Market Arrangements Code Change Proposal – Ref CPM019

Modification proposal	Market Arrangements Code Change Proposal – CPM019 – GDPR Data Security Standards
Decision	The Authority has decided to approve this Change Proposal
Publication date	1 October 2020
Implementation date	6 November 2020

Background

All UK companies must be compliant with the new standard of data protection set out within the General Data Protection Regulation EU 2016/679 (**'GDPR'**), which came into force on 25 May 2018 and the supplementary UK legislation, the Data Protection Act 2018 (**'DPA 2018'**). The Panel established the GDPR Issues Committee (**'the Committee'**) to assess the compatibility of the Wholesale Retail Code (**'WRC'**) and Market Arrangements Code (**'MAC'**) against the DPA 2018 and GDPR, in order to determine what changes would be needed to enable industry compliance.

As part of its work undertaken in 2017-2018, the Committee considered the question of data security and how this might be objectively measured, including by reference to published technical data security standards. As a result of this review, the Committee originally agreed a 'light touch' approach and recommended to the Panel that Schedule 13, section E, clause 1.2 of the MAC be updated as follows:

> *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 it 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.*

The Committee also recommended a watching brief of the technical data security standards provisions set out in Schedule 13 of the MAC. Since the Committee was re-established in 2019-20, it commissioned an independent data security expert to carry out a review of the technical standards set out in Schedule 13 of the MAC. The scope of the review focused on four questions:

1. What data security standards or schemes are presently available which allow objective benchmarking in a data sharing context?
2. Are there any schemes which are particularly suitable for use in this market, given the nature of personal data involved and the means by which it is presented?
3. Amongst the schemes available, are there any which could feasibly be utilised as a single standard that Trading Parties operating in the market carry varying size, risk and resource profiles?
4. Is it possible to enhance or improve the current data security benchmarking in the solution whilst maintaining Trading Party flexibility of choice?

The issue

At the August 2019 meeting, the Committee considered the advice of the expert, as set out in Attachment C of the Panel's Final Recommendation Report. One of the findings of the expert was that Cyber Essentials/ Cyber Essentials Plus, currently listed as an example in Schedule 13 of the MAC, does not meet certain key criteria when assessed against the Information Commissions Office guidance and the GDPR. Therefore, on its own, the guidance could not ensure compliance.

The expert identified alternative standards which would enable compliance and would be suitable for use in the business retail market. The expert also identified additional security controls which could be used to supplement Cyber Essentials to achieve compliance. This included risk assessment, information security policy, information security responsibility and training and awareness. The full list of supplementary controls is included in Appendix C of the Panel's Final Report.

The Change Proposal[1]

This Change Proposal seeks to update the example data security standards identified in section E of Schedule 13 of the MAC, to better facilitate compliance through the identification of data security standards compliant with GDPR security requirements.

As set out in section 3 of the Panel's Final Recommendation Report, the Committee asked the expert to rank the security standards listed in their findings report, taking into account the following criteria:

- particular suitability or relevance to the water business retail market

[1] The proposal and accompanying documentation is available on the MOSL website at https://www.mosl.co.uk/market-codes/change#scroll-track-a-change

- particular suitability taking into account the types of data processed and the specifics of processing and sharing (CMOS transactions)
- suitability to larger or smaller trading parties or both - especially bearing in mind costs or complexity
- suitability to Wholesalers, Retailers or both
- costs generally
- configurability or any restrictions.

Having reviewed the rankings provided by the expert, the Committee recommended the following security standards be listed as examples in the Schedule 13, section E of the MAC:

- Network and Information Systems Regulations 2018[2]
- Publicly Available Standard (PAS) 555:2013
- Centre for Internet Security (CIS)
- International Organisation for Standardisation (ISO) 27001[3].

Rationale on why these standards were selected is detailed in the table under section 3.1 of the Panel's Final Recommendation Report.

Industry consultation and assessment

An Industry Consultation was not carried out on this Change Proposal. The Committee decided that the wider industry need not be consulted as the change serves only to identify example standards which facilitate compliance and does not impose additional obligations upon Trading Parties. The Committee consulted with a data security expert and their own IT professionals and did not believe a consultation would bring any additional benefits.

