An Coimisiún
um Rialáil Fóntas
Commission for
Regulation of Utilities

Smart Meter Data Access Code

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

The Smart Meter Data Access Code

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Change Proposal included in this version	Change Proposal effective Date	Code Clauses Modified	Code Version if applicable
	DD-Mon-YY		n.n

1 Introduction

1.1. The purpose of this Code is to set out the rules and procedures for accessing and Processing of Smart Meter Data.

1.2. All references to "the Code", unless otherwise specified or implied by the context, shall be deemed to be references to the Smart Meter Data Access Code.

1.3. Smart Meter Data Access Code was developed by the Commission for Regulation of Utilities ("the Commission"), which was designated as the Competent Authority in accordance with Article 3 of 2019 EU Regulation on risk preparedness in the electricity sector ((EU) 2019/941) in August 2020, to manage and take responsibility for the tasks outlined in the Regulation and in accordance with Statutory Instrument 426 of 2014, and to enact the data management provisions of Statutory Instrument (SI) 37 of 2022.

1.4. Without prejudice to its right to delegate to a Code Manager and Code Compliance Officer, both of which may not be a Party or an Other User nor in the case of the Code Compliance Officer be affiliated with a Party or an Other User, the Commission shall enter into and at all times administer and maintain in force a Code which:

(a) sets out the terms of the arrangements for the access and Processing of Smart Meter Data;

(b) is designed to facilitate the achievement of the Code Objectives set out in Clause 2: Code Objectives, below; and

(c) contains Modification procedures which provide that any Modifications to the Code must be subject to the prior approval by either the Commission or the Panel under the circumstances set out in, and in accordance with, Clause 15: Change Management.

2 Code Objectives

2.1. The aim of this Code is to facilitate the achievement of the following objectives to:

(a) facilitate the efficient discharge by the Distribution System Operator (DSO), including as a Data Systems Provider, of the obligations imposed upon it by its Distribution System Operator Licence and SI 37/2022;

(b) facilitate the efficient discharge by Electricity Suppliers of the obligations imposed upon them by their Electricity Supply Licences and SI 37/2022;

(c) provide access to Metering and Consumption Data for Final Customers, eligible Parties and Other Users;

(d) facilitate the interoperability and increase the effectiveness of transactions that involve data access and exchange by market participants, and ultimately of energy services;

(e) ensure the protection of Final Customer Data and the security of Data and Systems in the operation of this Code;

(f) facilitate the efficient and transparent administration and implementation of this Code; and

(g) ensure no undue discrimination between persons who are Parties or Other Users.

3 Appendices and Schedules

3.1. The Appendices and the Schedules, as may be amended or modified from time to time, shall be construed as, and form part of, this Code and shall be subject to the terms of this

Code. The Schedules set out the detail of procedures to be followed by Parties and Other Users in performing obligations and functions under this Code.

4 Definitions and Interpretation

4.1. The defined terms and other rules of interpretation used in this Code are set out in the Schedule 1: Interpretations.

5 Categories of Parties and Data Access

5.1. The following categories of person are eligible to become a Party (Eligible Party):

(a) the DSO;

(b) Electricity Suppliers;

(c) the Transmission System Operator (TSO); and

(d) The Single Market Operator (SMO).

5.2. In addition to 5.1, the Commission is a Party for the purpose of the administration and maintenance of this Code but is not entitled to access Data.

5.3. The DSO is eligible to become a Party for the purpose of:

(a) the collection and Processing of Smart Meter Data, acting as the Data Systems Provider (DSP); and

(b) for the purpose of the business authorised by its Licence.

5.4. Electricity Suppliers are eligible to become Parties for the purpose of the business authorised by their Licence.

5.5. The TSO is eligible to become a Party for the purpose of the business authorised by its Licence.

5.6. The SMO is eligible to become a Party for the purpose of the business authorised by its Licence.

5.7. The Access Agreements for those Eligible Parties is set out in Schedule 2: Access Arrangements.

5.8. Other organisations cannot become a Party, but some organisations which are not Parties are able to obtain access to Smart Meter Data either:

(a) by entering into an Access Agreement as an Other User, as further described in Schedule 2: Access Arrangements; or

(b) as provided directly from each individual Final Customer.

5.9. Final Customers cannot become a Party, but may, in accordance with the provisions of Schedule 5: Data Privacy:

(a) obtain access to their own Smart Meter Data from the DSO or their Electricity Supplier in accordance with their rights as Final Customers; and

(b) provide such to a Party or Other Party, as they see fit.

6 Becoming a Party

6.1. This Clause is to be read in accordance with Schedule 2: Access Arrangements, Schedule 3: Accession and Schedule 6: Assessments.

6.2. A person may only become a Party to the Code in accordance with the terms of the Code.

6.3. In order to become a Party, a person (the "Applicant") must apply to the Code Manager in accordance with Schedule 3: Accession. Schedule 3 specifies all conditions which the Applicant must meet to become a Party which include that the Applicant shall, when provided, execute the Accession Agreement to adhere to the Code.

7 Compliance

7.1. This Clause 7 sets out the Entry Assessment criteria that must be met by organisations who wish to become a Party to this Code, or to access any Smart Meter Data System as an Other User subject to an Access Agreement in accordance with Schedule 2: Access Arrangements.

7.2. This Clause 7 also sets out the post entry assurance and compliance provisions for Parties and Other Users. The process is designed to provide assurance that a Party's or Other User's Systems, processes and information security standards are compliant with the provisions of this Code and with associated legislation.

Entry Assessment

7.3. For a Party to become a user of the Smart Meter Data System and receive access to Smart Meter Data, they must first successful complete an Entry Assessment and receive confirmation from the Code Compliance Officer that it has successfully demonstrated the appropriate data security and data privacy controls to meet the requirements of Schedule 4: Data Security and Schedule 5: Data Privacy.

7.4. The scope of activities required as part of Entry Assessment will vary depending on the User Category and the category of Data that the Party or Other User is applying to access.

7.5. Prior to becoming a Party in accordance with Clause 6.2 and accessing the Smart Meter Data System, each person must complete an Entry Assessment to demonstrate that it is able to comply with its obligations under this Code, as set out in Schedule 4: Data Security and Schedule 5: Data Privacy prior to accessing the Smart Meter Data System.

7.6. Each Other User must have completed an Entry Assessment before being approved to access any Smart Meter Data System and prior to accessing the Smart Meter Data System. Each Other User's Access Agreement will specify the security and privacy requirements applicable to each Other User Category.

Code Audit

7.7. The Commission shall instruct the Code Compliance Officer to conduct an audit of the Code, associated Code procedures and processes, Code operation and governance of the Code at least once a year.

Compliance and Assurance

7.8. An Assurance Strategy will be developed and maintained by the Code Compliance Officer in accordance with Schedule 6: Assessments. The scope of assurance activities and

assurance techniques to be applied will be defined within this Strategy. The Assurance Strategy shall be approved by the Panel.

7.9. All Parties and Other Users and the DSP shall be required to complete an annual Data Security and Data Privacy Assessment (Annual Self-Assessment). The scope of this Assessment will be based on the User Category, with details provided within the Assurance Strategy.

7.10. The Panel reserves the right to subject any Party or Other User, the Code Manager or the DSP to an Ad-Hoc Assessment, if deemed necessary by the Code Compliance Officer in accordance with Schedule 6: Assessments.

7.11. The Code Compliance Officer shall provide advice and guidance regarding compliance with this Code to Parties and Other Users intending to make changes to their information security standards, Systems and processes.

7.12. Parties and Other Users found non-compliant with the obligations imposed by the Code as a result of the Assessment may be considered to be in breach of the Code, in accordance with Clause 21: Events of Breach and Consequences of Breach.

8 Panel

Establishment of the Panel

8.1. The Panel shall be established in accordance with the further provisions of this Clause 8.

8.2. It is acknowledged that, in conducting its activities in accordance with Clauses 8.5 to 8.6, the Panel shall Process Personal Data as a Data Controller.

8.3. The Panel shall:

(a) pursue the objectives, undertake the duties, and have the powers set out in Clauses 8.4 to 8.6 and as delegated by the Commission as the Commission determines within the remit of the Commission's purpose under this Code, as defined under Clause 5.2;

(b) be composed of the Panel Members described in Clauses 8.7 to 8.9 and in accordance with Schedule 7: Panel, some of whom will be elected; and

(c) conduct its activities in accordance with the procedures set out in Schedule 7: Panel.

Panel Objectives

8.4. The Panel shall, in all its activities, always act in a manner designed to achieve the following objectives:

(a) that this Code is given full and prompt effect in accordance with its provisions, in a manner consistent with the Code Objectives, and without undue discrimination between Parties or Other Users or any classes of Party or Other User; and

(b) that the Panel conducts its affairs in an open and transparent manner.

Panel Duties

8.5. The Panel shall have the power to do anything necessary for, or reasonably incidental to, the governance, management, operation or other purposes of this Code, which shall include but not limited to:

(a) oversee the process by which Applicants apply to become a Party, as set out in

Clause 6: Becoming a Party;

(b) approve the addition of new User Categories under the Code, as per the process in accordance with Schedule 2: Access Arrangements;

(c) approve the Entry Assessment criteria that must be met by organisations who wish to become a Party, or to access any Smart Meter Data System as an Other User and post entry assurance and compliance provisions for Parties and Other Users, as set out in Clause 6: Compliance;

(d) oversee and co-ordinate the process for assessing and approving certain Modification Proposals and Change Proposals, and implement successful Modification Proposals and Change Proposals, each as set out in Clause 15 Change Management;

(e) oversee and co-ordinate the process and obligations for data security and data privacy, each set out in Clause 17 Data Security and Data Privacy Obligations and Schedule 4: Data Security and Schedule 5: Data Privacy;

(f) oversee and co-ordinate arrangements in response to a Force Majeure under or in relation to this Code, as set out in Clause 18 Force Majeure;

(g) manage and co-ordinate arrangements for the resolution of certain Disputes under or in relation to this Code, as set out in Clause 19: Disputes;

(h) oversee and co-ordinate the process for assessing and approving derogations to this Code, and their retracting, additions and amendments, in accordance with Clause 20: Derogations;

(i) investigate the circumstances relating to such potential Event of Breach, as set out in Clause 21: Events of Breach and Consequences of Breach;

(j) take one or more steps in relation to an Event of Breach, as set out in Clause 21: Events of Breach and Consequences of Breach;

(k) manage and co-ordinate the suspension of Parties' and Other Users' rights under this Code, as set out in Clause 21: Events of Breach and Consequences of Breach;

(l) manage and co-ordinate the withdrawal or expulsion of Parties from this Code, as set out in Clause 22: Ceasing to be a Party;

(m) by no later than 30 Working Days following the end of each calendar year prepare and publish a report on the implementation of this Code and the activities of the Panel during that calendar year, including so as to evaluate whether this Code continues to meet the Code Objectives;

(n) at the written request of the Commission at any time, undertake a review of such parts of this Code as the Commission may specify to evaluate whether this Code continues to meet the Code Objectives;

(o) at the written request of the Commission, collect and provide to the Commission (or publish in such manner as the Commission may direct) such information regarding the Smart Meter Data Access Arrangements as the Commission may reasonably request (and each Party shall provide to the Panel such information as the Panel reasonably requires in order to enable the Panel to comply with any such request of the Commission);

(p) hold a general meeting during the month of [Month] each year, which each Panel Member will (subject to unforeseen circumstances) attend, at which a representative of each Party shall be entitled to attend and speak, and at which the Panel will endeavour to answer any reasonable questions submitted to the Code Manager in advance of the meeting;

(q) establish (and, where appropriate, revise from time to time) joint working arrangements with responsible managers for the governance and operation of other Electricity Industry Arrangements, in order to facilitate the timely identification, co-ordination, making and implementation of changes to other Electricity Industry Arrangements consequent on a Modification Proposal (and vice versa); and

(r) establish joint working arrangements subject to a memorandum of understanding with the Data Protection Commissioner pursuant to which the Panel shall notify the Data Protection Commissioner of matters in which the Panel believes the Data Protection Commissioner may have an interest.

Panel Powers

8.6. Without prejudice to any other rights or powers granted to the Panel in this Code, the Panel shall, subject to and in accordance with the other provisions of this Code, have the power to:

(a) constitute Sub-Committees in accordance with Clause 9: Security Sub-Committee and other Sub-Committees;

(b) execute Accession Agreements in accordance with Clause 6: Becoming a Party;

(c) enter into Access Agreements with Other Users, in accordance with Schedule 2: Access Arrangements, with the signatory being the Panel Chair;

(d) be involved in approving decisions to use certain service providers or systems (such as for the Code Manager's secretariat functions); and

(e) do anything necessary for, or reasonably incidental to, the discharge of its duties under this Code.

Panel Appointments

8.7. The Panel shall initially comprise those willing individuals designated by the Commission at or around the date of this Code's designation.

8.8. Thereafter, the Panel shall consist of members (each a Panel Member, and the Panel Members referred to in Clause 8.7 (a) being the Elected Members), appointed as follows and in accordance with Schedule 7: Panel, such persons to include at all times:

(a) Two (2) members nominated by or elected in respect of Electricity Suppliers;

(b) one member appointed by the DSO;

(c) one member appointed by the TSO;

(d) one member appointed by the SMO;

(e) one member appointed by the DSP;

(f) a Panel Chair, who shall be a person appointed by the Commission; and

(g) any additional person appointed by the Panel Chair.

8.9. Each Panel Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Panel Member.

Vacation of Office by a Panel Member

8.10. The vacation of office by a Panel Member is set out in Schedule 7: Panel.

Duties of Panel Members

8.11. A person appointed as Panel Member, when acting in that capacity, shall:

(a) act independently, not as a delegate, and without undue regard to the interests, of any Related Person;

(b) not at any time disclose to any person any and all Confidential Information disclosed during the course of the Panel's business nor the affairs of the any Party or Other User, except,

(i) where required to do so to the Security Sub-Committee and/or the Code Compliance Officer;

(ii) required by Law, court order or by any governmental or regulatory authority;

(iii) to the extent the Confidential Information has become publicly available or generally known to the public at the time of the disclosure other than as a result of a breach of this Clause 8.11

(c) exercise reasonable skill and care to the standard reasonably expected of a director of a company under Part 5 of the Companies Act 2014; and

(d) act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

8.12. A person shall not be appointed as a Panel Member unless they shall have first confirmed in writing to the Code Manager for the benefit of all Parties that they:

(a) agree to act as a Panel Member in accordance with the Code and acknowledge the requirements of Clauses 8.11 and 8.13; and

(b) will be available as reasonably required throughout their term of office, both to attend Panel meetings and to undertake work outside those meetings as may reasonably be required.

Where that person is employed, provided to the Code Manager a letter from their employer agreeing that they may act as Panel Member, and that the requirement in Clause 8.10 shall prevail over their duties as an employee.

8.13. Each Panel Member shall, at the time of appointment and upon any change in such interests or circumstance, disclose in writing to the Panel the name of each Related Person who is a Party, Other User, a DSP Service Provider or is otherwise likely to be materially affected by these Code arrangements (other than in the capacity of a Final Customer).

8.14. The appointment of a person who would otherwise be a Panel Member shall lapse (and the relevant office shall become vacant) if that person does not comply with the requirements of Clause 8.11 within 20 Working Days after a request from the Code Manager to do so.

8.15. Without prejudice to the generality of Clause 8.13, where an Elected Member changes employer, the Panel Member shall (as soon as reasonably practicable after such change) notify the Code Manager of such change in writing. The Elected Member will then be removed as a Panel Member and the Code Manager shall then initiate an election in accordance with Schedule 7: Panel.

Protections for Panel Members and Others

8.16. The Code Manager shall indemnify, and keep indemnified:

(a) each Panel Member;

(b) each Alternate;

(c) each person who serves on a Sub-Committee or Working Group; and

(d) each Party, or an Affiliate of a Party, as the employer of any person referred to in Clause 8.16(a) to (c),

from and against any and all costs (including legal costs), charges, expenses, damages or other liabilities properly incurred or suffered by that person or employer in relation to the exercise of the person's powers, duties or responsibilities under this Code, including where such powers, duties or responsibilities are exercised negligently.

8.17. The indemnity set out in Clause 8.16 shall not apply to any costs, charges, expenses, damages or other liabilities that are:

(a) costs and expenses expressly stated to be incapable of recovery by the Panel under Clause 13: Costs, Annual Budgets and Cost Recovery; or

(b) suffered or incurred or occasioned by the wilful default, fraud or bad faith of the relevant person.

Panel Procedures/Proceedings of the Panel

8.18. The Panel shall determine its procedure as it sees fit, subject to the express requirements of this Code and those proceedings set out in Schedule 7: Panel.

9 Security Sub-Committee and Other Sub-Committees

9.1. The Panel may establish such sub-committees from time to time and consisting of such persons as it considers desirable (referred to as Sub-Committees), which shall be considered to act on behalf of the Panel.

