MARKET CODE / OPERATIONAL CODE CHANGE PROPOSAL			Form version 2.3
Change Proposal reference (To be completed by the TP Sec.)	**MCCP221**	Version No.	**B.5**

PART A — SUBMISSION

A.1. GENERAL DETAILS			
A.1.a. TITLE	GDPR		
A.1.b. COMPANY	CMA		
Change Proposals must be authorised by the person designated by the signatory to the Market Code Framework / Accession Agreement			
A.1.c. AUTHORISED SIGNATURE		NAME	
A.1.d. CONTACT NAME	Neil Cohen	CONTACT EMAIL; TEL/MOB.	Neil.cohen@cmascotland.co.uk 0117 942 3272
A.1.e. ASSOCIATED MCCP / OCCP			
A.1.f. ASSOCIATED DOCS.	Annex 1: Schedule 25 (Data Protection) Annex 2: Additional Services Schedule Mark Up Annex 3: CMA Website Additional Text and pages Annex 4: CMA LWI Mark Ups (not attached; for CMA purposes only).		
A.1.g. PROPOSED URGENCY	NON-URGENT		
A.1.h. REASONS FOR URGENCY			
The CMA CEO will review this information and make a decision as to whether to take this MCCP / OCCP forward as urgent as defined under Market Code Part 8.9.1			

A.2. MCCP / OCCP DETAILS

A.2.a. ISSUE OR DEFECT WHICH THIS MCCP / OCCP SEEKS TO ADDRESS
Required under Market Code Parts 8.7.1 (ii) (b) and 8.8.1 (ii) (b)

GDPR

The General Data Protection Regulation (GDPR) is a legislative item which is due to be implemented within the European Union in May 2018. The UK government intends to retain these rules notwithstanding Brexit and build on the existing data protection infrastructure established under the Data Protection Act 1998 (DPA). The main thrust of the GDPR, aside from some new obligations and requirements, is for data protection arrangements to be more fully documented and to be more comprehensively demonstrable.

A summary of the key reforms is set out below.

Personal Data

The data covered by the GDPR is largely that covered by the DPA and is defined as 'personal data', being any information relating to an identified or identifiable natural person. Where;

- Data can be information held on an IT system or in hard-copy,
- 'Identifiable' is taken to be anything that can relate to such natural person, such as an ID, a location or address, a pseudonym, etc.
- A natural person is an individual.

There is also a further category of data; 'sensitive personal data', which includes special categories of personal data, such as medical records and this is as per existing definitions in the DPA.

Data Subjects

Data Subjects are the individuals about whom the personal data is being processed. Data Subjects will have the right to the following, with regard to personal data (and sensitive personal data) that pertains to them:

- Access to their data and to relevant supplemental data and confirmation as to the nature of any data processing, as per the relevant Privacy Notice. This builds on existing requirements under the DPA.
- Rectification. This is largely the same requirement as currently exists in the DPA.
- To be informed of the manner in which data is being used (via a Privacy Notice).
- Portability. The ability to obtain and re-use their personal data. This is a new right identified in the GDPR.
- Restriction of processing. This builds on existing requirements under the DPA.
- Erasure. The 'right to be forgotten'. Data should be deleted or removed if there is no compelling reason for continued processing, on request. This is a new right identified in the GDPR.

Data Handlers

Any organisation that handles personal data will be governed by the GDPR in one of two ways;

- A Data Controller, responsible for determining the purposes for which personal data is to be processed,
- A Data Processor, responsible for undertaking the data processing activities on behalf of the Data Controller.

These definitions are largely those already identified in the DPA. However, the GDPR imposes duties on Data Processers for the first time.
The definition of processing is that identified in the DPA and means, in relation to personal data, obtaining, recording or holding the personal data or carrying out any operation or set of operations on the personal data, including;

- The organisation, adaptation or alteration of the personal data,
- Retrieval, consultation or use of the personal data,
- Disclosure of the personal data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the personal data.

The GDPR builds on the underlying rules already set out in the DPA. These rules are known as the 'principles' and include the following:

- The need to obtain the consent of the Data Subject to process his/her personal data or demonstrate that processing is necessary for pursuing the legitimate business interests of the organisation;
- That personal data is always relevant and not excessive;
- That personal data is kept for no longer than necessary;
- That personal data is processed only for specific purposes;
- That personal data is kept secure;
- That personal data is not transferred to countries outside the EEA without there being the same security laws in place as exist in the EEA;
- Requests for information from Data Subjects about personal data being processed and deleting or changing if requested should be met.

