# Market Arrangements Code and Wholesale Retail Code Change Proposal – Ref CPW029 and CPM007

| | |
|---|---|
| **Modification proposal** | Market Arrangements Code and Wholesale Retail Code change proposals CPW029 & CPM007 – General Data Protection Regulation and Data Protection Provisions Update |
| **Decision** | Ofwat has decided to accept these change proposals |
| **Publication date** | 27 February 2018 |
| **Implementation date** | 30 March 2018 |

## Background

In 2016, market participants began to express concern that market opening may impact their ability to comply with data protection legislation. It was felt that market participants would be dependent on MOSL and other trading parties in order to comply with the legislation. As a result of concerns raised, MOSL commissioned a Privacy Impact Assessment (PIA) to deliver recommendations as to how the Market Codes could provide for data protection. A Data Management Protocol was drafted following conclusion of the PIA.

Change proposal MAC005 suggested adding a further schedule to the Market Arrangements Code (MAC) to include the Data Management Protocol. At the time, the Interim Code Panel did not recommend the implementation of MAC005. The Panel noted that the proposal required refinement and suggested that the proportionality of the proposal required consideration. When making its decision, consideration was also given to the pending introduction of the General Data Protection Regulation (GDPR).

The GDPR is being introduced to protect all European Union (EU) citizens from privacy and data breaches by putting individuals in control of their personal data. It comes into effect on 25 May 2018 and will automatically replace the Data Protection Act 1998 (DPA). By 25 May 2018, all organisations must be compliant with the GDPR.

The GDPR introduces a new standard of data protection applying to both Data Controllers and Data Processors. It requires a company to demonstrate how it complies with the following principles:

- Lawful processing
- Consent
- Enhanced Privacy Notices
- Accountability and Governance
- Breach Notifications

A GDPR Issues Committee (the GDPR Committee) was introduced by the Panel in May 2017, following the work undertaken on MAC005 and due to the pending introduction of the GDPR. The purpose of the GDPR Committee was to identify a solution to ensure that the industry and MOSL were compliant with data protection laws. It was delegated a number of responsibilities, inclusive of providing expert advice relating to the GDPR and making recommendations to the Panel on any changes to the Market Codes.

On 5 December 2017, following industry consultation, the GDPR Committee made its recommendation to the Panel setting out proposed changes to align the Market Codes with data protection legislation (including the pending GDPR). These proposals have been packaged together as CPW029 and CPM007 into a single 'whole' change proposal.

The change proposals were submitted to Ofwat on 2 February 2018.

## The issue

As the GDPR will replace the DPA on 25 May 2018, code modifications are required to ensure industry compliance with the GDPR and to remove reference to the DPA from the MAC and the WRC.

## The modification proposal[1]

The Panel recommends code amendments in the following areas:

### CPW029

[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

1. A simplified part K of the Wholesale Retail Code (WRC) removing duplicated references to data protection and requiring that parties to the WRC comply with the provisions for Data Protection set out in the MAC;
2. A new form to give effect to processes related to Data Subject rights;
3. Clarification of the data items in the Data Catalogue (Code Subsidiary Document 0301), and also the bilateral forms in the Operational Terms that may contain Market Personal Data;

### CPM007

4. Additional definitions in the MAC to reflect drafting changes;
5. A re-drafted Section 15 of the MAC setting out key data protection obligations including general compliance, roles and responsibilities, data processor obligations and provisions relating to use of market data; and
6. A new Schedule 13 for the MAC containing detailed provisions for data protection, including processes for trading parties and the Market Operator to address any Data Subject requests.

## Industry consultation and assessment

The GDPR Committee conducted an industry consultation prior to submitting its recommendation of changes required to align the Market Codes to data protection legislation. The GDPR Committee issued its consultation on 16 October 2017. There were 17 respondents to the GDPR Committee's consultation, including ten wholesalers, six retailers and the Consumer Council for Water.

The GDPR Committee considered the responses during its November and December 2017 meetings and made a number of amendments to its recommendations before submitting its report on 5 December 2017.

