedback.
- 8.2 DSIT had requested examples from the Business Advisory Group of anticipated problems/grey areas/nuances which could be clarified in the next version of the Bill. Committee Members were invited to provide any examples which could be relayed back to the Business Advisory Group.

- 8.3 It was still unclear what impact the next version of the Bill would have on:
- 8.3.1 the UK's adequacy determination, particularly as it was noted that the Bill was creating its own standard for UK Adequacy regulations which was materially different to the European Commission's; and
  - 8.3.2 DSARs, particularly as the Information Commissioner, from the event with him, was focussed on DSARs being a fundamental right, irrespective of motivation/use of DSARs as a tactical approach or to circumvent disclosure.

## **9. DSARs**

The Committee discussed the recent decision from the CJEU (which was put forward by the Austrian Supreme Court) that in a DSAR, controllers must provide the data subject with the identity of recipients to whom his or her personal data had been disclosed. The Committee agreed that this decision was very problematic and would have confidentiality implications.

## **10. Data transfers**

The Committee exchanged various comments about data transfers, namely:

- 10.1.1 The finding of MI5's unlawful collection and use of bulk surveillance warrants was interesting and arguably not dissimilar to US practices;
- 10.1.2 Discussions around the nature of the US Executive Order and that it was not fully binding on all surveillance committees at present as they had a year to change their policies etc. Therefore, some Committee members took the view that the Executive Order could not change the outcome/risk assessment in TIAs or that a conservative approach should be taken when considering TIAs of transfers to the US; and
- 10.1.3 It was noted that the Spanish data protection regulator took a more proportionate view to Google Analytics (as it found that the use of Google Analytics did not breach data protection laws and rejected NYOB's complaints) as configuration/use of newer versions of Google Analytics was taken into account.

## **11. Cookies**

- 11.1 The Committee briefly discussed what impact generative AI such as ChatGPT could have on cookies and online services that benefit from use of cookies etc.
- 11.2 A view was expressed that the consent model for use of most cookies was challenging and could not work in practice as individuals could not meaningfully give consent. It was considered whether changes to the model would be dictated by market forces rather than legislation.

## **12. AOB**

### **12.1 CLLS**

It was noted that CLLS will have: (i) a new chair, Colin Passmore of Simmons and Simmons and he would join a Data Law Committee meeting in due course; and (ii) two new specialist ESG and arbitration law committees.

### **12.2 *Summer Social***

The Committee agreed that a summer social should be organised.

### **12.3 *Upcoming meetings***

The next Committee meeting will be held on 11 May 2023.