Under the GDPR, such organisations need to undertake the following:

- Establish Data Protection Officers (DPOs). A DPO is only required where the core activities of the Data Controller or the Data Processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale
- Document the legal basis for data processing. Such legal basis must be one of; consent of the Data Subject, necessary for the performance of a contract, legal obligation, public functions, or if processing is necessary to enable the Data Controller to pursue its legitimate interests. Consent is therefore an option. Consent will now require clear affirmative action by the customer. It will no longer be possible to rely on implied consent or opt-outs. Categories of information will need to be included in the record of processing operations.

- Content of Privacy Notices. New rules on content require the following information to be included:
    - the categories of personal data being processed
    - the purposes and legal basis of processing
    - recipients of data collected
    - security applied to data
    - any transfers of personal data outside of the EU
    - retention periods
    - details of individual rights and
    - the existence of any automated decision making.
- Accountability. Controllers must demonstrate compliance with data protection principles. This is a new GDPR requirement.
- The Data Controller will be required to include certain mandatory contract terms in any data processing contracts with Data Processors.
- Ensure adequate procedures exist for notifications of any security breaches to the Data Subject and to the Information Commissioner's Office.
    - A personal data breach will be defined as; a breach of security, leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
    - Data Controllers and Data Processors will need to notify the ICO and possibly the Data Subject, if practical within 72 hours of any security breach.
    - Failure to report could result in penalties of up to 2% of turnover or €10m (Sterling equivalent), whichever is the greater.
- Demonstrate that they have carried out a privacy impact assessment under certain circumstances, namely when data processing activity is likely to result in a high risk to individuals e.g. processing of sensitive personal data or transferring personal data outside the EEA.
- Implement appropriate technical and organisational measures designed to implement the underlying data protection rules. This is known as "privacy by design".

<u>Liabilities</u>
Breaches of the GDPR could result in fines of up to 4% of turnover or €20m (equivalent in Sterling), whichever is the greater.

A.2.b. DESCRIPTION OF THE NATURE AND PURPOSE OF THE MCCP / OCCP AND HOW IT MEETS THE MARKET CODE / OPERATIONAL CODE OBJECTIVES AND PRINCIPLES FOR THE MARKET DOCUMENTS
Required under Market Code Parts 8.7.1 (ii) (c) and 8.8.1 (ii) (c)

General Description

This proposal identifies updates to the Market Code to establish appropriate obligations regarding the security and use of data covered by the Market Code, such that GDPR requirements are fulfilled.

It may be the case that some or all market participants will have internal data management or data handling activities that require GDPR compliance. This proposal, based on the framework above, covers only those systems that utilise data arising directly from Market Code obligations;

- The CMA website
- The CMA Central Systems (via LVI or HVI)
- The SLP
- Any Trading Party system or website that holds any data from any of the above systems.

The proposal has made full use of similar work undertaken by MOSL and English water and sewerage market participants (in particular, CPM007 and CPW029 along with Code Panel paper P15-09), such that the framework proposed for the Market Code is as close as is practical to that adopted in England and the detailed arrangements are broadly convergent with those in England, wherever practical.

The framework for the Market code updates proposed is as follows;

Document	**Heading**	**Content**	**Comments**
Market Code	Compliance statement	General obligation to comply with Data Protection legislation	
	Statement on roles and responsibilities	Identifies the CMA and TPs as Data Controllers.	
	Statement on Data Processors	Obligation to ensure that Service Providers and 3rd Parties comply	
	Statement on the use of Personal Data	General statement limiting the use of Personal Data to what is identified in the MC	
Data Protection Schedule	Data Subject Rights	Processes and pro-formas for; • Portability • Restrictions on Processing • Erasure • Corrections/Rectifications • Objections to Processing • Access	The expectation is that any Data Subject requests would come via their LP and LPs may then put such requests to the CMA. CMA Additional Services arrangements would then be required to deliver such.