Details of the consultation questions, and summaries of the responses received are set in Appendix 1.

The Panel considered change proposals CPW029 and CPM007 at its meeting on 12 December 2017. There were two specific clauses (E1.2 relating to technical and organisational security measures to meet Data Protection Laws and E2.1 relating to a Data Controller's notification responsibilities in the event of a Personal Data Breach) that meant the Panel was unable to reach an agreement regarding the recommendation at its meeting on 12 December 2017. As a result of this, the task of reviewing, and if necessary amending, these clauses was delegated to a Panel Sub-Group. Following the Sub-Group's work, the Panel voted in favour of accepting the changes made to clauses E1.2 and E2.1 of the MAC providing these did not make the terms of the clauses broader or more onerous.

The Panel Sub-Group met on 18 December 2017 to review the wording of clauses E1.2 and E2.1 of the MAC. The Sub-Group agreed the revised wording of E2.1 but was unable to reach an agreement in respect of E1.2 so decided to refer the clause to the GDPR Committee to obtain expert views. The GDPR Committee provided views on 8 January 2018, where it agreed to improved wording of E1.2 and recommended two consequential changes (to clauses E1.3 (a) and (c)). On 15 January 2018, the Panel Sub-Group held a meeting to discuss the recommendations of the GDPR Committee and agreed the revised drafting did not make the clause more onerous. However, it sought endorsement of its recommendation in its report, dated 30 January 2018, as consequential changes to other clauses had been made.

## Panel recommendation

The Panel considered the change proposals CPW029 and CPM007 at its meeting on 12 December 2017. There were 9 votes in favour of recommending these changes for approval by Ofwat and three against. There was an additional vote to establish a Panel Sub-Group which had delegated authority from the Panel, by a vote of 11 to one, to review and amend the recommendation in relation agreed clauses of the MAC (E1.2 and E2.1). The Panel Sub-Group sought endorsement of its suggested changes to the relevant clauses of the MAC at the Code Panel meeting on 30 January 2018 and the Panel agreed to recommend CPW029 and CPM007 to Ofwat.

## Our decision

We have carefully considered the issues raised by the modification proposal and supporting documentation provided in the Panel's recommendation report. We have concluded that the implementation of CPW029 and CPM007 will better facilitate the principles and objectives of the WRC detailed in Schedule 1 Part 1 Objectives, Principles and Definitions and is consistent with our statutory duties. It is agreed that the changes will have a positive impact on a number of Objectives and Principles.

This decision has been made on the basis that approving the proposed changes will assist MOSL and trading parties to fulfil their data protection obligations. However, the provisions of the MAC and the WRC in and of themselves do not guarantee compliance with data protection legislation. Ultimately, each company retains responsibility for ensuring its compliance with the relevant legislation by the relevant implementation date.

# Reasons for our decision

We have set out below our views on which of the applicable code principles are better facilitated by the modification proposals.

### Efficiency

Establishing a consistent set of requirements across trading parties is the most efficient way to meet the GDPR requirement rather than parties developing independent approaches to meeting the GDPR in respect of Market Personal Data.

### Proportionality

The provisions have been developed so as to allow trading parties of differing sizes to comply in a proportionate way. As the provisions are flexible, undue burdens are not placed on small retailers.

### Transparency

The changes helps to clearly communicate the requirements of the GDPR to trading parties and are the standards they are expected adhere to when communicating with each other.

### Simplicity, cost-effectiveness and security

Having a consistent approach requiring similar standards of data security and protection across the industry should ensure efficient operation of data protection related processes.

### Customer Participation

The GDPR includes the objective of providing customers with control of their own data, these modifications will help facilitate this objective through the new data subject rights processes.

# Decision notice

In accordance with paragraph 7.2.8 of the Market Arrangements Code, Ofwat approves this change proposal.

