GDPR Issue Committee Meeting 11

8th January 2018| 10:30 – 12:00
By teleconference

Status of the Minutes: Final

MEMBERS PRESENT

Helyn Mensah	HM	Chair	Hugh Laurie	HL	Committee Member (Wholesaler)
Louise Fox	LF	Committee Member (Retailer)	Nick Rutherford	NR	Committee Member (Wholesaler)
Caroline Gould	CG	Committee Member (Wholesaler)	Maureen Wilkinson	MW	Committee Member (Retailer)
Gillian Hill	GH	Committee Members (Retailer)			

OTHER ATTENDEES

Adam Richardson	Panel Secretary (MOSL)

APOLOGIES

James Gilbert	Committee Member (Wholesaler)
Sally Marshall	Committee Member (Retailer)

1. Welcome and Introductions

Purpose: For Information

1.1. The Chair welcomed everyone to meeting 11 of the GDPR Issues Committee.

1.2. It was noted that this meeting has been called following concerns raised by a sub-group of Panel Members in relation to MAC Schedule 13, section E, clause 1.2 of the drafting as recommended to the Panel by the GDPR Issues Committee.

2. Committee Discussion

Purpose: For Discussion

2.1. The Committee noted that a Panel sub-group ('PSG') had met on Monday 18 December to consider these matters. The concerns related to the last part of this clause, which required that technical and organisational security measures must be "consistent with or equivalent to industry standards, best practices and frameworks".

2.2. The Chair thanked Committee Members for providing their views ahead of the meeting on the concerns set out in the ex-committee note of 19 December 2017. Members observed that this note also proposed amended drafting that had been considered by the Panel sub-group.

2.3. The Chair invited Members to raise any further comments.

2.4. One Committee Member expressed concern regarding any reference to best practices, suggesting this implied high standard over and above that required for compliance with the General Data Protection Regulation (GDPR). They felt this was too vague and cautioned against drafting which could be interpreted in multiple ways.

2.5. Another Member was concerned that if the last part of the clause was removed entirely then the drafting was back to square one as a data sharing agreement for mutual assurance. They acknowledged that 'frameworks' alone may not be specific enough and agreed this could make interpretation hard to manage.

2.6. The Chair referenced the language used in the Information Commissioners Office (ICO) Code of Conduct on Data Sharing which is a statutory requirement. The Committee noted that this code of conduct indicates: "It is good practice to take reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement."

2.7. A Member felt Parties would look to MOSL for advice on what the code drafting meant if it was ambiguous. Another Member agreed that there was a need to be specific as the code drafting was the vehicle for outlining the data sharing arrangement.

2.8. One Member confirmed they were happy with the original text as recommended to the Panel. In their view, it allowed for some consideration within the scope of an audit that took account of the various companies' size and shape.

2.9. The Chair reminded Members that there was a balance to be struck between light touch and prescription in the drafting while remaining mindful that the requirements must offer mutual

assurance between data controllers. It was noted that, in this context, there remained a need for an objective benchmark.

2.10. The Committee noted that, while every company was different, smaller Trading Parties have access to the same information as larger Trading Parties via the central system so all Trading Parties face the same risk. The data sharing arrangement needed to ensure there was no weak link in the chain.

2.11. One Committee Member re-iterated concern on the ambiguous nature of references to 'best practice' and 'frameworks'. They felt there may be a middle ground offered by citing examples of what to take account of. In their view it would be possible to require Parties to have considered, or have given due consideration of specific ICO guidance or other standards.

2.12. The Chair queried whether the Committee felt the standards that were referenced in the existing drafting related to standards for the water industry (e.g. Water UK guidance on cyber security) or the IT industry. There were diverging views across the Committee Members on this point.

2.13. The Committee reached a consensus that removing the wording in clause 1.2(a) (after the words "Data Protection Laws"), without providing any alternative, would remove means of objective benchmarking and lead to difficulties in demonstrating compliance to the ICO, that due and proper consideration and provision had been made in relation to data security in a data sharing context (as is particularly the case in this market). In doing so, the Committee noted that data security was a fundamental factor in considering data protection. The Committee also noted that all Trading Parties regardless of size or sophistication have access to the full data set. The Committee therefore considered that it was necessary to preclude the possibility of individualised or subjective interpretations of data security.