	Data Security Standards	Appropriate measures, to include (where appropriate); • Pseudonymisation • Encryption • Ongoing confidentiality, integrity, availability and resilience of processing • Ability to restore, following an event • Processes for regular testing, assessment and evaluation of the effectiveness of data security measures • Data security to be compliant with, consistent with, or equivalent to ISO27001 (Cyber Essentials Scheme)	For CMA CS and the SLP, CMA IT Policies will be updated to reflect these requirements and further change proposals progressed, where necessary.
	Data Management	Reporting and monitoring arrangements, to include an annual review by the CMA.	Will be delivered by an annual report to the Technical Panel (as for the Performance Measures review).
	Privacy Notices	CMA to provide (on its website) a Market Privacy Notice, as a template for individual Privacy Notices, to be subject to review for any proposed changes. Parties to ensure that Privacy Notices are made available to Data Subjects, as necessary.	It is assumed that such Privacy Notices will be required for any IT web page or other interface potentially available to a Data Subject which might pertain to CMA CS or SLP data.
	Breach Notifications	Identifies joint liability and processes for notification to Data Subjects and to the Information Commissioner of any data security breach.	Note the ref to the Info Commissioner, but not the Scottish Info Commissioner (who is only responsive for FoI requests).
	Data Governance	Nomination of Data Protection Officers and notification of such to the CMA. Use of Privacy Impact Assessments for changes. CMA website to summarise Data Protection arrangements, content to be subject to market review.	It is assumed that existing Delegated Authorities could fulfil the duties of DPOs. For Market Code change management, PIAs will be added to existing IA pro-forma. Website text changes will be managed via CPs

CMA internal documents and systems	Data deemed to be Market Personal Data	• CMA CS 'My Details' (User Name, e-mail, Org) • SLP 'My Details' (User Name, e-mail, Org) • CMA Enquiry Listing (Name, Contact, TP Name and enquiry history) • CMA CS 'Trading Party' listing (Contact Name, e-mail categories, TP Name) • SLP 'Org Details' (Landlord Name, Landlord Type, Contact No, web address) • CMA CS 'SPID View/Customer Name' and MDS (Customer Name, SPID, SPID Address, GIS X, Y and Z, Meter IDs, DPIDs, Main SPIDs and Sub SPIDs) • SLP 'Current Data' or 'Historic Data/Landlord Name' (Landlord Name, SPID, SPID Address, Customer Name, Vacancy status)	Both 'My Details' sets of data are already available to individual Users and any objections by such Users can be accommodated by their removal as Users. Hence, no further action has been defined for these data sets.
Ops Code		Data aspects to be consistent with the above.	An OCCP may be required for these changes.

Principles and Objectives affected
CMA Guidance Note GN009 may be referred to for assistance with this section

PRINCIPLE	AFFECTED (Y/N)	DESCRIPTION
Proportionality	Y	The proposal seeks to implement an optimal response to GDPR requirements.
Transparency	Y	Data Protection obligations will be set out consistently for all participants, so far as Market Code data is concerned.
Simplicity, Cost-effectiveness, and Security	Y	Allows for any security requirements not already catered for to be incorporated.
Non-exclusivity	N	
Barriers to Entry	Y	Allows new entrants to meet GDPR requirements unambiguously and in a manner consistent with incumbents.
Customer Contact	N	

Non-discrimination	N	
Non-detrimental to SW Core Functions	N	
MC / OC OBJECTIVES	N	

A.2.c. IMPACT Required under Market Code Parts 8.7.1 (ii) (d), (f) and (g), and 8.8.1 (ii) (d) and (f)		
CONFIGURED ITEM	IMPACTED (Y/N)	DESCRIPTION
MC / OC	Y	See legal drafting
CSDs	N	
Wholesale Services Agreements	N	
Licenses	N	
CMA Central Systems	Y	Some changes to security and to Additional Services may be required.
CMA business processes	Y	Additional Services may need to be supplemented, along with notification arrangements and review processes.
Trading Party systems	Y	Some changes to security may be required
Trading party business processes	Y	Some notification and customer liaison activities may need to be modified.

A.2.d. DRAFT LEGAL TEXT
Required under Market Code Parts 8.7.1 (ii) (d) and 8.8.1 (ii) (d)

The following new definitions should be added to Schedule 1 of the Market Code:

Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Protection Laws	All applicable data protection and privacy laws in force in the UK from time to time including the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the General Data Protection Regulation (Regulation (EU) 2016/679) all as amended from time to time and any further legislation implemented in the UK in substitution for or to give effect to any of the above
Data Subject	The natural person on whom Personal Data is held by the Data Controller
Information Commissioner	The supervising authority in the UK responsible for monitoring compliance with Data Protection Laws
Market Personal Data	Personal Data either: (a) stored in, accessed through or downloaded from Central Systems, or the SLP; and/or (b) Personal Data shared between Market Participants as required by the Market Code.
Market Privacy Notice	A privacy or fair processing notice which is published by the CMA following consultation with Trading Parties regarding the use of Market Personal Data
Personal Data	Any information which can identify a natural person directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
User	An individual who is registered to access and make use of the Scottish Landlord Portal (or'SLP') or the Central Systems.

