Schedule 25

Data Protection

This schedule sets out how the Parties will allocate and discharge their respective responsibilities as Data Controllers of Market Personal Data.

A DATA GOVERNANCE

1. Summary of Arrangements

1.1 Data Controllers who jointly control how Market Personal Data is processed must make available to Data Subjects a summary of the arrangements and allocation of responsibilities between them (which may include a summary of matters dealt with in this Schedule).

1.2 **Allocation of responsibilities**

The CMA shall produce and publish on its website a summary of the arrangements for the sharing of Market Personal Data between Code Parties, including compliance with Data Subject rights and the provision of privacy notices.

1.3 **Interactions to deliver compliance**

The CMA shall:

(a) Provide a copy of its proposed summary (and thereafter any changes to it) to all Trading Parties for review and comment;

(b) Trading Parties shall provide comments within 20 Business Days of receipt of the summary or any proposed changes to it;

2. Nominated Contact Points

2.1 Data Controllers may be obliged by law or may elect to appoint a Data Protection Officer (as defined by Data Protection Laws). In cases where a Data Protection Officer has not been appointed, Data Controllers will nevertheless be required to provide contact point details to the CMA of appropriate personnel to ensure that any data protection issues that may arise can be promptly notified.

2.2 **Allocation of Responsibilities**

(a) All Trading Parties will provide the CMA with details of their nominated contact point for any data protection issues that may arise.

2.3 **Interactions to deliver compliance**

(a) The details to be provided by Trading Parties for their nominated contact points include name, job title, email address and business telephone number. Details should be provided for queries arising both during and out of Business Hours.

(b) All Trading Parties must promptly advise the CMA of any change to their nominated contact point.

B DATA MANAGEMENT

1. Review of Market Personal Data

1.1 Market Personal Data shall be limited to what is necessary for the purpose for which they are processed.

1.2 **Allocation of responsibilities**

Once a year the Technical Panel shall review the Market Personal Data that is processed to assess whether the Market Personal Data captured and stored is necessary for the proper operation of the Market Code and is no more than is required for this purpose.

2. Privacy by Design

2.1 Data Controllers shall adopt internal compliance policies and implement appropriate technical and organisational measures to meet the principles of privacy by design and by default

2.2 **Allocation of responsibilities**

(a) Each of the Code Parties shall implement internal policies and processes to ensure that only those within its organisation with a legitimate requirement to access the Market Personal Data can do so**;**

(b) The CMA shall implement, or instruct the implementation of, measures in relation to pseudonymisation of Market Personal Data where it is possible and practical to do so.

2.3 **Interactions to deliver compliance**

A Code Party shall provide evidence in writing of compliance with the above within 20 Business Days of any reasonable request by any other Code Party.

3. Privacy Impact Assessments

3.1 Privacy impact assessments are required to be conducted by Data Controllers where processing of Market Personal Data is likely to result in a high risk to the rights of Data Subjects

3.2 **Allocation of responsibilities**

(a) The CMA shall be responsible for ensuring there is a clear process for conducting privacy impact assessments on any changes to the processing of Market Personal Data to identify its necessity and proportionality, any impact upon Data Subjects and how such impacts could be mitigated or addressed.

(b) The CMA shall be responsible for reviewing any privacy impact assessment regarding the Market Personal Data.

(c) Trading Parties shall provide such information and assistance to the CMA as is necessary and reasonable in order for it to ensure the appropriate conduct of privacy impact assessments

3.3 **Interactions to deliver compliance**

The CMA shall:

(a) Share the outcome of any relevant privacy impact assessment with Trading Parties including any recommended actions;

(b) Liaise accordingly with Trading Parties and any other third party to ensure any recommended actions are implemented accordingly;

(c) Document the above process and outcomes as appropriate.

4. Records of Processing

4.1 Each Data Controller must maintain a formal written record of processing activities under its responsibility which shall include the legal basis upon which any processing of Market Personal Data is conducted as well as any other requirements under Data Protection Laws.

4.2 **Allocation of responsibilities**

(a) The CMA shall produce and maintain a description of processing for Market Personal Data undertaken for the proper operation of the Market Code.