2.14. In determining alternative wording, the Committee recognised that more specificity in the language was required to remove any ambiguity and the possibility of conflicting interpretations of the terms "industry" and "best practices", as well as to ensure demonstrable compliance. It was however agreed that a degree of flexibility for Trading Parties to adopt IT security standards which accord with their own business and risk profiles should be maintained.

2.15. Committee Members agreed that the drafting recommended to the Panel should be updated. They agreed that these updates should:

a) Remove ambiguity on industry best practice and frameworks;
b) Provide clarity by referencing example standards; and
c) Ensure objective benchmarking was required to demonstrate compliance.

2.16. Committee Members noted agreed that this represented a move from its original view based on a need for mutual assurance and the requirement of GDPR for clear standards. Members also agreed it would be sensible to maintain a watching brief on security standards as the market matures going forward.

2.17. The Committee:

- **AGREED** that MOSL should draft amended text in line with principles (a)-(c) for ex-committee agreement; and

- **AGREED** that, subject to this agreement, this revised wording be proposed to the Panel Sub-Group for agreement as an amendment to the drafting for Change Proposal CPM007 'GDPR and Data Protection Provisions Updates'.

2.18. The Chair thanked Members for their views and closed the meeting.

3. Post Meeting Addendum

Purpose: For Information

3.1. The revised drafting for MAC Schedule 13, section E, clause 1.2(a) together with the consequential change to 1.3(a) and 1.3(c) was agreed by all Committee Members via e-mail correspondence on 9 January 2018.

3.2. The wording imposes a clearer positive obligation on Trading Parties to meet ascertainable security standards which are capable of objective assessment for the essential purpose of mutual assurance, but also for demonstrating continuing security of shared data to the ICO. The revised wording maintains flexibility of choice within a set class and is the 'lightest touch' possible without compromising compliance.

3.3. The revised drafting agreed by the Committee is set out below:

Original	
Section E, Clause 1.2 (a)	Each Party must implement appropriate technical and organisational security measures that meet the requirements of Data Protection Laws and are consistent with or equivalent to industry standards, best practices and frameworks.
Clarified revision – 9 January 2018	
Section E, Clause 1.2 (a)	Each Party must implement appropriate technical and organisational security measures that meet the requirements of Data Protection Laws and which are consistent with or equivalent to at least one identifiable and objective IT security standard as published from time to time, for example (but not limited to) the Information Commissioner Office's Practical Guide to IT Security: Ideal for the Small Business or Cyber Essentials/Cyber Essentials Plus or ISO 27001 on information security management.

Original	
Section E, Clause 1.3 (a)	Trading Parties shall provide to the Market Operator on a reasonable basis evidence of having in place appropriate technical and organisational security measures for example by evidencing formal accreditation, certification or independent audit of information security systems.
Clarified revision – 9 January 2018	
Section E, Clause 1.3 (a)	Trading Parties shall provide to the Market Operator on a reasonable basis evidence of having in place appropriate technical and organisational security measures for example by evidencing formal accreditation, certification or independent audit of information security systems and, in doing so, shall identify which IT security standard or standards have been used for the purposes of compliance with 1.2(a) above.

Rationale for clarification:

- Revision (i) – Inserted wording to cross reference to the requirements of clause 1.2(a)

Original	
Section E, Clause 1.3 (c)	the Market Operator shall make available to any Trading Party on reasonable request evidence of having in place appropriate technical and organisational security measures for example by evidencing any formal accreditation, certification or audit of information security systems.
Clarified revision – 9 January 2018	
Section E, Clause 1.3 (c)	the Market Operator shall make available to any Trading Party on reasonable request evidence of having in place appropriate technical and organisational security measures for example by evidencing any formal accreditation, certification or audit of information security systems and, in doing so, shall identify which IT security standard or standards have been used for the purposes of compliance with 1.2(a) above.

Rationale for clarification:

- Revision (i) – Inserted equivalent wording to apply the application of standards to the Market Operator as well as Trading Parties.