9.2. The Security Sub-Committee is a Sub-Committee. The Panel shall, at a time it considers appropriate, establish the Security Sub-Committee. Until any such Sub-Committees have been established, the functions, duties and powers assigned to them under this Code and Schedule 10: Security Sub-Committee, shall be performed and exercised by the Panel.

9.3. The Panel may establish a Sub-Committee on a standing basis or for a fixed period or a finite purpose. The Panel may decide that a Sub-Committee is to be dissolved (save for those expressly required by this Code).

9.4. Each Sub-Committee expressly required by this Code, shall perform the functions and duties and have the powers expressly assigned to it by this Code.

9.5. Each Sub-Committee shall be subject to such written terms of reference and such procedures as the Panel may determine (as long as those terms of reference do not conflict with the other requirements of this Code).

Membership

9.6. Each Sub-Committee expressly provided for in this Code shall be composed of such persons as are determined in accordance with the provisions of this Code (if any) that prescribe such membership (and otherwise in accordance with Clause 9.7).

9.7. Subject to Clause 9.6:

(a) each Sub-Committee shall be composed of such persons of suitable experience and

qualifications as the Panel shall decide and as are willing to serve thereon, and which may include any Panel Member;

(b) before establishing each Sub-Committee, the Panel shall invite (by such means as it considers appropriate) applications from individuals who wish to serve on that Sub-Committee;

(c) once a Sub-Committee has been established, the Panel may admit such additional persons to, or remove any person from, that Sub-Committee as the Panel considers appropriate (including on the application of any Party or any member of the Sub-Committee).

9.8. Each person serving on a Sub-Committee shall, when acting in that capacity:

(a) act independently, not as a delegate, and without undue regard to the interests, of any Related Person; and

(b) act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

Member Confirmation

9.9. Unless the Panel otherwise directs, a person who is to serve on a Sub-Committee shall not do so unless they have first provided a written confirmation to the Code Manager (for the benefit of the Code Manager and each Party) that that person:

(a) agrees to serve on the Sub-Committee in accordance with this Code, including the requirements of Clause 9.8; and

(b) will be available as reasonably required throughout their term of office, both to attend Sub-Committee meetings and to undertake work outside those meetings as may reasonably be required.

Terms of Reference and Procedural Requirements

9.10. The Panel shall set out in writing the duties, powers, and functions of the Panel that it has delegated to each Sub-Committee. The Panel shall also specify in the same document the terms of reference and procedural rules that are to be followed by the Sub-Committee (which may be revised from time to time by the Panel); provided that, in the case of Sub-Committees expressly provided for in this Code, the Panel must specify terms of reference and procedural rules consistent with the requirements (if any) expressly set out in this Code.

9.11. Save to the extent otherwise specified by the Panel in accordance with Clause 9.10, each Sub-Committee shall conduct its business in accordance with the requirements applying to the Panel in accordance with Clause 8: Panel and Schedule 7: Panel.

9.12. No Sub-Committee may further delegate any of its duties, powers and functions unless expressly authorised to do so by the terms of reference and procedural rules specified in accordance with Clause 9.10.

Decisions of Sub-Committees

9.13. Resolutions of Sub-Committees shall only have binding effect as decisions of the Panel if the Panel has formally delegated the decision-making powers to the Sub-Committee.

9.14. The Panel shall be deemed to have delegated its decision-making powers to each Sub-Committee expressly provided for in this Code, insofar as such decision-making powers

relate to the functions of the Sub-Committee. The delegation of decision-making powers to any other Sub-Committee shall require the unanimous agreement of all Panel Members at the meeting at which the decision to delegate such powers is agreed.

9.15. For the avoidance of doubt, the delegation to a Sub-Committee of any duties, powers and functions of the Panel shall not relieve the Panel of its general responsibility to ensure that such duties, powers and functions are exercised in accordance with this Code.

10 Code Manager

10.1. The Commission shall (subject to Clause 10.7) from time to time appoint, and may from time to time remove, a person or persons to be known as the Code Manager.

10.2. In no event shall the Code Manager be a Party or an employee of a Party.

10.3. The Code Manager shall, in all its activities, always act in a manner designed to achieve the following objectives:

(a) that this Code is given full and prompt effect in accordance with its provisions, in a manner consistent with the Code Objectives, and without undue discrimination between Parties or Other Users or any classes of Party or Other User; and

(b) that the Code Manager conducts its affairs in an open and transparent manner.

10.4. It is acknowledged that, in conducting its activities in accordance with Clause 10.5, the Code Manager shall Process Personal Data as a Data Controller.

10.5. The Code Manager shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Commission and/or the Panel (or any Sub-Committee) may assign to the Code Manager from time to time. Without limitation, the Code Manager shall (subject to Clause 10.7):

(a) manage applications from potential New Parties to become a Party in accordance with Clause 6: Becoming a Party;

(b) convene and minute meetings of the Panel (and its Sub-Committees) in accordance with Clause 8: Panel and Clause 9 Security Sub-Committee and other Sub-Committees;

(c) circulate all relevant notices, papers and minutes of the Panel (and its Sub-Committees) in accordance with Clauses 8: Panel and Sub-Committees and Clause 9: Security Sub-Committee and other Sub-Committees; and

(d) manage the process for progressing Modifications Proposals and Change Proposals in accordance with Clause 15: Change Management;

(e) have the power to enter into contracts with to certain service providers or systems as necessary for the Code Manager's secretariat functions, subject to the approval of the Panel.

10.6. The Commission shall be responsible for ensuring that the Code Manager undertakes its tasks and functions in respect of this Code. In particular, the Commission shall (subject to Clause 10.7) ensure that the arrangements under which the Code Manager is appointed oblige the Code Manager to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

10.7. The Commission may, where consistent with the Code Objectives, decide not to outsource some or all the Code Manager functions to a service provider, and may instead decide that some or all of those functions shall instead be performed by the Commission. Where this

is the case, the relevant references in this Code to the Code Manager will be interpreted as references to the Commission.

10.8. Until such time as the Commission appoints a Code Manager in accordance with Clause 10.1 and/or decides that some or all of the Code Manager's functions shall instead be performed by the Commission in accordance with Clause 10.7, such functions may on an interim basis be performed by the Commission or a person nominated by the Commission.

11 Code Compliance Officer

11.1. The Commission shall (subject to Clause 11.9) from time to time appoint, and may from time to time remove, a person or persons to be known as the Code Compliance Officer.

11.2. For the purposes of Clause 11.1, the person or persons shall:

(a) be suitably qualified to act as the Code Compliance Officer, including demonstrable experience or accreditation of conducting security assessments in line with ISO/IEC 27001:2022;

(b) employed assessors will hold internationally recognised industry certifications such as Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM), Certified Information Privacy Professional (CIPP) schemes, or another membership, accreditation, approval or form of professional validation that is in the opinion of the Panel substantially equivalent in status and effect;

(c) engage the individuals referred to in Clause 11.2(b) for the purposes of carrying out assessment activities and other functions of the Code Compliance Officer under Clause 11.6;

(d) shall be suitably independent, including in accordance with Clause 11.3; and

(e) must be capable of meeting the Panel's estimate of the demand for its services under Clause 11.1 throughout the period in relation to which those services are being procured.

11.3. In no event shall the Code Compliance Officer be a Party or Other User, an Affiliate of a Party or Other User, an employee of a Party or Other User or an employee of an Affiliate of a Party or Other User.

11.4. It is acknowledged that, in conducting its activities in accordance with Clause 11.6, the Code Compliance Officer shall Process Personal Data as a Data Processor on behalf of the Panel. The Personal Data which the Code Compliance Officer shall Process as a Data Processor shall include Smart Meter Data as Processed in the course of its assessment activities or during incident investigation and management. The Code Compliance Officer shall enter into a data protection agreement (which shall include provisions for the storage, retention and disposal of any Data relating to the Code Compliance Officer duties) with the Panel Chair that shall establish its responsibilities as a Data Processor over such Data.

11.5. The Code Compliance Officer shall, in all its activities, always act in a manner designed to achieve the following objectives:

(a) that this Code is given full and prompt effect in accordance with its provisions, in a manner consistent with the Code Objectives, and without undue discrimination between Parties or Other Users or any classes of Party or Other Users; and

(b) that the Code Compliance Officer conducts its affairs in an open and transparent manner.

11.6. The Code Compliance Officer shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Commission and/or the Panel (or any Sub-Committee) may assign to the Code Compliance Officer from time to time. Without limitation, the Code Compliance Officer shall (subject to Clause 11.9):

(a) carry out Entry Assessments and manage the Entry Assessment process by which Applicants become Users in accordance with Clause 7: Compliance and Schedule 6: Assessments;

(b) maintain the Assurance Strategy in accordance with Schedule 6: Assessments;

(c) review the outcome of Annual Self-Assessments completed by the DSP, Parties and Other Users;

(d) carry out Ad-Hoc Assessments on the DSP, Parties and Other Users at such times and in such a manner as required by the Panel in accordance with Clause 7.10;

(e) carry out any other assessment, including of the DSP's and/or Code Manager's performance, as required by the Panel;

(f) produce Assessment Reports in relation to Users that have been the subject of an Entry Assessment or Ad-Hoc Assessment;

(g) review and consider Assessment Responses submitted by Users following an Entry Assessment or Ad-Hoc Assessment, in accordance with Schedule 6: Assessments;

(h) propose, for the consideration of the Security Sub-Committee, a Remedial Plan in relation to an Assessment Report for the Party or Other User to achieve compliance with the Code;

(i) provide the Panel and Security Sub-Committee with such advice and support as may be requested by it from time to time, including advice in relation to the suitability of any Remedial Plan, and advice in relation to an Event of Breach in accordance with Clause 21: Events of Breach and Consequences of Breach;

(j) provide the Panel and Security Sub-Committee and, at its request, the DSP, with such advice and support as necessary for the investigation and management of a Security Incident;

(k) provide the Panel, Security Sub-Committee, and any other Sub-Committees with such advice and support as to the requirement for a Data Protection Impact Assessment to be conducted on Processing activities, including those referred to in Clause 3.14 of Schedule 2: Access Arrangements and conduct, at the request of the Panel, such a Data Protection Impact Assessment;

(l) following a notification from the Code Manager under Schedule 8: Party Exit, provide the Code Manager with such advice and support in accordance with Schedule 5: Data Privacy in relation to investigating and identifying that:

(i) The Party has demonstrated that Data, including Personal Data, received from the Smart Meter Data System has been deleted in accordance with Schedule 5: Data Privacy, unless otherwise needed in accordance with that Schedule; and

(ii) No Metering Points are registered and no gaining Metering Points to be gained due to Change of Supplier process prior to a Party's exit from the Code;

(m) at the request of the Security Sub-Committee, attend any Security Sub-Committee meetings, and at the request of the Panel, attend any Panel meetings;

(n) manage the Code Audit in accordance with Clause 7: Compliance;

(o) manage the compliance and assurance processes in accordance with Clause 7: Compliance;

(p) support the Code Manager with impact assessments in relation to Modification Proposals, as required in accordance with Schedule 9: Change Management; and

(q) at the request of the Panel, undertake any other activities designated and/or delegated by the Panel.

11.7. It is acknowledged that, during the operation of the Code, in carrying out its functions in accordance with the provisions of this Clause, the Code Compliance Officer shall act in the capacity of a 'Data Processor' on behalf of the Panel. The Code Compliance Officer shall enter into a data processing agreement with the Panel, signed by the Panel Chair, that shall outline its data Processing responsibilities where it acts in the capacity of a 'Data Processor' on behalf of the Panel.

11.8. The Commission shall be responsible for ensuring that the Code Compliance Officer undertakes its tasks and functions in respect of this Code. In particular, the Commission shall (subject to Clause 11.9) ensure that the arrangements under which the Code Compliance Officer is appointed oblige the Code Compliance Officer to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

11.9. The Commission may, where consistent with the Code Objectives, decide not to outsource some or all of the Code Compliance Officer functions to a service provider, and may instead decide that some or all of those functions shall instead be performed by the Commission. Where this is the case, the relevant references in this Code to the Code Compliance Officer will be interpreted as references to the Commission.

11.10. Until such time as the Commission appoints a Code Compliance Officer in accordance with Clause 11.1 and/or decides that some or all of the Code Compliance Officer's functions shall instead be performed by the Commission or another person, such functions may on an interim basis be performed by the Commission or a person nominated by the Commission.

12 Data Systems Provider

12.1. In accordance with 5.3(a), the DSP is a Party and cannot be removed as a Party.

12.2. In no event shall the DSP be a user.

12.3. The DSP shall, in all its activities, always act in a manner designed to achieve the following objectives:

(a) that this Code is given full and prompt effect in accordance with its provisions, in a manner consistent with the Code Objectives, and without undue discrimination between Parties or Other Users or any classes of Party or Other Users; and

(b) that the DSP conducts its affairs in an open and transparent manner.

12.4. It is acknowledged that, in conducting its activities in accordance with Clause 12.5, the DSP shall Process Personal Data as a Data Controller.

12.5. The DSP shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Commission and/or the Panel (or any Sub-Committee) may assign to the DSP from time to time. Without limitation, the DSP shall:

(a) manage the provision of access to the Smart Meter Data System;

(b) ensure that any of its any of its policies, procedures, Systems or processes, including those applicable to Data and the Smart Meter Data System, comply with the provisions of Schedule 4: Data Security and Schedule 5: Data Privacy in relation to the DSP;

(c) shall do all such things as may be reasonably requested by the Security Sub-Committee or by the Code Compliance Officer for the purposes of facilitating an assessment of the DSP's obligations under this Code;

(d) ensure the functionalities of the Smart Meter Data System, including in relation to:

(i) ensuring the availability of Data on the Smart Meter Data System as received from Smart Meters and other Systems;

(ii) ensuring the ability to allow the access to Data, and to export Data from, of the Smart Meter Data System, to all Parties and Other Users and Final Customers, as reasonably appropriate;

(iii) ensuring the provision and assignment of identifiers to Parties and Other Users (and User Personnel) wishing to access Data on the Smart Meter Data System;

(e) inform all Parties and Other Users with a minimum of 10 Working Days of any planned maintenance activities on the Smart Meter Data System;

(f) inform all Parties and Other Users within a reasonable period of time of any unplanned maintenance activities on the Smart Meter Data System;

(g) provide each User with the appropriate functionalities and access to Data on the Smart Meter Data System as necessary for their User Category;

(h) provide each Final Customer with the appropriate functionalities and access to Data on the Smart Meter Data System;

(i) maintain a Data Dictionary to provide a list of, and relevant information on, the Data Items available on the Smart Meter Data System; and

(j) support the Code Manager with impact assessments in relation to Modification Proposals, as required.

12.6. The DSP shall, following a notification from the Code Manager in relation to the creation of a new User Category or a User's request to access any new Data Items under Schedule 2: Access Arrangements, ensure that the relevant User(s) identified by the Code Manager in the notification is provided with access to the appropriate Data Items on the Smart Meter Data System, within 30 days of the receipt of the notification.

12.7. The DSP shall, following a notification in relation a User's request to cease access to certain Data Items from the Code Manager under Schedule 2: Access Arrangements, ensure that the relevant Parties identified by the Code Manager in the notification are removed from access to the relevant Data Items on the Smart Meter Data System, within 30 days of the receipt of the notification.

12.8. The DSP shall, following a notification in relation to a Party's withdrawal or expulsion from the Code from the Code Manager under Schedule 8: Party Exit, ensure that the relevant Parties identified by the Code Manager in the notification are removed from access to the Smart Meter Data System, within 30 days of the receipt of the notification.

12.9. The Commission shall be responsible for ensuring that the DSP undertakes its tasks and functions in respect of this Code. In particular, the Commission shall ensure that the arrangements under which the DSP is appointed in accordance with the SI 37 of 2022 oblige the DSP to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

13 Costs, Annual Budget and Cost Recovery [to be determined]

13.1. General

13.2. Strategy

13.3. Code Costs and Expenses

13.4. Reimbursing Panel Members

13.5. Cost Recovery

13.6. Draft Budgets and Work Plans

13.7. Preparation and Approval of Budgets

13.8. Appeal of Budget

13.9. Amendments to Budgets

13.10. Publication of Annual Budget

13.11. Payment of Costs Incurred

13.12. Recovery of Costs from Parties/Other Users

13.13. Bad Debt

13.14. Annual Report

13.15. Audit

14 Usage Charges [to be determined]

14.1. [To be drafted]

15 Change Management

15.1. Until the Go Live Date (or such earlier date as the Commission may designate, including on the application of the Panel), changes to this Code shall not be subject to Schedule 9: Change Management, and shall instead be subject to the Commission's approval.