(b) Trading Parties shall provide such information and assistance to the CMA as is necessary and reasonable in order for it to produce and maintain the description of processing activities.

4.3 **Interactions to deliver compliance**

(a) As a part of the annual review of Personal Market Data, the CMA shall make available to the Technical Panel, a copy of the description of processing activities.

(b) Trading Parties shall provide any comments which require to be taken account of or corrections which require to be made to the processing to the CMA following the review.

C USE OF PERSONAL DATA

1. Privacy Notices

1.1 Data Controllers must provide to Data Subjects fair processing information or notices that set out particular information in terms of the Personal Data, the rights of Data Subjects and obligations of Data Controllers in accordance with Data Protection Laws. Parties shall process Market Personal Data only in accordance with such fair processing information or notices.

1.2 **Allocation of responsibilities**

(a) The CMA shall publish a privacy notice on its website regarding Market Personal Data (**"the Market Privacy Notice"**). This shall include the information required by Data Protection Laws and specifically must include both the purpose and legal basis for processing.

(b) Licensed Providers shall ensure that privacy notices, consistent with the Market Privacy Notice, are provided to Data Subjects to whom they deliver services.

(c) All Code Parties shall maintain privacy notices consistent with the Market Privacy Notice for the purposes of Market Personal Data and shall process Market Personal Data only in accordance with such privacy notices.

1.3 **Interactions to deliver compliance**

(a) Any Code Party (including the CMA) may request a change to the Market Privacy Notice.

(b) The CMA shall notify the Trading Parties of any proposed change to the Market Privacy Notice and give Trading Parties 15 Business Days to comment, or 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.

(c) If the Market Privacy Notice is to be amended to permit the processing of Market Personal Data for an additional purpose then each Party shall update or amend its privacy notices, accordingly. Licensed Providers shall provide the Data Subjects associated with Supply Points for which they are responsible with a suitably updated or amended privacy notice within the timescales set under the Data Protection Laws.

D DATA SUBJECTS RIGHTS

1. Guidance

1.1 Data Controllers must provide guidance to Data Subjects on how their Data Subject rights can be exercised.

1.2 **Allocation of responsibilities**

(a) The CMA shall provide guidance on the CMA's website about how Data Subject rights may be exercised with regard to Market Personal Data.

(b) Each Code Party shall ensure that its own published statement about the exercise of Data Subject rights with regard to Market Personal Data is consistent with the statement on the CMA's website as published from time to time.

1.3 **Interactions to deliver compliance**

(a) The CMA shall notify the Trading Parties of any proposed changes to the wording on the CMA website about the exercise of Data Subject Rights and give Trading Parties 10 Business Days to comment.

(b) The CMA will take any comments from Trading Parties into account in determining the published wording. The CMA shall act reasonably when

deciding on the proposed wording and any subsequent changes to the wording but but will not be obliged to effect any suggested changes.

2. Data Subjects Access Request

2.1 Data Subjects can access their Market Personal Data and information about their Market Personal Data by making a Data Subject access request to Data Controllers.

2.2 Data Controllers may be required to provide Personal Data in a commonly used machine readable format to a Data Subject within one month (or two months for complex cases) of a request by a Data Subject.

2.3 **Allocation of responsibilities**

(a) Licensed Providers shall be responsible for the provision of Market Personal Data, in response to a Data Subject access request from a Data Subject associated with one or more Supply Points associated with that Licensed Provider. Such data should be provided in a machine readable format.

(b) The CMA shall be responsible for the provision of Market Personal Data, in response to a request from a Data Subject that is associated with a Trading Party. Such data should be provided in a machine readable format.

(c) The CMA shall make Market Personal Data available for the use of Licensed Providers, on request. The provision of such Market Personal Data to be treated as an Additional Service.

2.4 **Interactions to deliver compliance**

(a) If a Licensed Provider receives a request to exercise Data Subject access rights in relation to Market Personal Data from a Data Subject associated with one or more Supply Points associated with that Licensed Provider:

(i) If the Licensed Provider wishes to request that the CMA shall provide such Market Personal Data via an Additional Service, the Licensed Provider should first provide the duly completed Data Subject Access Request form. The CMA shall then provide the Market Personal Data to the Licensed Provider within 10 Business Days of receipt of the duly completed Data Subject Access Request form.