A new Section 10.6B should be added to the Market Code, as follows:

10.6B Data Protection

10.6B.1 General Compliance with Data Protection Laws

Each Party undertakes to comply with its obligations under the Data Protection Laws and, more specifically, in the performance of its obligations relating to Market Personal Data under the Market Code, including Schedule 25 (Data Protection).

10.6B.2 Roles and Responsibilities

10.6B.2.1 The CMA is a Data Controller of any Market Personal Data.

10.6B.2.2 Each Trading Party is also a Data Controller of any Market Personal Data that is:

(a) uploaded by that Trading Party to Central Systems and/or the SLP; and/or

(b) accessed by that Trading Party; and/or

(c) also held on that Trading Party's systems.

10.6B.2.3 It is the responsibility of each Party to ensure that its processing of Market Personal Data complies with Data Protection Laws and the Market Code, including Schedule 25 (Data Protection).

10.6B.3 Data Processors

10.6B.3.1 Each Party undertakes to enter into such appropriate arrangements as are necessary in respect of any third party that may be acting as a data processor and/or sub-contractor on its behalf to facilitate compliance of these third parties with Data Protection Laws including specifically having in place any appropriate legal mechanism for the transfer of Market Personal Data outside of the European Economic Area. Each Party shall procure that the mandatory contract terms which are prescribed by the General Data Protection Regulation (Regulation (EU) 2016/679) are included in any data processing contracts.

10.6B.3.2 The CMA undertakes to ensure that it has in place, at all times, appropriate and robust contractual arrangements with any such appointed service provider to comply with Data Protection Laws including specifically having in place any appropriate legal mechanism for the transfer of Market Personal Data outside of the European Economic Area.

10.6B.4 Use of Market Personal Data

10.6B.4.1 Market Personal Data shall only be used for the proper operation of the Market Code and shall not be used or disclosed to third parties for any other purpose unless required by Law.

This does not restrict the use of Personal Data that was not obtained or accessed from Central Systems, or the SLP, nor Market Personal Data obtained from a Party to the Market Code acting in pursuit of the proper operation of the Market Code.

10.6B.4.2 Each Party shall ensure that, only such of its officers, employees, or contractors as is necessary for the proper operation of the Market Code, shall process Market Personal Data and shall take all reasonable steps to ensure that access to Central Systems and the SLP and use of Market Personal Data is restricted to those who are authorised for that purpose.

10.6B.4.3 Each Party shall ensure that all of its officers and employees who are able to access Central Systems, or the SLP, and Market Personal Data are provided with regular appropriate training regarding the requirements of Data Protections Laws and the Market Code.

10.6B.4.4 The CMA shall monitor the accessing and downloading of Market Personal Data by Trading Parties.

The new Schedule 25 (Data Protection) is given in Annex 1.

CSD0001 Market Entry and Assurance should be modified, such that its Annex B (Self-Certification Form) should include an additional declaration, as follows (red text):

On behalf of …….. ("the Licensed Provider"), I declare that the Licensed Provider:

- Understands its obligations under the Market Code, Code Subsidiary Documents and the market framework generally;
- Confirms that it is compliant with the Data Protection obligations, as set out in Schedule 25 of the Market Code.
- Acknowledges that the Licensed Provider is bound by the Performance Standards and is liable for Performance Standard Charges in accordance with the Market Code;
- Has undertaken training provided by the Central Market Agency on the operation of the Low Volume Interface; and
- Can operate the Low Volume Interface for the Central Systems;
- Acknowledges that the Commission, the Central Market Agency and any of their agents will not be held responsible for any difficulty that the Licensed Provider may encounter using the Low Volume Interface.

CSD0001 will also be modified to include 'Data Protection Obligations' as a training topic.