15.2. Notwithstanding the Go Live Date, and until three months after Go Live Date (or such earlier or later date as the Commission may designate), the Commission may direct the Code Manager that any proposed changes to the Code which relate to the National Smart Metering Programme shall not be subject to the Schedule 9: Change Management, and shall instead be subject to the Commission's approval as described in Clause 15.1. Where the Commission does not so direct, the proposed changes shall remain subject to Schedule 9: Change Management .

15.3. While (and to the extent that) the National Smart Metering Programme's change process applies under Clauses 15.1 or 15.2, the Panel and its Sub-Committees and the Code Manager shall each participate in that change process, and assist and support that change process. If requested by the Commission, such participation shall include undertaking impact assessments and/or providing recommendations on proposed National Smart Metering Programme changes.

15.4. There may be instances where an inconsistency arises between the requirements of this Code and the requirements of Law, a Licence or other Electricity Industry Arrangement. Where a Party identifies such an inconsistency, the Party shall notify the Code Manager. Following such a notification by a Party (and an Other User as the case may be) to the Code Manager, the Party or Other User shall not be considered to be in breach of this Code in accordance with Clause 21: Event of Breach and Consequences of Breach where such breach arises as a result of the Party or Other User complying with its obligations under Law, a Licence and/or other Electricity Industry Arrangement.

16 Limitations of Liability [to be determined]

17 Data Security and Data Privacy Obligations

17.1. Each Party User shall comply with the Schedule 4: Data Security.

17.2. Each Party User shall comply with the Schedule 5: Data Privacy.

18 Force Majeure

18.1. If any Party (referred to as the “Affected Party”), other than the Commission, shall be unable to carry out any of its obligations under this Code due to a circumstance of Force Majeure, then this Code shall remain in effect but:

(a) the Affected Party's obligations; and

(b) any other obligations of the other Parties which a Party is unable to carry out directly as a result of the suspension of the Affected Party's obligations,

shall be suspended without liability for the period during which the circumstance of Force Majeure prevails (subject to Clause 18.2).

18.2. Relief under Clause 18.1 is subject to the following:

(a) the Affected Party shall give the Code Manager prompt notice describing the circumstance of Force Majeure including the nature of the occurrence and its expected duration and where reasonably practicable, shall continue to furnish regular reports with respect thereto during the period of Force Majeure;

(b) the suspension of performance shall be of no greater scope and of no longer duration than is required by the circumstance of Force Majeure;

(c) the obligations of any Party that arose before the circumstance of Force Majeure causing the suspension of performance shall not be excused as a result of the Force Majeure;

(d) the Affected Party shall take all reasonable steps to mitigate the impact of the circumstance of Force Majeure and to remedy its inability to perform as quickly as possible; and

(e) immediately after the end of the circumstance of Force Majeure, the Affected Party shall notify the other Parties in writing of the same and resume performance of its obligations under this Code.

18.3. On receiving notice from an Affected Party under 18.2(a), the Code Manager shall inform the Commission and Panel.

18.4. Following 18.3, the Panel shall meet in accordance with Clause 8: Panel.

19 Disputes

19.1. Save where expressly stated in this Code to the contrary, and subject to any contrary provision of Legislation or any Licence, any Dispute or difference of whatever nature and howsoever arising under, out of, or in connection with this Code (each a "Dispute") shall be resolved according to the provisions of this Clause 19.

19.2. Any Party shall refer a Dispute by notice in writing to all other Parties to the Agreement who are Party to the Dispute (the Party referring the Dispute and the other Parties to the Dispute each being a "Disputing Party"). The Disputing Parties shall endeavour to resolve the Dispute between them.

Arbitration

19.3. If the Disputing Parties are not able to resolve the Dispute within 10 Working Days of the reference of a Dispute to them, then any Disputing Party may, within 20 Working Days of such reference, refer the Dispute to arbitration before an arbitral tribunal composed of a single arbitrator pursuant to the rules of the Dublin International Arbitration Centre (subject to Clause 19.5).

19.4. Whatever the nationality, residence or domicile of any Disputing Party and wherever the Dispute or any part thereof arose the laws of the Republic of Ireland shall be the proper law of any reference to arbitration hereunder and in particular (but not so as to derogate from the generality of the foregoing) the seat of any such arbitration shall be Dublin and the provisions of the Arbitration Act 2010 shall apply to any such arbitration wherever the same or any part of it shall be conducted.

Claims by Third Parties

19.5. Subject to Clause 19.6, if any person who is not a Party to this Code brings any legal proceedings in any court against any Party and that Party considers such legal proceedings to raise or involve issues that are or would be the subject matter of a Dispute or potential Dispute that would (but for this Clause) be subject to arbitration, then (instead of arbitration) the court in which the legal proceedings have been commenced shall hear and determine the legal proceedings and the Dispute between such person and the Parties.

19.6. If any person who is not a Party to this Code brings any legal proceedings in any court against any Party and that Party considers such legal proceedings to raise or involve issues that are the subject matter of a Dispute that is already subject to an ongoing arbitration, then Clause 19.5 shall only apply where the arbitrator in that arbitration determines that such legal proceedings raise or involve issues that are the subject matter of the Dispute.

Determination by the Panel

19.7. Any Dispute of a nature that is expressly stated in this Code to be subject to determination by the Panel or a Sub-Committee shall be subject to determination by the Panel or a Sub-Committee. The Panel shall ensure that any such Dispute is determined within a reasonable period of time after its referral. Unless such determination is expressly stated in this Code to be subject to a further appeal, then the decision of the Panel or the Sub-Committee (as applicable) shall be final and binding for the purposes of this Code.

Appeals to the Panel

19.8. Where this Code expressly states that a decision is capable of appeal to the Panel (and not otherwise), then such decision may be appealed to the Panel. Any such appeal will only be validly made if notified to the Panel within 10 Working Days after the appellant received notice of the decision or such longer period as may be prescribed by this Code (unless the Panel waives such requirement). The Panel's determination in respect of such

appeal shall be final and binding for the purposes of this Code. The Panel may give notice that it dismisses the appeal where it considers that the appeal is trivial or vexatious or has no reasonable prospect of success.

Appeals to the Commission

19.9. Where this Code expressly states that a decision is capable of appeal to the Commission (and not otherwise), then such decision may be appealed to the Commission. Any such appeal will only be validly made if notified to the Commission within 10 Working Days after the appellant received notice of the decision or such longer period as may be prescribed by this Code (unless the Commission waives such requirement). The Commission's determination in respect of such appeal shall be final and binding for the purposes of this Code. The Commission may give notice that it dismisses the appeal where it considers that the appeal is trivial or vexatious or has no reasonable prospect of success.

20 Derogations

Application for Derogation

20.1. A Party may, at any time, apply to the Panel for a derogation under this Clause 20 by notice in writing to the Code Manager.

20.2. Where the Code Manager receives such an application, it shall ensure that the matter is considered by the Panel by the next meeting after receipt of such application, and shall give notice to all the Parties, the Panel and to the Commission, at least 10 Working Days before the meeting in question:

(a) setting out the identity of the Party by whom the application has been made and the terms of the derogation sought;

(b) specifying the date on which the Panel is due to consider the matter;

(c) inviting representations or objections with respect to the derogation before that time; and;

(d) where appropriate, bringing to the Panel’s attention to any relevant circumstances, previous derogations and views that may have been expressed by the Commission.

20.3. The Panel may (subject to Clause 20.5) resolve, on the application of any Party, to grant a derogation to any Party or Parties in relation to any obligation(s) contained in this Code. In resolving to grant such derogation, the Panel may impose such conditions as it sees fit, and shall specify the term, scope and application of such derogation.

20.4. The Panel may, from time to time and as it sees fit (subject to Clause 20.5), resolve to retract any derogation, or to amend or add to the conditions applicable to any derogation.

20.5. A derogation granted to any Party by the Panel, or any retraction, amendment or addition under Clause 20.4, shall, in each case, only be effective if made in conformity with any representations received from the Commission pursuant to Clause 20.3, and if not vetoed by the Commission within 10 Working Days after notification of the Panel's decision and the rationale for it.

Effect of Derogation

20.6. Where a Party is granted a derogation by the Panel in accordance with this Clause 20, that Party shall, for the period provided for in the derogation:

(a) be excused from complying with the obligations specified in the terms of that derogation;

(b) be deemed not to be in breach of this Code for failing to comply with the relevant obligations; and

(c) be required to comply with any modified obligations which are specified as a condition of the derogation.

20.7. A Party may, by notice in writing to the Panel at any time, reject any derogation then applying to the Party, in which case the derogation shall cease to apply from the date specified in the Party's notice.

20.8. The coming into effect of a derogation under this Clause 20 shall (unless otherwise stated in the derogation) be without prejudice to liabilities that arose prior to the derogation coming into effect. The ending of a derogation under this Clause 20 shall be without prejudice to any liabilities in respect of compliance with conditions of the derogation that arose prior to the derogation ending.

Code Manager's Role in respect of Derogations

20.9. In relation to each derogation request, the Code Manager shall consider whether there is an issue of general application, which would better be addressed by a Modification Proposal, and shall report to the Panel on the same. If, having considered the responses of the Panel, the Code Manager is of the view that a Modification Proposal is appropriate, then:

(a) the Code Manager shall develop a draft Modification Proposal in accordance with Schedule 9: Change Management, for discussion at a future meeting of the Panel; and

(b) the Panel may instruct the Code Manager to submit the Modification Proposal into the Change Management process in accordance with Schedule 9: Change Management, with or without any revision that the Data Protection Commission (DPC) may require.

21 Events of Breach and Consequences of Breach

21.1. An “Event of Breach” shall occur in respect of a Party (the “Breaching Party”), other than the Commission, where:

(a) the Breaching Party is:

(i) in breach of any of the material terms or conditions of this Code; and/or

(ii) in persistent breach of any of the terms or conditions of this Code and,

if the breach is or was capable of remedy, it fails to remedy the breach within 20 Working Days of receipt of a notice to the Panel or, where relevant, the Security Sub-Committee giving details of the breach, requiring the Breaching Party to remedy the breach and stating that a failure to remedy the breach may give rise to consequences set out in Clause 21.3;

(b) the Breaching Party is determined to have committed an Event of Breach under Clause 7: Compliance; and/or

(c) the Breaching Party has failed in a material respect to comply with an enforcement notice served by the Data Protection Commissioner pursuant to Data Protection Legislation, whether such failure has been notified to the Security Sub-Committee via the Panel by the Data Protection Commissioner; and/or;

(d) the Breaching Party has not paid any amount other than in respect of the Usage Charges, which the Breaching Party is due to have paid under this Code, and does not remedy such failure within 5 Working Days after a notice requiring it to do so; and/or

(e) the Breaching Party has made a material misrepresentation in its application for entry; and/or

(f) the Breaching Party suffers an Insolvency Type Event; and/or

(g) if the Breaching Party holds the DSO Licence, the Breaching Party has its DSO Licence revoked or the Commission has advised the Code Manager that it has initiated the revocation of the DSO; and/or

(h) if the Breaching Party holds the TSO Licence, the Breaching Party has its TSO Licence revoked or the Commission has advised the Code Manager that it has initiated the revocation of the TSO; and/or

(i) if the Breaching Party holds the SMO Licence, the Breaching Party has its SMO Licence revoked or the Commission has advised the Code Manager that it has initiated the revocation of the SMO; and/or

(j) if the Breaching Party holds an Electricity Supply Licence, the Breaching Party has its Electricity Supply Licence revoked or the Commission has advised the Code Manager that it has initiated the revocation of the Electricity Supply Licence.

21.2. Where the Panel or, where relevant, Security Sub-Committee has reason to believe that an Event of Breach may have occurred in respect of a Party, then the Panel, or on its behalf, the Security Sub-Committee, may investigate the circumstances relating to such potential Event of Breach. Each Party shall provide all reasonable data and cooperation as the Panel may reasonably request in respect of any such investigation.

21.3. Where an Event of Breach occurs in respect of a Breaching Party and while that Event of Breach is continuing, the Panel (or the Security Sub-Committee on its behalf) may take one or more of the following steps (in each case to the extent and at such time as the Panel sees fit, having regard to all the circumstances of the Event of Breach and any representations made by any Competent Authority or any Party):

(a) notify the Commission and the DPC that such Event of Breach has occurred in respect of the Breaching Party;

(b) notify the Breaching Party that such Event of Breach has occurred in respect of it;

(c) notify the DSP and each other Party that such Event of Breach has affected;

(d) request the Code Compliance Officer to conduct an Ad-Hoc Assessment of the Breaching Party;

(e) require the Breaching Party to give effect to a reasonable Remedial Plan designed to remedy and/or mitigate the effects of the Event of Breach within a reasonable timescale (a breach of which plan shall in itself constitute an Event of Breach);

(f) suspend the right of the Breaching Party to exercise its rights in respect of access to Smart Meter Data, except to such Data it requires to fulfil its Licence obligations;

(g) suspend the right of the Breaching Party to exercise its rights in respect of Change Proposals pursuant to Clause 15: Change Management; and/or

(h) recommend to the Commission that the Breaching Party be expelled from this Code subject to and in accordance with Clause 22: Ceasing to be a Party.

21.4. The suspension of any or all of the Breaching Party's rights referred to in Clause 21.3 shall be without prejudice to the Breaching Party's obligations and liabilities under and in relation to this Code (whether accruing prior to, during, or after such suspension).

21.5. Where the Panel has, pursuant to Clause 21.3, suspended a Party's rights, then the Commission may at any time thereafter end such suspension.

21.6. Where the Security Sub-Committee has, pursuant to Clause 21.3, suspended a Party's rights, then the Panel may at any time thereafter end such suspension.

21.7. Where the Panel or, where relevant, Security Sub-Committee resolves to suspend the rights of a Party pursuant to Clause 21.3, then that Party may at any subsequent time make an appeal to:

(a) the Panel, where such suspension is determined by the Security Sub-Committee, to have such suspension lifted (in accordance with Clause 19.8); or

(b) the Commission to have such suspension lifted (in accordance with Clause 19.9).

21.8. The Parties and the Panel shall give effect to any decisions of:

(a) the Panel pursuant to such application under Clause 19.8; and

(b) the Commission pursuant to such application under Clause 19.9,

which shall be final and binding for the purposes of this Code.

Other User Breach

21.9. An Other User may breach its Access Agreement by a breach of any of the material terms or conditions of that Access Agreement.

21.10. Where the Panel has reason to believe that an Other User may have breached its Access Agreement, then the Panel, or the Security Sub-Committee on its behalf, may investigate the circumstances relating to such potential breach. The Other User shall provide all reasonable data and cooperation as the Panel may reasonably request in respect of any such investigation.

21.11. Where an Event of Breach occurs in respect of an Other User and while that Event of Breach is continuing, the Panel may take one or more of the following steps (in each case to the extent and at such time as the Panel sees fit, having regard to all the circumstances of the Event of Breach and any representations made by any Competent Authority or any Party):

(a) notify the Commission and the DPC that such a breach has occurred in respect of the Other User;

(b) notify the Other User that such a breach has occurred in respect of it;

(c) notify the DSP and each or any Party that such a breach has affected;

(d) request the Code Compliance Officer to conduct an Ad-Hoc Assessment of the Other User;

(e) require the Other User to give effect to a reasonable Remedial Plan designed to remedy and/or mitigate the effects of the breach within a reasonable timescale (a breach of the plan shall in itself constitute a breach);

(f) suspend the right of the breach to exercise its rights in respect of access to Smart Meter Data;

(g) recommend termination of the Other User's Access Agreement.

21.12. The suspension of any or all of the Other User's rights referred to in Clause 21.11 shall be without prejudice to the Other User's obligations and liabilities under and in relation to its Access Agreement (whether accruing prior to, during, or after such suspension).

21.13. Where the Panel, or the Security Sub-Committee on its behalf, has suspended an Other User's rights, then the Commission may at any time thereafter end such suspension.

21.14. Where the Panel, or the Security Sub-Committee on its behalf, resolves to suspend the rights of an Other User pursuant to Clause 21.11(f), then that Other User may at any subsequent time make an appeal to the Panel, where such suspension is determined by the Security Sub-Committee, or to the Commission, the where such suspension is determined by the Panel, to have such suspension lifted. The Panel shall give effect to any decision of the Commission pursuant to such Application, which shall be final and binding for the purposes of this Code.

22 Ceasing to Be A Party

22.1. A Party:

(a) cannot be expelled from this Code by the Panel unless the Commission has approved such expulsion; and

(b) cannot voluntarily cease to be a Party unless the Commission has approved such withdrawal.

22.2. The processes applying to Parties which are expelled from this Code or which wish to voluntarily withdraw from this Code are set out in Schedule 8: Party Exit.

22.3. Where the Panel resolves to expel a Party from this Code, then that Party may at any subsequent time apply to the Commission to be reinstated as a Party. The Parties and the Panel shall give effect to any decision of the Commission pursuant to such application, which shall be final and binding for the purposes of this Code.