(ii) It shall be the responsibility of the Licensed Provider receiving the Data Subject Access Request form to respond to the request and provide the relevant data to the Data Subject (where appropriate) within the one month or two month time limit, as the case may be, imposed by Data Protection Laws.

(iii) The Licensed Provider shall confirm to the CMA that it has dealt with the request in accordance with Data Protection Laws by sending the CMA a Confirmation form within 2 Business Days of issuing the response to the Data Subject.

(b) If the CMA receives a request to exercise the right of subject access in relation to Market Personal Data relating to an individual associated with a Trading Party, the Trading Party should first provide the duly completed Data Subject Access Request form on behalf of that individual. The CMA shall then provide the Market Personal Data to the Trading Party within 10 Business Days of receipt of the duly completed Data Subject Access Request form.

(c) If the CMA, or Scottish Water, receives a request to exercise Data Subject access rights in relation to Market Personal Data from a Data Subject associated with one or more Supply Points associated with a Licensed Provider, or if a Licensed Provider receives a request from a Data Subject associated with another Licensed Provider, the CMA, Scottish Water, or the Licensed Provider will re-direct that Data Subject to the appropriate Licensed Provider.

(d) The CMA shall maintain a log of all Data Subject Access Requests made to the CMA from Trading Parties and the responses to any such requests.

3. Request for Correction/Rectification

3.1 Data Controllers may be required to correct or rectify Market Personal Data or to place a supplementary statement alongside allegedly incomplete Market Personal Data within one month (or two months for complex cases) of a request from a Data Subject.

3.2 **Allocation of responsibilities**

(a) Licensed Providers shall be responsible for initiating the rectification of data, in response to a Data Subject rectification/correction request for any Market Personal Data, from a Data Subject associated with one or more Supply Points associated with that Licensed Provider.

(b) Data rectification/correction shall be delivered in accordance with CSD0105.

4. Changes to Processing

4.1 Data Controllers may, in certain circumstances, be required to stop processing certain Market Personal Data within one month (or two months for complex cases), so far as is reasonably practicable, of a request to do so from a Data Subject. Where the objection relates to direct marketing, Data Controllers must stop processing Market Personal Data for direct marketing purposes as soon as an objection is received and there are no exemptions or grounds to refuse.

4.2 Data Controllers may be required to erase Market Personal Data in certain circumstances within one month (or two months for complex cases), so far as is reasonably practicable, of a request by a Data Subject.

4.3 Data Controllers may be required to restrict the processing of Market Personal Data in particular circumstances within one month (or two months for complex cases), so far as is reasonably practicable, of a request by a Data Subject.

4.4 **Allocation of responsibilities**

(a) Licensed Providers shall be responsible for progressing a request from a Data Subject regarding any objection or restriction to the processing of Market Personal Data.

(b) The CMA shall make any agreed changes to processing within the Central Systems and within the Scottish Landlord Portal, to accommodate the objection or restriction to the processing of Market Personal Data.

(c) Trading Parties shall make any agreed changes to processing by their systems, to accommodate the objection or restriction to the processing of Market Personal Data.

4.5 **Interactions to deliver compliance**

(a) If a Licensed Provider receives a request to exercise the right of objection, restriction, or erasure, in relation to Market Personal Data from a Data Subject associated with one or more Supply Points associated with that Licensed Provider. The Licensed Provider shall submit a duly completed Processing Change Request form to the CMA.

(b) If the CMA or Scottish Water receives a request regarding any objection or

restriction to the processing of Market Personal Data from a Data Subject associated with one or more Supply Points associated with a Licensed Provider, or if a Licensed Provider who is not associated with the Data Subject receives a request, the CMA, Scottish Water, or the Licensed Provider will re-direct that Data Subject to the relevant Licensed Provider.

(c) If the CMA receives a request from a Licensed Provider, to exercise the right to object, restrict, or erase, in relation to Market Personal Data:

(i) The CMA shall first consider whether it is possible and necessary to comply with any such request in accordance with Data Protection Laws.