**Emma Kelso,**
**Senior Director, Customers and Casework**

# Appendix 1: Summary of consultation responses

1. **Do you agree that the proposed solution supports compliance with GDPR, without being overly prescriptive?**

   12 respondents agreed. Those that did not agree made comments about the necessity to comply with Information Commissioners Office (ICO) non-mandatory guidance, concern regarding potential double jeopardy for non-compliance from both MOSL and the ICO and disagreement with how the term "Data Controllers" was applied in the definition of in common and joint liability. Some parties also requested clarification of the use of data for other purposes, including marketing.

2. **Are there any requirements of the GDPR or related/consequential market requirements missing from the proposed solution?**

   Eight respondents thought there weren't any. Respondents who thought there were expressed concern with the implications for data protection from the bilateral transfer of forms containing Personal Data. They thought a robust data processor agreement was required and recommended the following additions: additional definitions (such as Data Controller and Data Subject); clear designation of liability; Supply Point Identification Numbers (SPID) to be listed as a Personal Data Item.

3. **Are there any substantial impacts on the trading parties arising from the proposed changes to the MAC that would not otherwise be incurred complying with the GDPR?**

   Eight respondents agreed. Concerns raised included potential issues relating to joint liability, the DPO's requirement for 24 hour contacts (which they thought could impact trading parties significantly), potential for double jeopardy from MOSL and the ICO, the potential for significant reduction of the dataset currently used by trading parties for pricing and marketing purposes.

4. **Do you agree the solution proposed is proportionate for all trading parties? If not, please explain why and identify anything you believe should change**

   Nine respondents agreed. Those that did not agree raised concerns, including needing more assistance on technical security for parties if they are jointly liable, that the ICO guidance might be more difficult to follow for smaller players, that privacy notes should be at the discretion of trading parties and that retailers will be disproportionately affected by the new Data Subject rights processes and the forms/communications required.

5. **Do you agree that the provisions should require trading parties to comply with all guidance (both mandatory and non-mandatory) supplied by the ICO? Please explain your answer.**

   Ten respondents disagreed with this question. The responding parties suggested that this would impose stricter requirements than the GDPR itself and that the ICO guidance was not intended to be mandatory but was proposed to be best practice. It was suggested that it trading parties should evaluate whether is proportionate and appropriate for their organisations to implement any non-mandatory guidance supplied by the ICO.

6. **Do you agree that the current MAC Disputes Process is the most efficient way to manage disputes that arise relating to GDPR compliance? Alternatively, do you think a new process is required? Please explain your answer.**

   Ten respondents agreed that the MAC Disputes Process is the most efficient way to manage disputes that arise relating to GDPR compliance. Alternative suggestions were; to amend the MAC disputes process to reduce delays, to develop an entirely new MAC governed process or to allow the Panel or a new Committee to govern the process.

7. **Do you believe that the Market Audit would be the best way to measure trading parties' compliance with these data protection provisions? What alternatives would you suggest?**

   13 respondents agreed that a Market Audit would be the best way to measure trading parties' compliance with data protection provisions. Those who did not agree indicated that self-assurance may be an alternative option to reduce an onerous process and highlighted that the trading parties internal compliance procedure should take precedence.

8. **Do you believe that proposed clause 15.4.1 of the MAC will lead to unintended consequences that might impact parties' ability to serve customers? If so, how?**

   Ten respondents did not believe that proposed clause 15.4.1 would lead to unintended consequences that might impact parties' ability to serve customers. Those that considered there may be unintended consequences, expressed concern that the proposed wording did not reflect the agreement by the Committee that there should not be an express prohibition on the use of market data for marketing. It was suggested that that without marketing there could be potential issues developing the market and keeping customers informed.

9. **Would you find it useful for the provision on security requirements to reference existing industry standards and frameworks that could be used as a basis for determining compliance? Please explain your answer.**

   Ten responding parties disagreed that it would be useful for the provision on security requirements to reference existing industry standards and frameworks which could be used as a basis for determining compliance. A reason provided by parties for disagreeing with this question was that this would become prescription rather than a guideline.