When voting on whether to recommend CPM019 to the Panel, the Committee members agreed unanimously with the proposed solution. The Committee agreed that this Change Proposal would further the market objectives and principles of proportionality, transparency, barrier to entry, non-discrimination and customer

[2] The EU Security of Networks and Information Systems (NIS) Directive, which provides Competent Authorities the ability to assess the cyber security of Operators of Essential Services known as the Cyber Assessment Framework, was recommended by the independent expert. The Committee recommended the UK Network and Information Systems Regulations 2018 as this implements that Directive into UK law.

[3] ISO27001 is already currently listed as an example in Schedule 13. The work undertaken for this change confirmed that it is a suitable standard to cite.

participation. The Committee also provided the following rationale on the benefits of CPM019:

- The change will result in the requirements for compliance with the GDPR being more transparent to Trading Parties and therefore may result in improved compliance with the GDPR.
- It removes Cyber Essentials and Cyber Essentials Plus from the list as they do not meet certain key security criteria. Therefore, the change removes examples that are not fully compliant with the GDPR requirements on data security.
- No party is excluded by these standards as there is a range of options to work towards, each with their own benefits.

The Final Recommendation Report states that "one Committee Member raised the concern that because the change is not mandating any security standards it does not better facilitate compliance with the GDPR. Another felt that the list should be a framework of requirements used as a benchmark for minimum standards that Trading Parties could self-certify against. This is because some of the standards are onerous, and possibly a barrier to entry, to be able to achieve an absolute certification against".

The Committee agreed that Cyber Essentials and Cyber Essentials Plus should be removed from the list of examples in the MAC. This is because the expert advised that on their own, Cyber Essentials and Cyber Essentials Plus do not meet the ICO requirements of data security. It was agreed that best practice would be to include example security standards that are able to meet the ICO requirements without additional controls. This would not prevent a Trading Party from using Cyber Essentials and bolstering it with other controls. As such, Committee Members felt it would be wrong to recommend this, when by itself it does not meet the minimum requirements.

Views of the Customer Representative

With regards to CPM019, from the perspective of the Customer Representative, the Customer Representative welcomed the review carried out by independent expert. They noted that the MAC must comply with data security standards and they support the work that has been carried out by the GDPR Committee. Furthermore, they highlighted that it is essential that data security standards protect personal customer data in the business retail market. Finally, they agreed with the introduction of the proposed change as it should help to ensure GDPR compliance which, in turn, could improve customer confidence the market.

Panel recommendation

The Panel considered this Change Proposal at its meeting on 28 January 2020. It recommended, by unanimous decision, that the Authority approve this proposal. This recommendation has been made on the basis of improving the principles of proportionality, transparency, barrier to entry, non-discrimination and customer participation. The recommended date of implementation is 15 May 2020.

Our decision

We have considered the issues raised by the Change Proposal and the supporting documentation provided in the Panel's Final Report. We have concluded that the implementation of the of CPM019 will better facilitate the principles and objectives of the Wholesale Retail Code detailed in Schedule 1 Part 1 Objectives, Principles and Definitions, and is consistent with our statutory duties.

Reasons for our decision

The independent data security expert was a company that brought together experienced professionals from across various industries. At the time of the report, the company had provided personal data protection and information security consultancy for over 12 years.

Having reviewed the evidence provided by the Panel in its Final Recommendation Report, we understand the issues it seeks to address and the rationale for recommending this Change Proposal.

We are approving this Change Proposal on the basis it will provide transparency and help reduce barriers to entry to Trading Parties in terms requiring Trading Parties to operate to identifiable standards of data security and protection to better facilitate compliance with GDPR. In addition, the Change Proposal does not mandate specific security standards, but provides some indicative examples to enable compliance, allowing Trading Parties some degree of flexibility. Ultimately, this Change Proposal should have a positive effect on business retail customers because by strengthening the governance relating to compliance with GDPR in the MAC, Trading Parties cannot but be aware of their obligations under the GDPR.

We have set out below our views on which of the code principles are better facilitated by the Change Proposal.

Transparency

We agree with the rationale provided by the Panel and the Committee that this Change Proposal helps provide assurance amongst Trading Parties to operate to agreed standards of data security and protection to better enable compliance with GDPR obligations.

Barriers to Entry

We believe CPM019 will help reduce barriers to entry as the solution provides a range of data security and protect standards Trading parties can choose to comply with in order to better facilitate compliance with GDPR in the most efficient way.

Decision notice

In accordance with paragraph 7.2.8 of the MAC, the Authority approves this Change Proposal.

Georgina Mills
Director, Business Retail Market