(ii) If the CMA does consider it is possible and necessary to comply then it shall inform relevant Data Owners about the request using the Processing Change Request form, within 10 Business Days, along with recommended actions to be undertaken by each Trading Party and the CMA. The CMA shall obtain the Data Owner's relevant consent. Any such actions should be set out in accordance with Section 8.7 of the Market Code, in respect of any changes to the Market Code. Any action undertaken by the CMA, other than a change to the Market Code, will be treated as an Additional Service.

(d) It shall be the responsibility of any Trading Party receiving the Processing Change Request form to respond to the request and take any appropriate actions within 10 Business Days.

(e) Each relevant Trading Party shall confirm to the CMA that it has fulfilled its actions as per the request in accordance with Data Protection Laws by sending the CMA a Confirmation form within 5 Business Days of taking any such appropriate actions.

(f) The CMA shall inform the Licensed Provider that received the request from the Data Subject that all actions related to the request have been completed, within 5 Business Days of such completion and within one month (or two months for complex cases), so far as is practical, of the request being initiated, using the Confirmation form.

(g) The Licensed Provider that received the request from the Data Subject shall notify the Data Subject on the actions taken within 2 Business Days of receipt

of the notification of completion by the CMA and shall confirm that such notification has been made, to the CMA, within 2 Business Days of that notification, using the Confirmation form.

(h) The CMA shall maintain a log of all Data Subject Processing Change Requests made to the CMA from Licensed Providers and the responses to any such requests.

E DATA SECURITY

1. Standards of Security

1.1 Data Controllers must have in place appropriate technological and organisational security measures having regard to the state of technological development and cost of implementation, the nature, scope, context, and purposes of the processing as well as the risk of and impact on Data Subjects. The measures must ensure a level of security appropriate to the risk, including as appropriate:

(a) the pseudonymisation and encryption of Market Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Market Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.2 **Allocation of responsibilities**

(a) Each Code 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 Offices' Practical Guide to IT Security, Ideal for the Small Business, or Cyber Essentials/Cyber Essentials Plus, or ISO27001 [Cyber Essentials Scheme****].

(b) Each Trading Party must remain compliant with CSD0001, which shall

include suitable obligations regarding data protection.

1.3 **Interactions to deliver compliance**

(a) Processes described in CSD0001 to ensure ongoing compliance shall be followed.

2. Notification of Data Security Breaches

2.1 Data Controllers must notify (i) the Information Commissioner and (ii) Data Subjects of the occurrence of a Market Personal Data breach, unless such breach is unlikely to result in a risk to the rights and freedoms of affected Data Subjects. Such notifications must be notified within 72 hours of a Data Controller becoming aware of such a breach. Data Subjects must be notified without undue delay.

2.2 **Allocation of responsibilities**

(a) Within 24 hours of becoming aware of an actual or likely Market Personal Data breach, a Code Party shall notify all nominated contact points of the other Code Parties of that actual or likely Market Personal Data breach, via the CMA.

(b) All Code Parties shall be responsible and liable for any actions and consequences arising from their own Market Personal Data breaches.

(c) In the event of a Market Personal Data breach that has or is likely to have a material impact on the Market Dataset, the CMA shall co-ordinate / direct how this is to be handled including any notifications to be made to the Information Commissioner and/or affected Data Subjects. This shall not prevent any Code Party from complying with their obligations under the Data Protection Laws.

(d) All Code Parties must have in place appropriate policies and processes setting out how they will deal with the occurrence of a Market Personal Data breach.

2.3 **Interactions to deliver compliance**

(a) All Parties shall maintain, as a minimum:

(i) A Market Personal Data security breach response policy together with appropriate template documents that clearly demonstrate the process that the Party will follow in the event of a Market Personal Data breach; and

(ii) A Market Personal Data breach register.

(b) The Trading Parties shall confirm that their Market Personal Data breach policy documents comply with these requirements as part of the processes identified under CSD0001.

(c) the CMA shall make available to any Trading Party within 5 Business Days of any request a copy of the CMA's Market Personal Data breach policy documents.