10. **Should there be some specific measures in place to protect sensitive data such as functionality to restrict access to the sensitive customer field, and produce different versions of existing reports that remove this field without the required access? Please explain your answer.**

    Ten responding parties agreed that specific measures should be put in place to protect sensitive data. Those that did not agree indicated that it was unnecessary because CMOS already has access limited to very few personnel, all of whom require this access for operational reasons. Further, it was suggested that because of the limited timescales this would waste developer time and result in additional costs.

11. **Are there currently sufficient provisions in place to facilitate requests for Automated Decision Making to be completed manually? Please explain your answer.**

    Nine of the responding parties agreed that there are currently sufficient provisions in place. A number of parties didn’t feel they had sufficient information to be able to provide a response or suggested further investigation was required. One party did not agree that there were any automated processes and therefore, did not consider the question to be relevant.

12. **Do you agree with the use of Data Subject Process forms to facilitate the process described in the new Schedule? Should the forms be defined in the MAC or be governed separately by the Panel outside of the codes? Please explain your answer.**

    Ten respondents agreed with this question. Respondents highlighted that forms are useful however, should be flexible to allow them to accommodate legislative changes as they happen. In addition, it was suggested that the forms should be minimal in requirements to encourage their use. Two respondents felt that these should be defined in the MAC for clarity.

**13. Is the proposed process for communicating data subject requests required to support the correction of Personal Data where corrections can be made using existing industry transactions? Please explain your answer.**

11 respondents agreed that the existing processes should be incorporated into the provisions where possible, rather than relying solely on the drafted processes. Many respondents also felt that these processes could be revised and simplified. It was suggested that there should be a clear distinction between requests to update information as part of ‘business as usual’ (such as name or address changes) and formal requests to rectify data under the GDPR.

**14. Do you agree that Trading Parties and the Market Operator should transmit Data Subject Process Forms (which will contain Personal Data) via a secure platform? Please explain your answer.**

16 parties agreed that it would be necessary to use a secure platform to submit Data Subject Process forms. It was considered that emails are not secure enough to communicate this data and suggested that the platform should be proportionate to the sensitivity of the information.

**15. Are the terms of clause 10 (Claims Brought by Data Subjects) sufficient or should specific allocations of liability and mutual indemnities be instructed? Please explain your answer.**

Seven respondents agreed that the terms of clause 10 were sufficient and eight respondents disagreed. There was a mixed response to this question, some respondents raised concerns regarding joint liability, suggesting that where possible there should be a clear allocation of liability. Clarification was also requested regarding the definition of ‘claim’, as it was considered to be unclear whether the intention was for clause 10 to only be exercised for formal legal claims.

**16. Do you agree with the proposed implementation timetable that would provide trading parties with at least one month to align their privacy notices with the Market Operator?**

14 respondents agreed with the proposed implementation timetable. However, two respondents suggested that one months may not provide sufficient time to align their privacy notices with the Market Operator.

### 17. Do you have any further comments on the issue?

Respondents raised a number of additional points to this question:

- Concerns were expressed over whether all of the provisions could be implemented prior to the GDPR coming into force;
- A question was raised as to whether privacy by design and by default has been considered for development of CMOS;
- Suggestions were made that additional definitions were required (to include Data Owner, Data Subject and Data Controller amongst others);
- Suggestion that there is inconsistency in the drafting which will require review, it was stated that some of the defined terms are used interchangeably which could affect the aim of the changes;
- Comment was made that there was a need to engage the ICO throughout the GDPR amendment process;
- Confirmation was sought as to whether MOSL will appoint a Data Protection Officer;
- It was suggested that repetition of the GDPR elements in the codes is not required;
- A respondent challenged the requirement to include anything in the MAC or the GDPR suggesting that the recommendations provided by the ICO are sufficient to ensure compliance;
- It was highlighted that the lack of data mapping is an issue; and
- The provisions repeat many articles in the GDPR, it was highlighted that it is unclear whether this was the intention, it was suggested that it could simply reference the relevant articles.