Part 6 Data Protection

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

A DATA GOVERNANCE

1. Summary of Arrangements

1.1 Data Controllers who jointly control how Operational 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 Part).

1.2 Allocation of responsibilities

Each Party to the Operational Code shall produce and publish on its website a summary of the arrangements for the processing of Operational Personal Data including the transfer of such information between itself and SW in the case of an LP or between itself and each LP in the case of SW or between any Party and the CMA. The summary of arrangements shall include compliance with Data Subject rights and the provision of privacy notices.

2. Nominated Contact Points

2.1 SW shall provide each LP and each LP shall provide SW with contact point details of appropriate personnel to ensure that any data protection issues that may arise can be promptly notified.

2.2 Interactions to deliver compliance

2.2.1 It is expected that the personnel nominated for the Operational Code shall be the same as those nominated under Schedule 25 of the Market Code but to the extent that there are different personnel for Operational Personal Data the Code Party shall provide guidance as to what issues should be dealt with by different personnel. The details to be provided by 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 the Business Day.

2.2.2 All Parties must promptly advise any change to their nominated contact point details to any other Party to whom they are required to provide contact point details.
2.2.3 Parties may also choose to provide a dedicated email box for such correspondence.

B DATA MANAGEMENT

3. Review of Operational Personal Data

3.1 Each Party shall ensure that Operational Personal Data that they process including any Operational Personal Data they transfer to another Party or to the CMA shall comply with the requirements of Article 5 of the GDPR and any similar requirements under Data Protection Law.

4. Privacy by Design

4.1 Data Controllers shall adopt internal compliance policies and implement appropriate technical and organisational measures to meet the requirements of Article 25 of the GDPR and any similar requirements under any other Data Protection Law.

4.2 Allocation of responsibilities

Each of the Parties shall implement internal policies and processes to ensure that persons within its control are only authorised to access the Operational Personal Data where they have a legitimate requirement to do so.

4.3 Interactions to deliver compliance

The Parties shall provide evidence in writing of compliance with the above within 10 Business Days of any reasonable request by any other Party to whom they transfer data under this Code.

5. Data Protection Impact Assessments

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

5.2 Allocation of responsibilities

5.2.1 A clear process for conducting privacy impact assessments on any changes to the processing of Operational Personal Data to identify its necessity and proportionality, any impact upon Data Subjects and how such impacts could be mitigated or addressed will be established under the Market Code.

5.2.2 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.

6. Records of Processing

6.1 Each Data Controller must maintain a formal written record of processing activities under its responsibility which shall include the legal basis upon which any transfer of Operational Personal Data between that Party and any other Party or the CMA is conducted as well as any other requirements under Data Protection Laws.

6.2 Allocation of responsibilities

6.2.1 Each Party shall produce and maintain a description of processing for Operational Personal Data undertaken for the proper operation of the Operational Code consistent with the terms of Article 30 of the GDPR or any other similar requirement in Data Protection Law.

C USE OF PERSONAL DATA

7. Privacy Notices

7.1 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.

7.2 Each Party shall publish such a notice in relation to the processing of Operational Personal Data that they undertake. Such information or notices shall include information about the circumstances in which Personal Data may be transferred between the Parties. Parties shall process Operational Personal Data only in accordance with such fair processing information or notices.

D DATA SUBJECTS RIGHTS

8. Guidance

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

8.2 Allocation of responsibilities

Each Party shall publish a statement on its website in relation to the exercise of Data Subject rights with regard to their processing of Operational Personal Data including the transfer of Operational Personal Data to any other Party or to the CMA.

9. Requests from Data Subjects
9.1 Data Subjects rights include the ability to make the following requests, complaints or claims in relation to Operational Personal Data.

9.1.1 Requests to access their Personal Data

Data Subjects can access their Operational Personal Data and information about their Operational Personal Data by making a Data Subject access request to Data Controllers. Data Controllers may be required to provide Personal Data within one month (or two months for complex cases) of a request by a Data Subject.