22.4. Where an Parties is expelled or withdraws from this Code in accordance with the Schedule 8: Party Exit, then with effect from the time on the date at which such expulsion or withdrawal is effective (and subject to Clause 22.3):

(a) that Party's accession to this Code shall be terminated, and it shall cease to be a Party; and

(b) subject to Clause 22.5, that Party shall cease to have any rights or obligations under this Code.

22.5. The termination of a Party's accession to this Code shall be without prejudice to:

(a) those rights and obligations under this Code that may have accrued prior to such termination; or

(b) those provisions of this Code that are expressly or by implication intended to survive such termination.

23 Ceasing to Be an Other User

23.1. An Other User will cease to have its Other User role under the Code where its Access Agreement has been terminated in accordance with Clause 21.11 above.

23.2. Where its Access Agreement is terminated, the Other User shall still be required to comply with its obligations as set out in Schedule 8: Party Exit.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 1: Interpretations

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Schedule 1: Interpretations

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD-Mon-YY		n.n

1 General Interpretation

1.1. In this Code, the following interpretations shall apply unless the context requires otherwise:

(a) the Table of Contents, and any document name, with the exception of names which specify that what follows is a component of the Code, index and headings in this Code, are for ease of reference only and do not form part of the contents of this Code and do not and shall not affect its interpretation;

(b) words in the singular shall include the plural and vice versa and the masculine gender shall include the feminine and neuter;

(c) the word “including” and its variations are to be construed without limitation;

(d) any reference to any legislation, primary or secondary, in this Code includes any statutory interpretation, amendment, modification, re-enactment or consolidation of any such legislation and any regulations or orders made thereunder and any general reference to any legislation includes any regulations or orders made thereunder;

(e) any references to Clauses, Appendices and Schedules are references to Clauses, Appendices and Schedules of this Code as amended or modified from time to time in accordance with the provisions of this Code;

(f) any reference to another agreement or document, or any deed or other instrument is to be construed as a reference to that other agreement, or document, deed or other instrument as lawfully amended, modified, supplemented, substituted, assigned or novated from time to time;

(g) any reference to a day is to be construed as a reference to a calendar day except where provided otherwise, and any reference to a year is to be construed as a reference to a period of 12 months;

(h) any reference to a time is to be construed as a reference to the time prevailing in Dublin;

(i) where any obligation is imposed on any Party pursuant to this Code and is expressed to require performance within a specified time limit that obligation shall, where appropriate, continue to be binding and enforceable after that time limit if the Party fails to perform that obligation within that time limit (but without prejudice to all rights and remedies available against that person by reason of that person’s failure to perform that obligation within the time limit);

(j) capitalised words and phrases, acronyms, abbreviations and subscripts have the meaning given to them in the Definitions set out in Clause 2 except where otherwise specified;

(k) where a specified number of days is expressed to elapse or expire from or after the giving of a notice or the issue or making available of a document before an action may be taken or by which an action is required to be taken then, unless explicitly stated otherwise, the day on which the notice is given or issued or the document is made available shall not be counted in the reckoning of the period;

(l) where this Code requires data to be published by the Code Manager it shall be made publicly available (which, for the avoidance of doubt means available to all members of the public and not only to Parties) in a format that readily lends itself to processing by standard computer and analysis tools, through an easily accessible public interface and the terms "publish", "publication" and "published" shall be construed accordingly;

(m) where this Code requires the Code Manager to publish information and no timeline is specified for such publication, it shall be required to publish such information as soon as reasonably practicable.

(n) where no timeframe for performance is specified in respect of any obligation to be performed by a Party, then such obligation shall be performed within a reasonable time.

2 Definitions

Term	Acronym	Definition
Access Agreement		Means an Agreement by which an organisation that is not a Party can access the Smart Meter Data System.
Accession Agreement		Means an agreement by which a Party agrees to be bound by this Code, as set out in Schedule 3: Accession.
Access Log		Means a log of Third Parties' and users' access to Data, including Consumption Data, on the Smart Meter Data System, which includes: a) a timestamp of the time of access; b) the Data Items accessed; c) an identification of the Third Party or user accessing the Data; and d) the identification of the permission or other Legal Basis used by the Third Party to access the Data.
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or

Term	Acronym	Definition
		c) where a new User Category or Data Item is issued.
Affected Party		Means a Party which is unable to carry out its obligations under this Code due to circumstance of Force Majeure.
Affiliate		Means, in relation to a person, any group of undertaking of that person from time to time (and the expression "group undertaking".
Alternate		Means another natural person who may be appointed by a Panel Member or the Panel Chair to act as their alternate.
Alternative Modification Proposal		Has the meaning given to that expression in Clause 18.1 of Schedule 9: Change Management.
Annual Self-Assessment		Means a self-assessment questionnaire issued to all users on an annual basis to identify the extent to which, since the last occasion on which a Self-Assessment was carried out in respect of that Other User or Party, there has been any Material Change in the arrangements that the Other User has in place to comply with its obligations under the Code or in the quantity of Consumption Data being accessed by the Other User or Party.
Anomalous Event		Means, in relation to any System, an activity or event that is not expected to occur in the course of the ordinary operation of that system.
Anonymous Data		Means Data which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
Applicant		Means any person who applies to be admitted as a Party, subject to and in accordance with the Code.
Assessment Report		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.

Term	Acronym	Definition
Assessment Response		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.
Assurance Status		Has the meaning given to that expression in Clause 3.9 of Schedule 6: Assessments.
Assurance Strategy		Has the meaning given to that expression in Clause 7.8 of the Main Body.
Back-Up, Backed-Up		Means, in relation to Data which is held on any System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data.
Basic Access		Means, in relation to an application for access under Schedule 2: Access Arrangements, a request by a user for access that involves access to existing Data Items assigned to an existing User Category.
Breaching Party		Has the meaning given to that expression in Clause 21.1 of the Main Body:
Central Statistics Office	CSO	Means the legal entity responsible for providing an accurate picture of the Republic of Ireland's economic and social performance.
Certified Information Systems Security Professional	CISSP	Means the scheme of that name which is administered by the International Information System Security Certification Consortium (SC) or any successor to that scheme.
Certified Information Security Manager	CISM	Means the scheme of that name which is administered by the Information Systems Audit and Control Association (ISACA) or any successor to that scheme.
Certified Information Privacy Professional	CIPP	Means the scheme of that name which is administered by the International Association of Privacy Professionals (IAPP) or any successor to that scheme.

Term	Acronym	Definition
Change Management		Means the process by which a Modification to the Code is executed, in accordance with Schedule 9: Change Management.
Change of Legal Entity	CoLE	Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Change of Supplier	CoS	Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Change Proposal	CP	Means a proposal to change a subsidiary document to the Code and Schedules, in accordance with Schedule 9: Change Management.
Change Proposal Report		Means a written report on a Change Proposal.
Change Register		Means the register established and maintained by the Code Manager which contains all current and past Modification Proposals, as further described in Clause 5 of Schedule 9: Change Management.
Code Audit		Has the meaning given to that expression in Clause 7.7 of the Main Body.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Baseline Statement		Means the document of that name setting out a list of Schedules and documents that make up the Code and the Responsible Sub-Committee for approving changes to each document.
Code Compliance		Means the technical and organisational measures for ensuring compliance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility

Term	Acronym	Definition
		for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code. Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.
Code Objectives		Has the meaning given to that expression in Clause 2 of the Main Body.
Code Website		Means the dedicated website established by the Code Manager for the purposes of this Code.
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Commission Modification Proposal		Means a Commission-Approved Modification Proposal as set out in 9.3 of Schedule 9: Change Management.
Commission-Approved Modifications		Has the meaning as set out in 9.3 of Schedule 9: Change Management.
Competent Authority		Means the Authority, and any local, regional, national or supra-national agency, authority, department, inspectorate, minister, ministry, official or public or statutory person having (in each case) jurisdiction over the relevant Party, this Code or its subject matter.
Competition and Consumer Protection Commission	CCPC	Means the Competition and Consumer Protection Commission within the Republic of Ireland.
Complex Access		Means, in relation to an application for access under Schedule 2: Access Arrangements, a request by a user for access that involves: a) Access to a new Data Item, and/or; b) Access to a Data Item not assigned to that User Category,

Term	Acronym	Definition
		and/or; c) Access to Data Items by a user within a new User Category
Compromised		Means, in relation to the Smart Meter Data System, that the intended purpose or effective operation of the Smart Meter Data System is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity or availability of the Smart Meter Data System or of any Smart Meter Data that are stored on or communicated by means of it; or In relation to Smart Meter Data, that the confidentiality, integrity or availability of the Smart Meter Data is adversely affected by the occurrence of any event; and In relation to any process or to the functionality of any hardware, firmware or software, that the intended purpose or effective operation of that process or functionality is compromised by the occurrence of any event which has an adverse effect on its confidentiality, integrity or availability.
Confidential Information		means any and all confidential information and data (in whatever form communicated, obtained or maintained, whether orally, in writing, electronically, hard copy, computer storage, or otherwise) disclosed or made available (directly or indirectly) by a Disclosing Party to a Receiving Party for the purposes permitted under the terms of the Code, including but not limited to financial information, commercial and strategic data, details of employees and commercial information relating to operations, pricing, contracts, tenders processes, initiatives, plans, product information, technical or commercial know-how, specifications, inventions,

Term	Acronym	Definition
		designs, trade secrets, software, market opportunities and such expression shall include any reproduction or summary of a Disclosing Party's confidential information which a Receiving Party may make and any documents otherwise generated or prepared based on such information;
Consent		Means, in respect of the Processing of Smart Meter Data on the Smart Meter Data System, that the Final Customer has provided a freely given, specific, explicit, informed and unambiguous indication of their wishes by which they, by a statement or clear affirmative action, signify agreement to the Processing of Smart Meter Data, and that such Consent has not been withdrawn.
Consumption Data		Means, in respect of a premises, the quantity of electricity or gas measured by the Smart Meter as having been supplied to the relevant premises.
Cross Industry Change Arrangements		Means those arrangements established in accordance with Clause 4 of Schedule 9: Change Management.
DAR Change		Has the meaning of 3.4 of Schedule 9: Change Management.
DAR Release		Means a package of one or more approved DAR Change Proposals which is implemented in accordance with 27.1 of Schedule 9: Change Management.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Data Item		Means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for

Term	Acronym	Definition
		which are defined and controlled in the Data Access Register.
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data Controller		Has the meaning as defined in Data Protection Legislation.
Data Dictionary		Means a document maintained by the DSP that shall establish the Data Items, Identifiers and Description of the Data Items available on the Smart Meter Data System.
Data Glossary		Means a document maintained as per Appendix 1 of this Code that shall establish an explanation of the types of Data, including Personal Data, available on the Smart Meter Data System. The Data Glossary includes the information contained within the Data Dictionary.
Data Processor		Has the meaning as defined in Data Protection Legislation.
Data Protection Commission	DPC	Means the commissioner as defined in the Data Protection Legislation.
Data Protection Impact Assessment	DPIA	Has the meaning as defined in Data Protection Legislation.
Data Protection Legislation		Means the GDPR and any other implementing legislation with the Republic of Ireland, including the Data Protection Act 2018, and, in each case, all regulations, statutes and instruments made thereunder as may be amended from time to time.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, in accordance with Clause 12 of the Main Body.

Term	Acronym	Definition
Data Subject		Has the meaning as defined in Data Protection Legislation.
Data Subject Rights		Means the exercise of the rights of a natural person to their rights under Articles 15 to 22 of the General Data Protection Regulation, or otherwise as interpreted in Data Protection Legislation (where this takes precedence).
Department		Means the Department of the Environment, Climate and Communications within the Republic of Ireland.
Deputy Chair		Shall have the meaning as per Clause 3.2 of Schedule 7: Panel.
Denial of Service Event		Means any unauthorised attempt to make any part of a System wholly or partially unavailable for use for a period of time.
Disclosing Party		means a Party, Other User, Code Manager, Code Compliance Officer or DSP, when it discloses its Confidential Information, directly or indirectly, to the Panel.
Dispute		Means any dispute or difference (of whatever nature) arising under, out of or in connection with this Code and/or any bilateral agreement.
Disputing Party		Has the meaning given to that expression in Clause 19.1 of the Main Body.
Distribution System Operator	DSO	Means the legal entity holding the Distribution System Operator Licence.
DPC Self-Assessment Checklist		Means a checklist to evidence compliance with Data Protection Legislation provided by the Data Protection Commissioner.
DSP Personnel		Means those natural persons who are engaged by the Data Systems Provider (DSP), in so far as such persons carry out, or are authorised to carry out, any activity in relation to the DSP's

Term	Acronym	Definition
		responsibilities and obligations for the maintenance and administration of the Smart Meter Data System.
DSP Service Provider		Means a natural or legal person which carries out the functions or tasks of the Data Systems Provider (DSP) on behalf of the DSP.
Elected Member		Has the meaning given to that expression in Clause 3.3 of Schedule 7: Panel.
Electricity Industry Arrangements		Means any regulatory multilateral code or agreement, or obligations, maintained pursuant to one or more Licence Condition.
Electricity Supplier		Has the meaning as defined in the as defined in Statutory Instrument 426 of 2014.
Electricity Supplier Party		Means a Party that is an Electricity Supplier.
Entry Assessment		Means an assessment conducted on all Applicants or user prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
European Economic Area	EEA	Has the meaning as defined in Data Protection Legislation.
Event of Breach		Has the meaning given to that expression in Clause 21 of the Main Body.
Extraordinary Panel Meeting		Any meeting of the Panel that meets to discuss any business it deems urgent and can be convened on such notice (but in any event not less than one hour's notice) as the Panel Chair considers appropriate, and such that, where practicable within the time available, as many Panel Members as possible may attend but subject to the quoracy provisions of Clause 5.4 of Schedule 7: Panel.

Term	Acronym	Definition
Final Customer		Means a natural or legal person who receives, or wishes to receive, a supply of energy at any premises in the Republic of Ireland, in accordance with Statutory Instrument (SI) 37 of 2022.
Final DAR Change Proposal Report		Has the meaning given to that expression in Clause 27.10 of Schedule 9: Change Management.
Final Modification Report		Has the meaning given to that expression in Clause 20.2 of Schedule 9: Change Management.
Force Majeure		Means, in respect of any Party, the Affected Party, any event or circumstance which is beyond the reasonable control of the Affected Party, but only to the extent such event or circumstance (or its consequences) could not have been prevented or avoided had the Affected Party acted in accordance with Good Industry Practice. Neither lack of funds nor strikes or other industrial disturbances affecting only the employees of the Affected Party and/or its contractors shall be interpreted as an event or circumstance beyond the Affected Party's control. Circumstance of force majeure for the purposes of the Code as set out in Clause 18 of the Main Body.
Framework Agreement		Means an agreement in the form set out in Schedule 3: Accession.
GDPR		Means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such Data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Go Live Date		Means the time and date designated by the Commission when all exit criteria have been met and handover to steady state governance has taken place and

Term	Acronym	Definition
		the provisions of this Code are deemed to be in effect.
Good Industry Practice		Means, in respect of a person, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced organisation engaged in a similar type of undertaking as that person under the same or similar circumstances, complying with all applicable laws, codes of professional conduct, relevant codes of practice, Irish, European and other relevant standards.
Housekeeping Modification Proposal		Means a Modification Proposal which satisfies the requirements of Clause 24 of Schedule 9: Change Management.
Housekeeping Modification Report		Means a written report on a Housekeeping Modification Proposal, as described in Clause 24 of Schedule 9: Change Management.
Information Classification Scheme		Means a methodology for: a) the appropriate classification of all Data that are Processed or stored on a System by reference to the potential impact of those Data being Compromised; and b) determining the controls to be applied to the Processing, storage, transfer and deletion of each such class of those Data.
Insolvency Type Event		Means any legal proceedings or other procedure or step taken in relation to: (a) the suspension of payments, a moratorium of any indebtedness, winding-up, dissolution, administration or reorganisation (by way of voluntary arrangement, scheme of arrangement or otherwise), bankruptcy or sequestration of any Final Customer; (b) a composition, compromise, assignment or arrangement with any creditor of a Final Customer; (c) the appointment of a liquidator, receiver, administrative receiver, administrator, trustee in

Term	Acronym	Definition
		bankruptcy, trustee in sequestration, compulsory manager or other similar officer in respect of any Final Customer, (d) the enforcement of any guarantee or security over any assets of any Final Customer, or (e) any analogous procedure or step taken in any jurisdiction.
Interim Election		Means the process that applies in respect of a Panel Member being removed from office in accordance with Clause 3.3 of Schedule 7: Panel.
Legal Basis, Legal Bases		Has the meaning as defined in Data Protection Legislation.
Licence		The Licence granted by the Commission to the DSO / Electricity Suppliers under the Electricity Regulation Act, 1999.
Major Security Incident		Means, in relation to any System or Smart Meter Data, any event which results, or was capable of resulting, in that System or Smart Meter Data being Compromised to a material extent.
Material Change, Materially Changed		Means a change to a Party's Systems or processes which is of such a type or magnitude as to raise the reasonable expectation of an impact on that Party's ability to meet its obligations under this Code.
Meter Point Reference Number	MPRN	Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Meter Registration System Operator	MRSO	Means the legal entity responsible for the Change of Supplier process and the communication/aggregation of Consumption Data.
Metering Point		Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Modification		A modification, revision, amendment, supplementation, extension, consolidation or replacement to the

Term	Acronym	Definition
		provisions of the Code which is accepted and implemented in accordance with Schedule 9: Change Management.
Modification Path		Means one of the three modification paths followed by a Modification Proposal, being either a Commission-Approved Modification, a Self-Governance Modification or a Housekeeping Modification.
Modification Proposal		Means the term applied to a Modification proposed in accordance with Clause 15 of the Main Body and Schedule 9: Change Management.
Modification Proposal Plan		Means, in respect of a Modification Proposal, a plan produced in accordance with Clause 9.5 of Schedule 9: Change Management.
Modification Report		Has the meaning given to that expression in Schedule 9: Change Management.
National Smart Metering Programme	NSMP	Means the National Smart Metering Programme within the Republic of Ireland.
New Party		Means a person that has agreed to be bound by this Code in accordance with an Accession Agreement.
Non-Personal Data		Has the definition within Article 3(1) of Regulation 2018/1807 of the European Parliament and Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.
Objection Deadline		Means the period by which an objection can validly be raised, as defined in Clause 20 of the Main Body.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.