A.3. IMPLEMENTATION DETAILS

A.3.a. PROPOSED IMPLEMENTATION DATE OR LEAD TIME Timescale must not overlap with the period of consultation with the Commission and should take account of the impacts identified in Section A.2.c. Any quoted lead time should commence from date of Approval.
April 2018
A.3.b. ANY LIMITATIONS OR DEPENDENCIES FOR IMPLEMENTATION
Implementation assumes that GDPR will come into force in the UK in May 2018
A.4. ANY OTHER COMMENTS
The Additional Services Schedule should be amended, as given in Annex 2. The CMA website and the SLP home page will be amended, as given in Annex 3. The following CMA LWIs will be amended (and included in Annex 4, not attached, since these are wholly internal documents for the CMA, but are listed here for information): • LWI 101 (Accession and Termination); The existing DPA Notice in the CMA Membership Application should be replaced with a Data Protection Laws Notice and the Self-Certification pro-forma should reflect that in CSD0001, as modified. • LWI 102 (Enquiries, RAs, Additional Services and Disputes); Add a new category of Enquiry for 'Data Protection'. Also include Data Subject requests (to be managed via the CMA website and handled as bespoke Additional Services). • LWI 104 (CMA Reporting); Include 'Annual Reviews' as a reporting type and include the DP review. • LWI 108 (IT Security and Access); Include DAs to fulfil the duties of DPOs. • LWI 203 (Impact Assessment); Add 'Privacy Impact Assessment' to the IA pro-forma. • LWI 205 (IT Policies and Standards); Include explicit reference to the Data Protection Laws and include the specific Data Protection Policies.

PART B — TP ASSESSMENT

B.1. ASSESSMENT PROCESS			
B.1.a. ASSESSMENT START DATE	2018-11-15	ASSESSMENT END DATE	2018-02-15
B.1.b. IMPACT ASSESSMENT REQUIREMENT		IA REQUIRED (TRADING PARTY IMPACT)	
B.1.c. CONSULTATION REQUIREMENT		TP CONSULTATION NOT REQUIRED	
B.1.d. ASSOCIATED DOCUMENTS (to this Part B)			

B.2. ASSESSMENT DETAILS

B.2.a. CHANGE SPEC AND IMPACT (IF DIFFERENT FROM THAT ORIGINALLY SUBMITTED)

B.2.b. CMA INTERNAL SYSTEMS IMPACT

B.2.c. DRAFT LEGAL TEXT
(if different from that originally submitted)

Drafting should be further amended, as follows, as agreed by the TP:

Schedule 25 Clause A.1.3 (b) should read; 'Trading Parties shall provide comments within ~~10~~20 Business Days of receipt of the summary or any proposed changes to it.'

Schedule 25 Clause B.2.3 should read; 'The Parties shall provide evidence in writing of compliance with the above within ~~5~~20 Business Days of any reasonable request by any other Party.'

Schedule 25 Clause C.1.3 (b) should read; 'The CMA shall notify the Trading Parties of any proposed change to the Market Privacy Notice and give Trading Parties ~~10~~15 Business Days to comment, or ~~15~~20 Business Days if the proposed change adds an additional purpose of processing. The CMA will take any comments into account but will not be obliged to effect any suggested changes.'

Schedule 25; In a number of instances, the term 'Parties' occurs and these should be replaced with 'Trading Parties' or 'Code Parties' (or the singular thereof), as applicable, since these are the defined terms.

B.2.d. TP ASSESSMENT
Taking into account complexity, importance and urgency, and having regard to whether or not such proposal is within the relevant Objectives and Principles as required under Market Code Parts 8.7.1 (v) and 8.8.1 (iv)

Impact on Principles and Objectives (if different from that originally submitted)	
Cost Estimate	CMA website updates and CMA Admin System updates. Cost Model assumptions suggest: £16k

Benefit Estimate (L: < 10k, M: £10k to £100k, H: > £100k)	Legal requirement.
B.3. TP DECISION	TP APPROVED
B.4. FINAL TP VIEWS	
B.5. PLANNED IMPLEMENTATION DATE	March/April 2018

WITHDRAWN BY PROPOSER?	NO
COMMENTS	
DATE OF WITHDRAWAL	

PART C — COMMISSION APPROVAL	
C.1. DATE FINAL REPORT ISSUED TO COMMISSION	2018/03/02
C.2. APPROVAL STATUS	APPROVED CHANGE / REJECTED
C.3. DATE OF APPROVAL STATUS	yyyy-mm-dd
C.4. COMMISSION RESPONSE REFERENCE	

PART D — IMPLEMENTATION	
D.1. IMPLEMENTATION DATE	yyyy-mm-dd
D.2. IMPLEMENTATION DETAILS (MC version, CSD versions, CMA Central Systems release number, etc.)	