9.1.2 Requests for correction or rectification of data

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

9.1.3 Requests to stop processing certain Personal Data

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

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

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

9.1.4 Complaints

Other complaints and/or communications requiring a response ("Complaints") may be received from Data Subjects in relation to Operational Personal Data that are not covered in the sections above.

9.1.5 Claims

A Data Subject is entitled to bring a data protection breach claim ("Claim")
against any Data Controller who was involved with the relevant processing of their Personal Data and does not need to identify which particular Data Controller is at fault. Data Controllers can effectively have joint and several liability for Claims by Data Subjects.

9.1.6 Data Controllers have a duty to notify others affected Parties following amendment, rectification, deletion or restriction of processing where this happens at the request of a Data Subject or following a complaint or claim by a Data Subject. In all cases Parties will cooperate to fulfil the exercise of the Data Subject’s rights.

9.2 Customer Personal Data

9.2.1 Where a Data Subject is associated with one or more Supply Points registered to a Licensed Provider, that Licensed Provider shall be responsible for ensuring that the Data Subject is able to exercise its Data Subject Rights by providing an appropriate response to the request, complaint or claim as the case may be within the time limit imposed by Data Protection Laws. To the extent that the request, complaint or claim relates to Personal Data processed by more than one Party, all affected Parties shall cooperate with the responsible LP to fulfil the Data Subject's rights. In all cases such data should be provided to the Data Subject in a commonly used machine readable format.

9.2.2 Where SW receives a request, complaint or claim in relation to Operational Personal Data from a Data Subject associated with one or more Supply Points associated with a Licensed Provider, it shall promptly pass that request to that Licensed Provider and that LP shall then be responsible for the resolution of that request, complaint or claim.

9.2.3 Where SW receives a request, complaint or claim from a Data Subject which has not appointed a Licensed Provider in relation to the Premises that the request relates to, it shall be responsible for the resolution of the request, complaint or claim. To the extent that the request, complaint or claim nevertheless relates to Personal Data processed by more than one Party, all affected Parties shall cooperate with the responsible LP to fulfil the Data Subject’s rights. In all cases such data should be provided to the Data Subject in a commonly used machine readable format.

9.3 Employee Personal Data

Each Party shall be responsible for ensuring that Data Subjects are able to exercise their Data Subject rights as set out in Data Protection Laws in relation to a request,
complaint or claim which relates to the Employee Personal Data of a Data Subject associated with their organisation. This responsibility includes, where necessary, the provision of Employee Personal Data in response to a Data Subject access request. To the extent that the request, complaint or claim relates to Employee Personal Data processed by another Party, that other Party shall cooperate with the Party which received the request, complaint or claim to ensure that the Data Subject is able to exercise their Data Subject rights. In all cases such data should be provided in a commonly used machine readable format.

9.4 Interactions to deliver compliance with Data Subject access requests

If a Licensed Provider or SW receives a request to exercise Data Subject access rights and it is responsible for that request as set out in Section 9.2, it shall within the timescale set out in the Data Protection Laws provide such data and information as is required for compliance with the Data Protection Laws. The LP or SW may request the cooperation of SW or any LP or the CMA as the case may and this cooperation will not unreasonably be withheld.

9.5 Interactions to deliver compliance with requests for correction/rectification

If a Licensed Provider or SW receives a request for correction/rectification and it is responsible for that request as set out in Section 9.2 it shall within the timescale set out in the Data Protection Laws correct and/or rectify any such data as is necessary for compliance with the Data Protection Laws. The LP or SW may request the cooperation of SW or any LP or the CMA as the case may and this cooperation will not unreasonably be withheld.

9.6 Interactions to deliver compliance in relation to changes to processing

If a Licensed Provider or SW receives a request to exercise the right of objection, restriction, or erasure, in relation to Operational Personal Data and it is responsible for that request as set out in Section 9.2:

(i) The LP or SW as the case may be shall first consider whether it is possible and necessary to comply with any such request in accordance with Data Protection Laws.

(ii) If the LP or SW does consider it is possible and necessary to comply then it shall pass that request on to all Parties who may reasonably be affected by the request and to the CMA if appropriate along with recommended actions to be undertaken by each Party. The recipient of such a request shall take reasonable steps to comply with that request.