Term	Acronym	Definition
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Panel Chair		Has the meaning given to that expression in Clause 3.1 of Schedule 7: Panel.
Panel Chair Appointee		Shall have the meaning as per Clause 3.8 in Schedule 7: Panel.
Panel Meeting		Shall have a meaning as per Clause 5.1 to 5.3 of Schedule 7: Panel.
Panel Member		Has the meaning given to that expression in Clause 8.8 of the Main Body.
Panel Objectives		Has the meaning given to that expression in Clause 8.4 of the Main Body.
Panel Proceedings		Shall have the meaning as per Clause 5 of Schedule 7: Panel.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Party Category		Means one of the following categories of Party: (a) the DSO; (b) Electricity Suppliers; (c) the TSO; and (d) the SMO.
Performance Indicator		Means an indicator of service performance from time to time determined by the Panel, on which the DSP is to report.
Personal Data		Has the meaning as defined in the GDPR, as applicable to Data Processed on the Smart Meter Data System. This includes the Data Items marked as Personal Data within Appendix A: Data Glossary of the Code.
Personal Data Breach		Has the meaning as defined in Data Protection Legislation.

Term	Acronym	Definition
Preliminary DAR Change Proposal Report		Means a report which satisfied the requirements of Clause 27.5 of Schedule 9: Change Management.
Preliminary Modification Report		Means the written report on a Modification Proposal prepared by the Code Manager in accordance with Clause 19 of the Schedule 9: Change Management.
Privacy Controls Framework	PCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Privacy Statement		Has the meaning as defined in Data Protection Legislation.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Profiling		Has the meaning as defined in Data Protection Legislation.
Proposer		Means a person who submits a Modification Proposal or DAR Change Proposal.
Provisional DAR Change Proposal Report		Has the meaning given to that expression in Clause 27.6 of Schedule 9: Change Management.
Receiving Party		Means a Panel Member when it receives Confidential Information, directly or indirectly, from a Party, Other User, Code Manager, Code Compliance Officer or DSP.
Recognised Standards		A common set of acceptable international or national information security standards endorsed by the Competent Authority.
Registered Supplier		Means, in respect of a Metering Point and at any time, the Electricity Supplier recorded against that Metering Point in the MRSO at that time.
Related Person		Means, in relation to an individual: a) any member of that individual's immediate family (including parent, partner and children);

Term	Acronym	Definition
		b) any person in partnership with that individual or a member of that individual's immediate family; c) any employer of that individual or a member of the individual's immediate family; d) any Affiliate or related undertaking of such employer; and e) any related undertaking of that individual or a member of that individual's immediate family.
Release Plan		Means the document of that name published by the Code Manager in accordance with Clause 26 of Schedule 9: Change Management.
Remedial Plan		Means a document describing how a failure to comply with this Code will be remedied by the Party or Other User in question, and how the risk of future failures is to be mitigated.
Replacement Supplier		Means a supplier appointed by means of a direction by the Commission under its customer protection protocols.
Retail Market Procedures		Means the Republic of Ireland Retail Electricity Market processes which take place between Market Participants and ESB Networks.
Risk Treatment Plan		Has the meaning given to that expression in Clause 6.2(d) of Schedule 10: Security Sub-Committee.
Schedule		Means a Schedule to this Code.
Scheduled Election		Means an Election that occurs in accordance with the process described in Clause 4.4 of Schedule 7: Panel.
Secretariat		Means the allocated role to perform those tasks and functions expressly ascribed to it under the Code and any other tasks and functions as the Panel may assign to the Secretariat from time to time.
Security Controls Framework	SCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.

Term	Acronym	Definition
Security Incident		Means an actual or potential impact on the confidentiality, integrity or availability of Smart Meter Data or a System.
Security Risk Register		Means a register of data protection and information security risks in relation to the Smart Meter Data System and related Systems, maintained by the Security Sub-Committee.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Security Sub-Committee Chair		Has the meaning given to that expression in Clause 4.3 of Schedule 10: Security Sub-Committee.
Security Sub-Committee (Supplier) Member		Has the meaning given to that expression in Clause 4.6 of Schedule 10: Security Sub-Committee.
Security Sub-Committee Member		Has the meaning given to that expression in Clause 4.1 of Schedule 10: Security Sub-Committee.
Security Sub-Committee Terms of Reference		Means the terms of reference according to which the Security Sub-Committee shall be formed and shall operate.
Self-Governance Modification		Means a Modification Proposal which is a Panel approved change.
Separate, Separated		Means, in relation to any System, software or firmware, to establish controls which are appropriately designed to ensure that no communication may take place between it and any other System, software or firmware (as the case may be) except to the extent that such communication is for a necessary purpose having regard to the intended operation of the System, software or firmware.
Single Market Operator	SMO	Means the entity responsible for administering the market functions of the single electricity market (SEM).
Smart Meter Data		Has the meaning as defined in Statutory Instrument 37 of 2022. ***Potentially to be***

Term	Acronym	Definition
		replaced by the definition in the final legislation
Smart Meter Data Access Arrangements		Means such arrangements (including all necessary systems, contracts, processes, procedures, resources, products, and facilities) required to establish, procure, or otherwise have in place under or pursuant to the Code in connection with the provision of services, whether on behalf of or to Parties or otherwise.
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Smart Meter System		Means an electronic System that can measure energy consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication, as defined in Statutory Instrument 426 of 2014, and that connects to the Smart Meter Data System.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time in accordance with Schedule 9: Panel.
Sub-Processor, Sub-Processing		Has the meaning as defined in Data Protection Legislation.
Supplier of Last Resort	SoLR	Means, in respect of each premises supplied by a failing Electricity Supplier, the Supplier directed to supply gas and/or electricity to that premises by the Commission under the Commission's customer protection protocols.
System(s)		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware,

Term	Acronym	Definition
		software, firmware and Data associated therewith.
System Development Lifecycle		Means, in relation to any System, the whole of the life of that System from its initial concept to ultimate disposal, including the stages of development, design, build, testing, configuration, implementation, operation, maintenance, modification and decommissioning.
Test, Testing		Means carrying out the activities defined in the Test Strategy and/or Test Plan.
Test Data		Means the Data to be used for Testing Purposes during a Test Phase.
Test Environments		Means the testing environments as described in the Test Plan.
Test Phase(s)		Means each phase of testing as set out in the DSP Test Plan.
Test Plan		Has the meaning given to that expression in Clauses 26.1 and 26.2 of Schedule 9: Change Management.
Test Strategy		Means the document produced by the Code Manager setting out the Testing objectives and approach to coordinating testing activities between the DSP, Parties and Other Users.
Testing Purposes		Means for the purposes of testing as set out in the Code Test Strategy.
Third Party		A natural or legal person that accesses or uses Data (including but not limited to Consumption Data) on behalf of a Party or Other User, without themselves being a Party or Other User.
Transmission System Operator	TSO	Means the legal entity responsible for conveying electricity on the high voltage electricity network (the 'Transmission System') and for the operation and development of that system.
Unaggregated Bulk Data		Data which has been broken down into segments or categories, and which is

Term	Acronym	Definition
		accessed or received in a single packet or set of records.
User Category		A Category of user as defined in Schedule 2: Access Arrangements.
User Information Security Management System		Means a user's policies and procedures for systematically managing the user's Data and Systems, particularly with respect to Smart Meter Data and User Systems.
User Personnel		Means those persons who are engaged by a user, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the business of the user in the exercise of rights and compliance with obligations under this Code.
User System, User Systems		Means a user's System, which is used for accessing the Smart Meter Data System or using Smart Meter Data received from the Smart Meter Data System.
Voting Group		Means, in respect of each Party Category with a right to vote, each Party that falls into that Party Category collectively with that Party's Affiliates (if any) who also fall into that Party Category.
Vulnerable Customer		Means as defined in 7.1 of the Code of Practice for Vulnerable Customers
Withdrawal Date		Means the time and date on which a Party wishes to withdraw from this Code, as specified in its Withdrawal Notice.
Withdrawal Notice		Means a notice given by a Party in accordance with Clause 4 of Schedule 8: Party Exit indicating that Party's wish to withdraw from this Code.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.

Term	Acronym	Definition
Working Group		Means a group of persons, established by the Panel, for the purposes set out in Schedule 7: Panel and Schedule 9: Change Management.
Working Group Terms of Reference		Means the document produced by the Responsible Sub-Committee and published on the Code Website for the Working Group to operate in accordance with.
Working Hour		Means any hour between 09:00 and 17:00 on a Working Day.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 2:
Access Arrangements

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Schedule 2: Access Arrangements

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD-Mon-YY		n.n

1 Definitions

Term	Acronym	Definition
Access Agreement		Means an Agreement by which an organisation that is not a Party can access the Smart Meter Data System.
Access Log		Means a log of Third Parties' and users' access to Data, including Consumption Data, on the Smart Meter Data System, which includes: a) a timestamp of the time of access; b) the Data Items accessed; c) an identification of the Third Party or user accessing the Data; and d) the identification of the permission or other Legal Basis used by the Third Party to access the Data.
Anonymous Data		Means Data which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
Applicant		Means any person who applies to be admitted as a Party, subject to and in accordance with the Code.
Basic Access		Means, in relation to an application for access under Schedule 2: Access Arrangements, a request by a user for access that involves access to existing Data Items assigned to that User Category.
Central Statistics Office	CSO	Means the legal entity responsible for providing an accurate picture of the Republic of Ireland's economic and social performance.
Change Proposal	CP	Means a proposal to change a subsidiary document to the Code and Schedules, in accordance with Schedule 9: Change Management.

Term	Acronym	Definition
Code, Smart Meter Data Access Code	SMDAC	Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code. Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Complex Access		Means, in relation to an application for access under Schedule 2: Access Arrangements, a request by a user for access that involves: a) Access to a new Data Item, and/or; b) Access to a Data Item not assigned to that User Category, and/or; c) Access to Data Items by a user within a new User Category.
Consumption Data		Means, in respect of a premises, the quantity of electricity or gas measured by the Smart Meter as having been supplied to the relevant premises.
Data		Means any information, data, knowledge, figures, methodologies,

Term	Acronym	Definition
		minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Data Item		Means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for which are defined and controlled in the Data Access Register.
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data Dictionary		Means a document maintained by the DSP that shall establish the Data Items, Identifiers and Description of the Data Items available on the Smart Meter Data System.
Data Glossary		Means a document maintained as per Appendix 1 of this Code that shall establish an explanation of the types of Data, including Personal Data, available on the Smart Meter Data System. The Data Glossary includes the information contained within the Data Dictionary.
Data Protection Impact Assessment	DPIA	Has the meaning as defined in Data Protection Legislation.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, in accordance with Clause 12 of the Main Body.
Data Subject		Has the meaning as defined in Data Protection Legislation.

Term	Acronym	Definition
Distribution System Operator	DSO	Means the legal entity holding the Distribution System Operator Licence.
Electricity Supplier		Has the meaning as defined in the as defined in Statutory Instrument 426 of 2014.
Entry Assessment		Means an assessment conducted on all Applicants or user prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
Event of Breach		Has the meaning given to that expression in Clause 21 of the Main Body.
Final Customer		Means a natural or legal person who receives, or wishes to receive, a supply of energy at any premises in the Republic of Ireland, in accordance with Statutory Instrument (SI) 37 of 2022.
Go Live Date		Means the time and date designated by the Commission when all exit criteria have been met and handover to steady state governance has taken place and the provisions of this Code are deemed to be in effect.
Legal Basis, Legal Bases		Has the meaning as defined in Data Protection Legislation.
Licence		The Licence granted by the Commission to the DSO / Electricity Suppliers under the Electricity Regulation Act, 1999.
Modification Proposal	MP	Means the term applied to a Draft Proposal once the Panel has agreed it should be progressed further in accordance with Clause 15 of the Main Body.
Other User(s)		A natural or legal person that has access to the Smart Meter Data

Term	Acronym	Definition
		System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Personal Data		Has the meaning as defined in the GDPR, as applicable to Data Processed on the Smart Meter Data System. This includes the Data Items marked as Personal Data within Appendix A (Data Glossary) of the Code.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Schedule		Means a Schedule to this Code.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Single Market Operator	SMO	Means the entity responsible for administering the market functions of the single electricity market (SEM).
Smart Meter Data		Has the meaning as defined in Statutory Instrument 37 of 2022. ***Potentially to be replaced by the definition in the final legislation***
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time

Term	Acronym	Definition
		in accordance with Schedule 9: Panel.
Third Party		A natural or legal person that accesses or uses Data (including but not limited to Consumption Data) on behalf of a Party or Other User, without themselves being a Party or Other User.
Transmission System Operator	TSO	Means the legal entity responsible for conveying electricity on the high voltage electricity network (the 'Transmission System') and for the operation and development of that system.
User Category		A category of user, used to identify the class of user under these Access Arrangements. Each Party or Other User will be assigned to a User Category.

2 Introduction

2.1. This Smart Meter Data Access Schedule describes:

(a) how to become a user of the Smart Meter Data System;

(b) the Data Access Register which governs the data that each different User Category can access;

(c) the purposes for which each User Category is authorised to use the Smart Meter Data;

(d) the obligations on the Data System Provider (DSP) to make Data available;

(e) how changes to the Data Access Register will be made; and

(f) the mechanism by which Final Customers can request access to their Personal Data, including Consumption Data from the Smart Meter Data System, and a copy of their relevant Access Log in accordance with rights applicable to Final Customers under Schedule 5: Data Privacy.

3 Obtaining Access

Basic Principles

3.1. The Distribution Systems Operator (DSO), Transmission System Operator (TSO),

Single Market Operator (SMO) and Electricity Suppliers are entitled to become Parties to the Code as described in Clause 5 of the Main Body. These entities will still need to undertake Entry Assessment before access to the Smart Meter Data System will be permitted.

3.2. Any organisation wishing to become a user and access the Smart Meter Data System must apply to the Code Manager.

3.3. A Party will be required to undertake an Entry Assessment before access to the Smart Meter Data System will be approved, under Clause 7.3 of the Main Body.

3.4. Any organisation ('Other User') that is not a Party to the Code will be required to:

(a) sign an Access Agreement, which shall incorporate relevant Clauses of the Code, including Schedule 1: Interpretations, Schedule 4: Data Security, Schedule 5: Data Privacy, Clause 4 and 6 of Schedule 8: Party Exit and Clauses 21 and 23 of the Main Body, amongst other provisions and;

(b) undertake an Entry Assessment under Clauses 7.6 of the Main Body before access to the Smart Meter Data System will be approved.

Complex and Basic Access

3.5. Each application for specific access to Data Items shall be assessed by the Code Manager against criteria approved by the Panel.

3.6. Parties, including the Distribution Systems Operator (DSO), Transmission System Operator (TSO), Single Market Operator (SMO) Electricity Suppliers will be entitled to access Data Items on the Smart Meter Data System as defined for their User Category in the Data Access Register under the Basic Access procedure. These Parties will also have the ability to request access to additional Data Items on the Smart Meter Data System under the Complex Access process.

3.7. Other Users will be entitled to access Data Items on the Smart Meter Data System as defined in their Access Agreements under the Basic Access procedure. These Parties will also have the ability to request access to additional Data Items on the Smart Meter Data System under the Complex Access process.