9.7 Interactions to delivery compliance in relation to duty to notify others following amendment, rectification, deletion or restriction at Data Subject’s request
9.7.1 If a Licensed Provider or SW receives a request for any rectification, erasure or restricted processing and it determines that it is possible and necessary to comply with that request it shall notify other relevant Parties and the CMA as appropriate if it is possible and proportionate to do so.

9.8 Interactions to deliver compliance in relation to complaints from Data Subjects

If a Licensed Provider or SW receives a complaint from a Data Subject that it is responsible for as set out in Section 9.2:

9.8.1 The LP or SW shall first consider whether it is possible and necessary to accommodate the Complaint in accordance with Data Protection Laws.

9.8.2 If the LP or SW does consider it is possible and necessary to comply then it shall pass that complaint on to any Party who may reasonably be affected by the complaint and to the CMA if appropriate along with recommended actions to be undertaken by each Party.

9.8.3 It shall be the responsibility of any Party receiving the Complaint to respond and take any appropriate actions as soon as may be practical.

9.8.4 If the Complaint involves the Information Commissioner, the Licensed Provider or SW shall respond to the Information Commissioner within 2 Business Days of recommended actions being identified to them and also within 2 Business Days of notifying the Data Subject of the completion of actions taken.

9.9 Interactions to deliver compliance in relation to claims brought by Data Subjects

Each Party shall be responsible for any Claims arising out of their own acts, omissions, negligence, fault or breaches in relation to Operational Personal Data.

9.9.1 If a Licensed Provider or SW receives a Claim that it is responsible for as set out in Section 9.2 it shall within the timescale set out in the Data Protection Laws respond to that Claim.

9.9.2 The LP or SW shall promptly copy the Claim to any other Party affected by the Claim and to the CMA if they are affected by the Claim.

9.9.3 The LP or SW may request the cooperation of SW or any LP in resolving the Claim as the case may and the Parties shall use reasonable endeavours to provide any necessary assistance to each other in the conduct and handling of any such Claims.

E DATA SECURITY
10. Standards of Security

10.1 Data Controllers must comply with the requirements of Article 32 of the GDPR and any similar requirements under any other Data Protection Law. The measures must ensure a level of security appropriate to the risk, including as appropriate:

(a) the pseudonymisation and encryption of Operational 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 Operational 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.

10.2 Allocation of responsibilities

(a) Each Party must implement appropriate technical and organisational security measures for their own systems that meet the requirements of Data Protection Laws and are consistent with or equivalent to industry standards, and frameworks including in particular ISO27001 [Cyber Essentials Scheme****] including the holding of any recognised accreditations or certifications evidencing such compliance.

11. Notification of Data Security Breaches

11.1 Data Controllers must in certain circumstances notify (i) the Information Commissioner and (ii) Data Subjects of the occurrence of an Operational Personal Data breach. The Information Commissioner must be notified within 72 hours of a Data Controller becoming aware of such a breach. Data Subjects must be notified without undue delay.

11.2 Allocation of responsibilities

(a) Within 24 hours of a Party becoming aware of an actual or likely Operational Personal Data breach, if the Party is SW, they shall contact all nominated contact points of the other Parties whose data has or may have been subject to a breach, and if the Party is an LP they shall contact the nominated contact point of SW. In each case they shall notify the other Party or Parties of that actual or likely Operational Personal Data breach.

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

(c) In the event of an Operational Personal Data breach that has or is likely to have a material impact on data subject rights, the Party most closely associated with the data
breach shall co-ordinate how this is to be handled including any notifications to be made to the Information Commissioner and/or affected Data Subjects, or if it is not agreed which Party is most closely associated with the data breach then all affected Parties shall cooperate co-ordinate in 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 Party from complying with their obligations under the Data Protection Laws.

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

11.3 **Interactions to deliver compliance**

All Parties shall maintain, as a minimum:

(a) An Operational 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 an Operational Personal Data breach; and

(b) An Operational Personal Data breach register, which may be the same document as the Market Personal Data breach register.