3.8. Other Users in a new User Category, defined as a User Category not listed in the Data Access Register, will only be able to access pursuant to the Complex Access process.

3.9. Where an Applicant (a Party or Other User) requests access under the Basic Access procedure, the Code Manager shall assess their application on receipt.

3.10. Under both the Basic and Complex Access procedures, the criteria used by the Code

Manager in assessing the request for access may differ for each User Category and shall include as a minimum:

(a) Verification of the Applicant's identity;

(b) Confirmation that the Applicant meets the characteristics expected for the requested User Category;

(c) Confirmation that the relevant data security and data privacy controls are in place with respect to the risk associated with accessing the Data Item(s);

(d) Confirmation that the Data Items the Applicant wishes to access are consistent with the User Category permitted in the Data Access Register.

Assessments under the Complex Access procedure

3.11. Where a request for access to Data Items under the Complex Access process is submitted to the Code Manager, the Code Manager shall escalate this to the Panel, who will delegate the assessment to the Security Sub-Committee and Code Compliance Officer.

3.12. Where a request for access to Data in bulk format from the Smart Meter Data System occurs, the following procedure shall be followed:

(a) the request shall be assessed by the Code Manager against criteria provided by the Panel;

(b) on approval of the request, by the Panel, the DSP shall ensure that such bulk Data is provided to the user requesting the Data, and such Data will only be provided as Anonymous Data. The DSP shall be responsible for carrying out the anonymisation of Data prior to making the Data available to the user; and

(c) the DSP shall ensure that the Data is provided using a secure file transfer protocol ('SFTP') via a file share made available by the DSP for accessing the Data.

3.13. In accordance with Clause 3.11, the Code Compliance Officer shall conduct the assessment and submit a report the Panel for approval. Based on the report from the Code Compliance Officer, the Security Sub-Committee shall decide if the application for access should be approved or rejected based on its assessment of the criteria and shall advise the Applicant of the outcome, including the rationale for any rejection and make a recommendation to the Panel for approval.

3.14. In certain cases involving Complex Access and at the request of the Panel, the Code Compliance Officer shall conduct a Data Protection Impact Assessment on any proposed access to Smart Meter Data, which may involve the following:

(a) The creation of a new User Category, the effect of which would be to grant access to new organisations or groups of organisations not previously granted access to the Smart Meter Data System;

(b) Access to any new Data Items on the Smart Meter Data System, including if a previously unavailable Data Item becomes available on the Smart Meter Data System for users to access.

3.15. Where Clause 3.14 applies, the Security Sub-Committee shall consider the outcomes of the Data Protection Impact Assessment conducted by the Code Compliance Officer and any mitigating actions required to be implemented as identified by the Data Protection Impact Assessment in making its decision under Clause 3.13.

3.16. Where an Applicant disagrees with the Security Sub Committee's decision to reject its application, the Applicant may appeal that decision to the Panel in accordance with Clause 3.9 of the Main Body.

3.17. Once a Party or Other User has completed the necessary steps to become a user, the Code Manager shall:

(a) In the case of access to a new Data Item, update its Data Access Register and Data Glossary, and notify the DSP which shall update its Data Dictionary with the relevant Data Item and provide access to the appropriate users on the Smart Meter Data System as per Clause 12 of the Main Body.

(b) In the case of access to a new User Category, add the new User Category and the relevant Party or Other User's details to its Data Access Register and notify the DSP, which shall provide access to the appropriate users on the Smart Meter Data System, as per Clause 12 of the Main Body.

3.18. Each user that no longer wishes to access certain Data Items shall notify the Code Manager in writing of the date from which the user no longer wishes to access those Data Items. The relevant Party or Other User shall cease to be a user in with respect to the relevant Data Items with effect from the date specified in such notification.

3.19. Where the Code Manager receives a notification that a user no longer wishes to access certain Data Items in accordance with Clause 3.17, the Code Manager shall:

(a) update its Data Access Register to identify that the user will no longer have access to the relevant Data Items.

(b) notify the DSP which shall remove access to the appropriate user to the relevant Data Items on the Smart Meter Data System as per Clause 12 of the Main Body.

Final Customer Access

3.20. Final Customers shall have the right to request access to their Personal Data, including Consumption Data from the Smart Meter Data System, in accordance with Schedule 5: Data Privacy.

3.21. Final Customers shall have the right to request access to a copy of their relevant Access Log in accordance with Schedule 5: Data Privacy.

3.22. In accordance with their obligations under Schedule 5: Data Privacy, the DSP and Parties shall facilitate requests from Final Customers exercising their rights, including giving consent and revoking access to Data.

4 Data Access Register

4.1. The Data Access Register shall set out the Data Items that each User Category can access, the Legal Basis for Personal Data, the type of Data and the mechanism by which it can access them.

4.2. The Data Access Register shall also set out the Data Items that an Other User may have access to, subject to an Access Agreement.

4.3. The Data Access Register shall also set out where a user or User Category has access to Anonymous Data.

5 Purpose of Access or Use

5.1. Users shall only access Data in accordance with the terms set out in this Schedule.

5.2. Users are authorised to use Data only for the purposes specified in accordance with this Clause 5. No user shall use the Data, including Personal Data, for any other purpose unless as specified by Schedule 5: Data Privacy.

5.3. Within each purpose, users shall be permitted to access Smart Meter Data in accordance with the Legal Bases specified in Schedule 5: Data Privacy and the Access Agreement with the user, as applicable.

5.4. The Code Manager shall identify and maintain, within the Data Access Register, a list of authorised purposes, including each and any references to a Legal Basis, for which each User Category may access Data, including Personal Data, within the Data Access Register.

5.5. In addition to the purposes identified in accordance with Clause 5.4, each User Category may access Data for purposes as approved by the Panel from time to time. The Code Manager shall maintain a list the Panel approved purposes, for which each User Category may use Data, within the Data Access Register.

5.6. Any DAR Changes as a result of Clauses 5.4 or 5.5 shall not require a DAR Change Proposal and as such Schedule 9: Change Management shall not apply. However, the Code Manager shall inform all Parties, Other Users, the Commission and Code Panel of the DAR Changes and publish on the Code Website.

5.7. Any access of Data and/or use of Data other than in accordance with this Schedule shall be a breach of the Code and may lead to an Event of Breach.

6 Adding or Removing a Data Item in the Data Access Register

6.1. Register (DAR) Change Proposal, regardless of whether or not they are a Party, to add or remove a Data Item in the Data Access Register. Such submission should be made in accordance with Schedule 9: Change Management.

6.2. Where a DAR Change Proposal, that either adds or removes a Data Item is approved, the Code Manager shall, as part of the implementation of the approved DAR Change Proposal:

(a) update its Data Access Register detailing access to the relevant Data Items;

(b) update its Data Glossary under Appendix 1 with the relevant Data Items; and

(c) notify the DSP, which shall update its Data Dictionary with the relevant Data Item(s) and provide access to the appropriate users on the Smart Meter Data System as per Clause 12 of the Main Body.

7 Adding a New User Category to the Data Access Register

7.1. Where the Code Manager receives an application that does not conform to the characteristics of an existing User Category the Code Manager shall:

(a) identify the purpose for which users in this new User Category intend to use the Data; and

(b) notify the Applicant that a DAR Change Proposal is required in accordance with Clause 27 of Schedule 9: Change Management.

7.2. Where a DAR Change Proposal that adds a new User Category is approved, the Code Manager shall, as part of the implementation of the approved DAR Change Proposal:

(a) add the new User Category to the Data Access Register; and

(b) notify the DSP, which shall provide access to the appropriate user(s) on the Smart Meter Data System, as per Clause 12 of the Main Body.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 3: Accession

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Schedule 3: Accession

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD Month YYYY		n.n

1 Definitions

Term	Acronym	Definition
Accession Agreement		Means an agreement by which a Party agrees to be bound by this Code, as set out in this Schedule.
Applicant		Means any person who applies to be admitted as a Party, subject to and in accordance with the Code.
Assessment Report		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.
Assessment Response		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.
Assurance Strategy		Has the meaning given to that expression in Clause 7.8 of the Main Body.
Assurance Status		Has the meaning given to that expression in Clause 3.9 of Schedule 6: Assessments.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code. Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.

Term	Acronym	Definition
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, in accordance with Clause 12 of the Main Body.
Distribution System Operator	DSO	Means the legal entity holding the Distribution System Operator Licence.
Electricity Supplier		Has the meaning as defined in the as defined in Statutory Instrument 426 of 2014.
Entry Assessment		Means an assessment conducted on all Applicants or user prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
Final Customer		Means a natural or legal person who receives, or wishes to receive, a supply of energy at any premises in the Republic of Ireland, in accordance with Statutory Instrument (SI) 37 of 2022.
Licence		The Licence granted by the Commission to the DSO / Electricity Suppliers under the Electricity Regulation Act, 1999.
New Party		Means a person that has agreed to be bound by this Code in accordance with an Accession Agreement.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.

Term	Acronym	Definition
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Schedule		Means a Schedule to this Code.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Single Market Operator	SMO	Means the entity responsible for administering the market functions of the single electricity market (SEM).
Smart Meter Data		Has the meaning as defined in Statutory Instrument 37 of 2022. ***Potentially to be replaced by the definition in the final legislation***
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time in accordance with Schedule 9: Panel.
Third Party		A natural or legal person that accesses or uses Data (including but not limited to Consumption Data) on behalf of a Party or Other User, without themselves being a Party or Other User.
Transmission System Operator	TSO	Means the legal entity responsible for conveying electricity on the high

Term	Acronym	Definition
		voltage electricity network (the 'Transmission System') and for the operation and development of that system.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.

2 Eligible Parties

2.1. Clause 5 of the Main Body sets out those categories of person that are eligible to become a Party (Eligible Party). This Schedule is applicable to the following Eligible Parties:

(a) the DSO;
(b) the Data Systems Provider (DSP);
(c) Electricity Suppliers;
(d) the Transmission System Operator (TSO); and
(e) the Single Market Operator (SMO).

2.2. The Access Arrangements for Eligible Parties are set out in Schedule 2: Access Arrangements.

2.3. Other Users cannot become a Party, but are able to obtain access to Smart Meter Data by either:

(a) by entering into an Access Agreement as an Other User, as further described in Schedule 2: Access Arrangements; or
(b) as provided directly from each individual Final Customer.

2.4. Final Customers cannot become a Party, but may, in accordance with the provisions of Schedule 5: Data Privacy:

(a) Obtain access to their own Smart Meter Data from the DSO or their Electricity Supplier in accordance with their rights as Final Customers; and
(b) provide such to a Third Party, as they see fit.

3 Becoming a Party

3.1. This Schedule is to be read in accordance with Clause 6 of the Main Body.

3.2. A person may only become a Party to the Code in accordance with the terms of the Code.

3.3. In order to become a Party, a person (the "Applicant") must apply to the Code Manager in accordance with this Schedule and the Assurance Strategy, which specify all conditions which the Applicant must meet to become a Party, including that the Applicant shall, when provided, execute the Accession Agreement to adhere to the Code.

3.4. Within 10 Working Days of receipt of the application, the Code Manager shall notify the Applicant if:

(a) the Applicant is to proceed to Entry Assessment;
(b) the Applicant is not eligible to become a Party (as described in Clause 2.1); or
(c) further information is required from the Applicant, as specified in such notice, in order to complete the information referred to in the application.

3.5. Where the Applicant is to proceed to undertake an Entry Assessment in accordance with Clause 7 of the Main Body, the Code Manager shall request the Code Compliance Officer to conduct such an assessment.

3.6. Where Clause 3.5 applies, the Code Compliance Officer shall liaise with the Applicant in order to organise an Entry Assessment in accordance with Schedule 6: Assessments at a time suitable for both Parties.

3.7. In accordance with the process under Schedule 6: Assessments, once the Code Compliance Officer has provided its Assessment Report and Assessment Response and the Security Sub-Committee has set the Assurance Status of the Applicant, then the Code Manager shall notify the Applicant, the Panel and the Commission that:

(a) the Applicant is to be admitted as a Party;
(b) the Applicant is not eligible to become a Party (as described in Clause 2.1); or
(c) further information is required from the Applicant, as specified in such notice, in order to complete the information referred to in the application.

3.8. If the Code Manager does not receive the clarification or the additional information from the Applicant within 20 Working Days after the Code Manager's request for information under Clause 3.4(c), the application shall lapse. An Applicant may request additional

time to provide any additional information and the Code Manager shall not unreasonably withhold consent to any such request. If the application lapses, this does not prevent the Applicant submitting a new application at a later date. Following the provision of further information by the Applicant, Clause 3.4 shall apply again.

3.9. If the Code Manager decides that the Applicant is not to be admitted as a New Party, then the Code Manager shall provide the Applicant with the reasons for the decision. The Applicant may appeal the decision in accordance with Clause 3.4 to the Panel for determination. Any such appeal is subject to the Appeals process in Clause 19.8.

3.10. Where:

(a) the Code Manager issues a notice in accordance with Clause 3.4 that the Applicant is to be admitted as a New Party; or

(b) the Panel determines that the Applicant shall be admitted as a New Party,

then the Code Manager shall, within 10 Working Days of the decision under Clause 3.7(a) or 3.7(b), send to the Applicant the Accession Agreement executed by the Panel on behalf of all the Parties.

3.11. Each Party hereby authorises and instructs the Panel to execute each Accession Agreement on the Party's behalf. Each Party undertakes not to withdraw, qualify or revoke any such authority or instruction at any time.

3.12. The Applicant must submit an executed Accession Agreement within 20 Working Days of receipt from the Code Manager. An Applicant may request additional time to submit an executed Accession Agreement and the Code Manager shall not unreasonably withhold consent to any such request, provided that the date of receipt of the executed Accession Agreement shall be earlier than the effective date specified in the Accession Agreement.

3.13. Upon the execution and delivery of an Applicant's Accession Agreement by the Panel and the Applicant, the Applicant shall become a Party for all purposes of this Code from the date specified in such Accession Agreement.

3.14. The Code Manager shall publish the fact and date of the accession of each new Party to the Code.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 4: Data Security

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Schedule 4: Data Security

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD Mon YY		n.n

1 Definitions

Term	Acronym	Definition
Access Agreement		Means an Agreement by which an organisation that is not a Party can access the Smart Meter Data System.
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or c) where a new User Category or Data Item is issued.
Annual Self-Assessment		Means a self-assessment questionnaire issued to all users on an annual basis to identify the extent to which, since the last occasion on which a Self-Assessment was carried out in respect of that Other User or Party, there has been any Material Change in the arrangements that the Other User has in place to comply with its obligations under the Code or in the quantity of Consumption Data being accessed by the Other User or Party.
Anomalous Event		Means, in relation to any System, an activity or event that is not expected to occur in the course of the ordinary operation of that system.
Anonymous Data		Means Data which does not relate to an identified or identifiable natural person or to Personal Data

Term	Acronym	Definition
		rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
Applicant		Means any person who applies to be admitted as a Party, subject to and in accordance with the Code.
Back-Up, Backed-Up		Means, in relation to Data which is held on any System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Compromised		Means, in relation to the Smart Meter Data System, that the intended purpose or effective operation of the Smart Meter Data System is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity or availability of the Smart Meter Data System or of any Smart Meter Data that are stored on or communicated by means of it; or In relation to Smart Meter Data, that the confidentiality, integrity or availability of the Smart Meter Data is adversely affected by the occurrence of any event; and

Term	Acronym	Definition
		In relation to any process or to the functionality of any hardware, firmware or software, that the intended purpose or effective operation of that process or functionality is compromised by the occurrence of any event which has an adverse effect on its confidentiality, integrity or availability.
Consumption Data		Means, in respect of a premises, the quantity of electricity or gas measured by the Smart Meter as having been supplied to the relevant premises.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Data Item		Means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for which are defined and controlled in the Data Access Register.
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, as defined in Schedule 2: Access Arrangements.
Data Subject		Has the meaning as defined in Data Protection Legislation.
Denial of Service Event		Means any unauthorised attempt to make any part of a System wholly

Term	Acronym	Definition
		or partially unavailable for use for a period of time.
DPC Self-Assessment Checklist		Means a checklist to evidence compliance with Data Protection Legislation provided by the Data Protection Commissioner.
DSP Personnel		Means those natural persons who are engaged by the Data System Provider (DSP), in so far as such persons carry out, or are authorised to carry out, any activity in relation to the DSP's responsibilities and obligations for the maintenance and administration of the Smart Meter Data System.
DSP Service Provider		Means a natural or legal person which carries out the functions or tasks of the Data System Provider (DSP) on behalf of the DSP.
Entry Assessment		Means an assessment conducted on all Applicants or user prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
Event of Breach		Has the meaning given to that expression in Clause 21 of the Main Body.
Good Industry Practice		Means, in respect of a person, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced organisation engaged in a similar type of undertaking as that person under the same or similar circumstances, complying with all applicable laws, codes of professional conduct, relevant codes of practice, Irish, European and other relevant standards.
Information Classification Scheme		Means a methodology for:

Term	Acronym	Definition
		a) the appropriate classification of all Data that are Processed or stored on a System by reference to the potential impact of those Data being Compromised; and b) determining the controls to be applied to the Processing, storage, transfer and deletion of each such class of those Data.
Legal Basis, Legal Bases		Has the meaning as defined in Data Protection Legislation.
Major Security Incident		Means, in relation to any System or Smart Meter Data, any event which results, or was capable of resulting, in that System or Smart Meter Data being Compromised to a material extent.
Material Change, Materially Changed		Means a change to a Party's Systems or processes which is of such a type or magnitude as to raise the reasonable expectation of an impact on that Party's ability to meet its obligations under this Code.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Personal Data		Has the meaning as defined in the GDPR, as applicable to Data Processed on the Smart Meter Data System. This includes the Data Items marked as Personal Data

Term	Acronym	Definition
		within Appendix A (Data Glossary) of the Code.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Recognised Standards		A common set of acceptable international or national information security standards endorsed by the Competent Authority.
Schedule		Means a Schedule to this Code.
Security Controls Framework	SCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Security Incident		Means an actual or potential impact on the confidentiality, integrity or availability of Smart Meter Data or a System.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Separate, Separated		Means, in relation to any System, software or firmware, to establish controls which are appropriately designed to ensure that no communication may take place between it and any other System, software or firmware (as the case may be) except to the extent that such communication is for a necessary purpose having regard to the intended operation of the System, software or firmware.
Smart Meter Data		Has the meaning as defined in Statutory Instrument 426 of 2014. ***Potentially to be replaced by the definition in the final legislation***
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other

Term	Acronym	Definition
		Data associated with the Smart Meter.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time in accordance with Schedule 9: Panel.
System(s)		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith.
System Development Lifecycle		Means, in relation to any System, the whole of the life of that System from its initial concept to ultimate disposal, including the stages of development, design, build, testing, configuration, implementation, operation, maintenance, modification and decommissioning.
Test, Testing		Means carrying out the activities defined in the Test Strategy and/or Test Plan.
Test Environments		Means the testing environments as described in the Test Plan.
Test Plan		Has the meaning given to that expression in Clauses 26.1 and 26.2 of Schedule 9: Change Management.
Test Strategy		Means the document produced by the Code Manager setting out the Testing objectives and approach to coordinating testing activities between the Data System Provider and Parties and Other Users.
Unaggregated Bulk Data		Data which has been broken down into segments or categories, and which is accessed or received in a single packet or set of records.

Term	Acronym	Definition
User Category		A Category of user as defined in Schedule 2: Access Arrangements.
User Information Security Management System		Means a user's policies and procedures for systematically managing the user's Data and Systems, particularly with respect to Smart Meter Data and User Systems.
User Personnel		Means those persons who are engaged by a user, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the business of the user in the exercise of rights and compliance with obligations under this Code.
User System, User Systems		Means a user's System, which is used for accessing the Smart Meter Data System or using Smart Meter Data received from the Smart Meter Data System.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.
Working Hour		Means any hour between 09:00 and 17:00 on a Working Day.

2 Introduction

2.1. This Schedule sets out the obligations for data security for anyone accessing Smart Meter Data from any Smart Meter Data System. It is applicable to Parties and also to Other Users requesting access to Smart Meter Data.

3 Obligations on the Data System Provider

DSP Information Security Management System

3.1. The Data System Provider (DSP) shall establish, give effect to, maintain, and comply with a set of policies and procedures to be known as the DSP Information Security

Management System.

3.2. The DSP Information Security Management System shall incorporate an Information Security Policy, which makes appropriate provision in respect of:

(a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of any Smart Meter Data System, including measures relating to Data handling, retention and protection.

3.3. The DSP Information Security Management System shall specify the approach of the DSP to:

(a) information security, including its arrangements to review that approach at planned intervals;

(b) human resources security;

(c) physical and environmental security; and

(d) ensuring that any DSP Service Providers establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the DSP

3.4. The DSP Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:

(a) measures to restrict access to Data that is stored on or communicated by means of any Smart Meter Data System to those who require such Data and are authorised to obtain it;

(b) the designation of appropriate levels of identity assurance in respect of those who are authorised to access such Data;

(c) procedures for granting, amending and removing authorisations in respect of access to such Data; and

(d) measures to ensure that the activities of one individual may not become a means by which the Smart Meter Data Systems is Compromised to a material extent.

3.5. The DSP Information Security Management System shall incorporate procedures on the management of Security Incidents which, in particular, make provision for:

(a) the allocation of clearly defined roles and responsibilities to DSP Personnel;

(b) the manner in which such Security Incidents will be monitored, classified, reported to the Code Compliance Officer and managed;

(c) a communications plan in relation to all communications with respect to such Security Incidents; and

(d) the use of recovery systems in the case of Major Security Incidents.

3.6. The DSP Information Security Management System shall incorporate procedures on the management of business continuity that comply with Recognised Standards.

Unauthorised Activities: Duties to Detect and Respond

3.7. The DSP shall take reasonable steps to ensure that any Smart Meter Data System is capable of:

(a) detecting any unauthorised connection that has been made to it, and any unauthorised attempt to connect to it, by any other System, and

(i) if the Smart Meter Data System detects such a connection or attempted connection, to ensure that the connection is terminated or the attempted connection prevented (as the case may be);

(b) detecting any unauthorised software that has been installed or executed on it and any unauthorised attempt to install or execute software on it, and

(i) if the Smart Meter Data System detects any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(ii) where any such software has been installed or executed, to take appropriate remedial action;

(c) identifying any deviation from its expected configuration, and

(i) any such identified deviation is rectified; and

(ii) for these purposes, maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of any Smart Meter Data System; and

(d) identifying any unauthorised or unnecessary network port, protocol, communication, application or network service.

3.8. The DSP shall take reasonable steps to ensure that any Smart Meter Data System causes or permits:

(a) to be open at any time only those network ports, and allows only those protocols, which are required at that time for the effective operation of that System, and blocks all network ports and protocols which are not so required; and

(b) at any time only the making of such communications and the provision of such applications and network services as are required at that time for the effective operation of that System.

3.9. The DSP shall take reasonable steps to ensure that each component of any Smart Meter Data System is, at each point in time, enabled only with the functionality that is necessary for it effectively to fulfil its intended role within the Smart Meter Data System at that time.

3.10. The DSP shall:

(a) ensure that any Smart Meter Data System records all System activity (including all attempts to access resources or Data held on it) in audit logs;

(b) ensure that any Smart Meter Data System detects any attempt by any person to access resources or Data held on it without possessing the authorisation required to do so; and

(c) take reasonable steps to ensure that any Smart Meter Data System prevents any such attempt at unauthorised access.

3.11. The DSP shall take reasonable steps to ensure that any Smart Meter Data System is capable of detecting any instance of Data leaving it by any means (including, in particular, by network transfers and the use of removable media) without authorisation.

Adverse Events – Duties to Detect and Prevent

3.12. The DSP shall take reasonable steps to ensure that:

(a) any Smart Meter Data System detects any Denial of Service Event; and

(b) any unused or disabled component or functionality of any Smart Meter Data System is incapable of being a means by which that System is Compromised.

3.13. The DSP shall use its best endeavours to ensure that the Smart Meter Data System is not Compromised by:

(a) where a Smart Meter Data System is Compromised, minimising the extent to which it is Compromised and any adverse effect arising from it having been Compromised; and

(b) ensuring that the Smart Meter Data System detects any instance in which it has been Compromised.

Security Incident Management

3.14. The DSP shall ensure that, where any Smart Meter Data System detects any:

(a) unauthorised event or deviation; or

(b) event which results, or was capable of resulting, in a Smart Meter Data System being Compromised, the DSP takes all of the steps required by the DSP Information Security Management System.

3.15. The DSP shall, on the occurrence of a Major Security Incident in relation to any Smart Meter Data System:

(a) promptly notify the Code Compliance Officer within 8 hours of identification of the suspected or confirmed Incident. Where an incident occurs out of normal Working Hours, the 8 hours will commence from the start of the next Working Day.

System Design and Operation

3.16. The DSP shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate any Smart Meter Data System so as to protect it from being Compromised.

Management of Vulnerabilities

3.17. The DSP shall ensure that an independent organisation carries out assessments that are designed to identify any vulnerability of any Smart Meter Data System:

(a) on at least an annual basis;

(b) in respect of each new or Materially Changed component or functionality of any Smart Meter Data System, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to any Smart Meter Data System.

3.18. The DSP shall ensure that it carries out assessments that are designed to identify any vulnerability of any Smart Meter Data System:

(a) on at least an annual basis;

(b) in respect of each new or Materially Changed component or functionality of any Smart Meter Data System, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to any Smart Meter Data System

3.19. Where, following any assessment of a Smart Meter Data System any such vulnerability has been detected, the DSP shall:

(a) take reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable; and

(b) in the case of a material vulnerability, promptly notify the Code Compliance Officer of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed.

Management of Data

3.20. Where the DSP carries out a Back-Up of any Data held on any Smart Meter Data System, it shall ensure that the Data which are Backed-Up are:

(a) protected in accordance with the requirements of the Code is respect of data security and data protection, including when being transmitted for the purposes of Back-Up; and

(b) stored on media that are located in physically secure facilities, at least one of which facilities must be in a different location to that part of the Smart Meter Data System on which the Data being Backed-Up is ordinarily held.

3.21. The DSP shall develop and maintain, and hold all Data in accordance with, a DSP Data Retention Policy.

3.22. The DSP shall ensure that where, in accordance with the DSP Data Retention Policy, any Data are no longer required is securely deleted.

Smart Meter Data Systems: Duty to Separate

3.23. The DSP shall take reasonable steps to ensure that any software or firmware installed on any Smart Meter Data System for the purposes of security is Separated from any software or firmware that is installed on that System for any other purpose.

3.24. The DSP shall ensure that any Test Environments shall not contain Data, other than Anonymous Data, from any live environment.

Monitoring the Audit

3.25. The DSP shall ensure that all System activity audit logs are reviewed regularly in accordance with the DSP Information Security Management System.

3.26. The DSP shall take reasonable steps to ensure that any Smart Meter Data System is capable of detecting Anomalous Events, in particular by reference to the:

(a) audit logs of each component of the Smart Meter Data System; and

(b) error messages generated by each device, which forms part of the Smart Meter Data System.

3.27. The DSP shall:

(a) take reasonable steps to ensure that any Smart Meter Data System detects all Anomalous Events; and

(b) ensure that, on the detection of any Anomalous Event, it takes all steps required by the DSP Information Security Management System.

Manufacturers: Duty to Notify and Be Notified

3.28. Where the DSP becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which forms part of any Smart Meter Data System, it shall:

(a) wherever it is reasonably practicable to do so, notify the manufacturer of the hardware or the developer of the software or firmware (as the case may be);

(b) take reasonable steps to ensure that the cause of the vulnerability, or likely cause of the material adverse effect, is rectified or its potential impact is mitigated, as soon as is reasonably practicable; and

(c) promptly notify the Code Compliance Officer of the steps being taken to rectify the cause of the vulnerability, or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be) and the time within which those steps are intended to be completed.

3.29. The DSP shall not be required to notify a manufacturer or developer in where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

3.30. The DSP shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of any Smart Meter Data System arrangements designed to ensure that the DSP will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software or firmware.

Access and Identity Management

3.31. [TBC – pending details on ESBN solution(s)]

Cryptographic Credential Tokens and Smart Card Tokens

3.32. [TBC – pending details on ESBN solution(s)]

File Signing Software

3.33. [TBC – pending details on ESBN solution(s)]

4 Obligations on Parties and Other Users

4.1. Parties and Other Users requiring access to the Smart Meter Data held within any Smart Meter Data System shall apply for access to the Data in accordance with Schedule 2: Access Arrangements.

Data Security Assessment

4.2. Each Applicant shall submit the following information to the Code Compliance Officer, in accordance with its Entry Assessment under Schedule 6: Assessments:

(a) its internal information security and data protection risk assessment, including as a minimum:

(i) details of internal policies and procedures in place to mitigate information security and data protection risks associated with obligations under this Code (such as a Data Retention Policy, Acceptable Use Policy, Access Control Policy, Information Classification Policy, Business Continuity Policy);

(ii) internal user access controls;

(iii) management of security credentials; and

(iv) documentation of specific purpose for data access;

(b) evidence that it has a completed and up-to-date DPC Self-Assessment Checklist, available through the DPC's website; and

(c) evidence that it has appropriate information security controls reflective of the risks applicable to its organisation.

4.3. Where the application includes a request for access to Unaggregated Bulk Data from any Smart Meter Data System, the Applicant will be required to demonstrate compliance to a Recognised Standard.

4.4. Should an Applicant believe that its compliance with or certification under an existing Standard meets the requirements necessitated under this Schedule, the Applicant may present evidence of equivalent Standard to the Code Compliance Officer (e.g. Certification to ISO/IEC27001:2022 where the scope of the certification includes the Processing of Personal Data). The Code Compliance Officer will review the submitted evidence and evaluate the extent to which it conforms with the requirements of this Schedule.

Obligations on Applicants

4.5. Each Applicant shall:

(a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as its User Information Security Management System;

(b) ensure that its User Information Security Management System:

(i) provides for security controls which are proportionate to the potential impact of each part of its User Systems being Compromised, as determined by means of processes for the management of information risk; and

(ii) review its User Information Security Management System on at least an annual basis and make any changes to it following such a review in order to ensure that it remains fit for purpose

4.6. Each User Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:

(a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the User Systems, including measures relating to Data handling, retention and protection;

(b) the establishment and maintenance of an Information Classification Scheme in relation to the User Systems;

(c) the management of business continuity; and

(d) the education, training and awareness of User Personnel in relation to information security.

4.7. Each User Information Security Management System shall specify the approach of the user to:

(a) information security, including its arrangements to review that approach at planned intervals;

(b) human resources security;

(c) physical and environmental security; and

(d) ensuring that any person who provides services to the user for the purpose of ensuring that the user is able to comply with its obligations under this Code must establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the user.

4.8. Each User Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the Applicant to establish and maintain a register of the physical and information assets on which it relies for the purposes of complying with its obligations under this Code.

4.9. Each User Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:

(a) measures to restrict access to Data that is stored on or communicated by means of the User Systems to those who require such Data and are authorised to obtain it;

(b) procedures for granting, amending and removing authorisations in respect of access to such Data;

(c) measures to ensure that the activities of one individual may not become a means by which the User Systems are Compromised to a material extent;

(d) Measures to ensure that all access to the Smart Meter Data System is by unique user identifier; and

(e) Prohibit the sharing of access credentials.

4.10. Each User Information Security Management System shall incorporate procedures on the management of information Security Incidents including:

(a) provisions for reporting all Security Incidents involving a suspected or confirmed breach of confidentiality in respect of Data accessed from any Smart Meter Data System to the Code Compliance Officer;

(b) provisions for reporting all Security Incidents which could compromise the integrity of the Party's access control measures in relation to accessing Smart Meter Data Systems to the Code Compliance Officer; and

(c) provisions for reporting all such Security Incidents to the Code Compliance Officer within 8 hours of identification of the Security Incident. Where this identification occurs outside normal Working Hours, the 8 hours will commence from the start of the next Working Day.

Management of Data

4.11. Each Party and Other User shall:

(a) develop and maintain, and hold all Data in accordance with, a User Data Retention Policy; and

(b) when any Data held by it cease to be retained in accordance with the User Data Retention Policy, ensure that they are securely deleted in accordance with its Information Classification Scheme.

Party and Other User Systems Accessing Data by the API: Duties to Detect and Respond to Unauthorised Activities

4.12. Each Party and Other User shall:

(a) take reasonable steps to ensure that:

(i) its User Systems can identify any deviation from their expected configuration; and

(ii) any such identified deviation is rectified; and

(b) for these purposes always maintain an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of those User Systems.

4.13. Each Party and Other User shall take reasonable steps:

(a) to ensure that its User Systems can detect any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;

(b) if those User Systems detect any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

4.14. Each Party and Other User shall:

(a) ensure that its User Systems record all attempts to access resources, or Data held, on them;

(b) ensure that its User Systems detect any attempt by any person to access resources, or Data held, on them without possessing the authorisation required to do so; and

(c) take reasonable steps to ensure that its User Systems prevent any such attempt at unauthorised access.

Security Incident Management

4.15. Each Party and Other User shall, on the occurrence of a Major Security Incident in relation to its User Systems, ensure that the Code Compliance Officer and the Security Sub-Committee are promptly notified.

System Design and Operation

4.16. Each Party and Other User shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate its User Systems to protect them from being Compromised.

Management of Vulnerabilities

4.17. Each Party and Other User shall ensure that penetration tests that are designed to identify any vulnerability of its User Systems to Compromise are performed:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or Materially Changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

4.18. Each Party and Other User shall ensure that it carries out assessments that are designed to identify any vulnerability of its User Systems that access Data via the API to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or Materially Changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

Party and Other User Systems: Duty to Separate

4.19. Each Party and Other User shall take reasonable steps to ensure that any software or firmware that is installed on its User Systems for the purposes of security is Separated from any software or firmware that is installed on those Systems for any other purpose.

Obligations for Other Users

4.20. The obligations set out here under Clause 4 for data security for Other Users will be replicated and where necessary further specified in each Access Agreement, which shall include reference to this Schedule by incorporation and will be determined by the type and quantity of Data requested.

5 Additional Provisions

5.1. Each Party and Other User shall maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the Party and Other User to demonstrate its compliance with its obligations under this Schedule 5: Data Security.

5.2. Each Party and Other User shall complete an Annual Self-Assessment in accordance with Schedule 6: Assessments.

5.3. Each Applicant User shall cooperate with the Code Compliance Officer, including by providing the necessary evidence as requested the Code Compliance Officer, in the course of an Entry Assessment.

5.4. Each Party and Other User shall cooperate with the Code Compliance Officer, including by providing the necessary evidence as requested the Code Compliance Officer, in the course of an Ad-Hoc Assessment.

5.5. Each Party and Other User shall maintain technical and organisational measures, including working arrangements, in accordance with Good Industry Practice, as is necessary to demonstrate compliance with its respective obligations under this Schedule.

5.6. The Security Sub-Committee shall maintain a Security Controls Framework [to be developed] in accordance with Schedule 10: Security Sub-Committee, which shall establish examples of evidence for a Party and Other User to demonstrate procedures required under this Schedule, in accordance with Good Industry Practice.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 5: Data Privacy

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Schedule 5: Data Privacy

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD Mon YYYY		n.n

1 Definitions

Term	Acronym	Definition
Access Agreement		Means an Agreement by which an organisation that is not a Party can access the Smart Meter Data System.
Accession Agreement		Means an agreement by which a Party agrees to be bound by this Code, as set out in Schedule 3: Accession.
Access Log		Means a log of Third Parties' and users' access to Data, including Consumption Data, on the Smart Meter Data System, which includes: a) a timestamp of the time of access; b) the Data Items accessed; c) an identification of the Third Party or user accessing the Data; and d) the identification of the permission or other Legal Basis used by the Third Party to access the Data.
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or c) where a new User Category or Data Item is issued.
Annual Self-Assessment		Means a self-assessment questionnaire issued to all users on an annual basis to identify the

Term	Acronym	Definition
		extent to which, since the last occasion on which a Self-Assessment was carried out in respect of that Other User or Party, there has been any Material Change in the arrangements that the Other User has in place to comply with its obligations under the Code or in the quantity of Consumption Data being accessed by the Other User or Party.
Anonymous Data		Means Data which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
Applicant		Means any person who applies to be admitted as a Party, subject to and in accordance with the Code.
Basic Access		Means, in relation to an application for access under Schedule 2: Access Arrangements, a request by a user for access that involves access to existing Data Items assigned to that User Category.
Change of Legal Entity	CoLE	Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.

Term	Acronym	Definition
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code. Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.
Complex Access		Means, in relation to an application for access under Schedule 2: Access Arrangements, a request by a user for access that involves: a) Access to a new Data Item, and/or; b) Access to a Data Item not assigned to that User Category, and/or; c) Access to Data Items by a user within a new User Category.
Consent		Means, in respect of the Processing of Smart Meter Data on the Smart Meter Data System, that the Final Customer has provided a freely given, specific, explicit, informed and unambiguous indication of their wishes by which they, by a statement or clear affirmative action, signify agreement to the Processing of Smart Meter Data, and that such Consent has not been withdrawn.
Consumption Data		Means, in respect of a premises, the quantity of electricity or gas measured by the Smart Meter as having been supplied to the relevant premises.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).

Term	Acronym	Definition
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data Controller		Has the meaning as defined in Data Protection Legislation.
Data Processor		Has the meaning as defined in Data Protection Legislation.
Data Protection Commission	DPC	Means the commissioner as defined in the Data Protection Legislation.
Data Protection Impact Assessment	DPIA	Has the meaning as defined in Data Protection Legislation.
Data Protection Legislation		Means the GDPR and any other implementing legislation with the Republic of Ireland, including the Data Protection Act 2018, and, in each case, all regulations, statutes and instruments made thereunder as may be amended from time to time.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, as defined in Schedule 2: Access Arrangements.
Data Subject		Has the meaning as defined in Data Protection Legislation.
Data Subject Rights		Means the exercise of the rights of a natural person to their rights under Articles 15 to 22 of the General Data Protection Regulation, or otherwise as interpreted in Data Protection Legislation (where this takes precedence).
Distribution System Operator	DSO	Means the legal entity holding the Distribution System Operator Licence.

Term	Acronym	Definition
DPC Self-Assessment Checklist		Means a checklist to evidence compliance with Data Protection Legislation provided by the Data Protection Commissioner.
Electricity Supplier		Has the meaning as defined in the as defined in Statutory Instrument 426 of 2014.
Entry Assessment		Means an assessment conducted on all Applicants or user prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
European Economic Area	EEA	Has the meaning as defined in Data Protection Legislation.
Final Customer		Means a natural or legal person who receives, or wishes to receive, a supply of energy at any premises in the Republic of Ireland, in accordance with Statutory Instrument (SI) 37 of 2022.
Good Industry Practice		Means, in respect of a person, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced organisation engaged in a similar type of undertaking as that person under the same or similar circumstances, complying with all applicable laws, codes of professional conduct, relevant codes of practice, Irish, European and other relevant standards.
Legal Basis, Legal Bases		Has the meaning as defined in Data Protection Legislation.
Licence		The Licence granted by the Commission to the DSO / Electricity Suppliers under the Electricity Regulation Act, 1999.
Meter Point Reference Number	MPRN	Means, in respect of a Smart Meter System, the supply meter point

Term	Acronym	Definition
		reference number allocated by the relevant Party to the premises at which the supply of gas is recorded by that Smart Meter System.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Personal Data		Has the meaning as defined in the GDPR, as applicable to Data Processed on the Smart Meter Data System. This includes the Data Items marked as Personal Data within Appendix A: Data Glossary of the Code.
Personal Data Breach		Has the meaning as defined in Data Protection Legislation.
Privacy Controls Framework	PCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Privacy Statement		Has the meaning as defined in Data Protection Legislation.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Schedule		Means a Schedule to this Code.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Single Market Operator	SMO	Means the entity responsible for administering the market functions of the single electricity market (SEM).

Term	Acronym	Definition
Smart Meter Data		Has the meaning as defined in Statutory Instrument 37 of 2022. ***Potentially to be replaced by the definition in the final legislation***
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Smart Meter System		Means an electronic System that can measure energy consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication, as defined in Statutory Instrument 426 of 2014, and that connects to the Smart Meter Data System.
Sub-Processor, Sub-Processing		Has the meaning as defined in Data Protection Legislation.
System(s)		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith.
Testing Purposes		Means for the purposes of testing as set out in the Code Test Strategy.
Third Party		A natural or legal person that accesses or uses Data (including but not limited to Consumption Data) on behalf of a Party or Other User, without themselves being a Party or Other User.
Transmission System Operator	TSO	Means the legal entity responsible for conveying electricity on the high voltage electricity network (the 'Transmission System') and for the

Term	Acronym	Definition
		operation and development of that system.
Unaggregated Bulk Data		Data which has been broken down into segments or categories, and which is accessed or received in a single packet or set of records.
User Category		A Category of user as defined in Schedule 2: Access Arrangements.
User Personnel		Means those persons who are engaged by a user, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the business of the user in the exercise of rights and compliance with obligations under this Code.
Vulnerable Customer		Means as defined in 7.1 of the Code of Practice for Vulnerable Customers
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.
Working Hour		Means any hour between 09:00 and 17:00 on a Working Day.

2 General Provisions

2.1. The definitions and interpretations referred to in this Schedule apply as defined in Schedule 1: Interpretations.

2.2. This Schedule governs the Processing of Personal Data by Parties and Other Users entitled to Process Personal Data, including Consumption Data, in accordance with Schedule 2: Access Arrangements.

2.3. This Schedule only applies where a Party or Other User accesses Personal Data, including Unaggregated Bulk Data, on the Smart Meter Data System, unless otherwise indicated.

2.4. This Schedule also applies to Personal Data accessed on the Smart Meter Data System, and to subsequent Processing on other Systems, unless otherwise indicated.

2.5. Where a Party, Other User or Applicant requests access to Anonymous Data from the Smart Meter Data System, the Party, Other User or Applicant will not be required to comply with this Schedule, notwithstanding:

(a) its obligations under Schedule 4: Data Security; and

(b) the requirement for the Party, Other User or Applicant to follow the Basic Access or Complex Access process in Schedule 2: Access Arrangements to access such Data.

3 Obligations

3.1. The provisions of this Schedule and obligations imposed on Parties and Other Users are without prejudice to any other obligations they each may have under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Data Protection Act 2018, and any other Data Protection Legislation, including any such obligations they each may have concerning Processing of Personal Data.

4 Categories of Users

4.1. For the purposes of Processing, certain users will act as Data Controllers. In particular, this shall include the following categories of users:

(a) Parties to the Code;

(b) Data System Provider (DSP); and

(c) Other Users as specified in Schedule 2: Access Arrangements, who are subject to an Access Agreement and by incorporation, Schedules 4 and 5, but are not Parties to the Code.

4.2. For the purposes of Processing, certain Parties or Other Users will act as Data Processors, as defined in Schedule 2: Access Arrangements.

5 Applicability of Obligations

5.1. The applicability of this Clause will be the following:

(a) obligations on Parties will apply by virtue of their accession to the Code and signed Accession Agreement; and

(b) obligations on Other Users will apply by virtue of an Access Agreement signed in accordance with Schedule 2: Access Arrangements and will be specified in each Access Agreement.

6 Obligations on Data Controllers

6.1. Where a user is a Data Controller for the purposes of Personal Data Processed via the Smart Meter Data System, it undertakes that it shall comply with the obligations in Clause 6 before requesting (including Processing) Personal Data from the Smart Meter Data System.

6.2. Legal Basis (Parties): Where the Data Controller is a Party, the Data Controller shall ensure, before requesting Personal Data from the Smart Meter Data System, that:

(a) the Data Controller has collected Consent from the Final Customer, either directly or via a Third Party, at any time; or

(b) that the Data Controller is Processing the Personal Data from the Smart Meter Data System:

(i) as necessary for a legal obligation, including a Licence obligation, incumbent on the Data Controller, where the Data Controller is the Distribution System Operator (DSO), Transmission System Operator, Single Market Operator (SMO), or the relevant Electricity Supplier for the relevant Final Customer(s);

(ii) as necessary for the performance of a contract to which the Final Customer is a party, as specifically requested by the Final Customer, or in order to take steps at the request of the Final Customer prior to entering into a contract; or

(iii) as necessary in order to protect the vital interests of the Final Customer or another natural person;

(iv) as necessary for the proper performance of a public interest task carried out by an administrative body to whom the Data are disclosed;

(v) as necessary for the purposes of the legitimate interests pursued by the TSO or DSO or by a Third Party to whom the Data are disclosed, except where such interests are overridden by the interests and/or fundamental rights and freedoms of the Final Customer or another natural person;

(vi) for Testing Purposes;

(vii) for any other purpose as defined in Schedule 2: Access Arrangements, as approved by the Panel for a particular user or User Category.

Where the Data Controller has identified Consent as a Legal Basis for accessing Personal Data, it shall ensure such consent is collected in a form in accordance with Good Industry Practice, and shall retain logs and evidence of the receipt of the Consent, the type of Consent provided, when and how such Consent was provided, and whether it has been subsequently withdrawn.

6.3. Legal Basis (Other Users): Where the Data Controller is an Other User, the Data Controller shall ensure, before requesting Personal Data from the Smart Meter Data System, that:

(a) the Data Controller has collected Consent from the Final Customer, either directly or via a Third Party; or

(b) another purpose as defined in Schedule 2: Access Arrangements applies, as approved by the Panel for a particular user or User Category.

Where the Data Controller has identified Consent as a Legal Basis for accessing Personal Data, it shall ensure such consent is collected in a form in accordance with Good Industry Practice, and shall retain logs and evidence of the receipt of the Consent, the type of Consent provided, when and how such Consent was provided, and whether it has been subsequently withdrawn, in line with Good Industry Practice.

6.4. Transparency: The Data Controller shall ensure, before requesting Personal Data from the Smart Meter Data System, that:

(a) the Data Controller has provided information to the Final Customer around the use of Personal Data (either directly or via a Third Party), as required by Data Protection Legislation, which shall include, at a minimum, the following:

(i) the identity of the Data Controller, and any other Third Parties, with whom the Personal Data may be shared;

(ii) the purposes for which access to Personal Data is being sought, and for which it may subsequently be used;

(iii) the time periods in respect of which the Data Controller shall Process Personal Data from the Smart Meter Data System;

(iv) information for the Final Customer about their right to object or withdraw Consent (as the case may be) to the Data Controller obtaining or accessing their Personal Data on the Smart Meter Data System, and the process by which the Final Customer may object or withdraw Consent; and

(v) information for the Final Customer about their other rights under the Code, as well as any limitations to these rights in line with Data Protection Legislation;

(b) where the Data Controller is the Electricity Supplier or DSO for the Final Customer, it may provide the information specified in Clause 5.4(a) above to the Final Customer in the course of the provision of its services;

(c) Data Controllers shall ensure that, for the purposes of Clause 6, where the Final Customer or another natural person at Final Customer's relevant premises is a Vulnerable Customer, the Final Customer is provided with the information specified in Clause 6.4(a) in a manner tailored to the specific needs of the Final Customer; and

(d) the Data Controller shall Process Personal Data only for the purposes permitted to it under Schedule 2: Access Arrangements and the Data Access Register.

6.5. Technical and Organisational measures: The Data Controller shall maintain technical and organisational measures to process and implement the following:

(a) a Final Customer's request to withdraw Consent (as the case may be) to the Data Controller's access to Personal Data on the Smart Meter Data System, unless other Legal Bases apply;

(b) a Final Customer's Change of Legal Entity (as the case may be), including where this constitutes an action to withdraw their Consent to the Processing of Personal Data or to the Data Controller's access to Personal Data on the Smart Meter Data System;

(c) where the Data Controller ceases to provide services to the Final Customer, to cease the Processing of Personal Data, or the Data Controller's access to the Final Customer's Personal Data, on the Smart Meter Data System;

(d) to allow the verification of the identity of an individual purporting to be the Final Customer, in addition to verifying the link between their identity and the relevant premise or Meter Point Reference Number, before facilitating or complying with Data Subject Rights, in line with Good Industry Practice;

(e) to allow the verification of any authorisation granted by Final Customer to a representative (whether this is a guardian, power of attorney, Third Party), in line with Good Industry Practice; and

(f) where Personal Data is no longer needed for a purpose under this Code, or the Data Controller no longer has a Legal Basis for Processing the Personal Data, technical and organisational measures to allow the organisation to cease Processing Personal Data, and to delete Personal Data Processed from the Smart Meter Data System, in line with Good Industry Practice.

6.6. Data Retention: The Data Controller shall only access or Process Personal Data for the relevant time period in which it has the Final Customer's Consent, or as otherwise required in accordance with Clause 6.2.

6.7. Consumer rights (Access): Where the Data Controller receives a request from a Final Customer to whom it provides services, and the request involves a request to access Personal Data, the Data Controller shall provide such information to the Final Customer or otherwise direct the Final Customer to the procedure identified by the DSP as required to access such Data on the Smart Meter Data System.

6.8. Consumer Rights (Additional): Where the Data Controller receives a request from a Final Customer to whom it provides services, and the request involves a request in relation to their Data Subject Rights (other than the right to access Personal Data) or other rights under this Code, the Data Controller shall provide the Final Customer with information on how they may exercise their rights in relation to Personal Data under this Code, as well as any limitations to these rights in line with Data Protection Legislation, or otherwise direct the Final Customer to the procedure identified by the DSP as required to exercise such rights with respect to Personal Data on the Smart Meter Data System.

6.9. International Data Transfers: The Data Controller shall ensure that, with respect to any Personal Data Processed from the Smart Meter Data System, the Data Controller shall comply with limitations on any transfers of Personal Data to a third country or international organisation outside the EEA in accordance with Data Protection Legislation.

6.10. Responsibility for Third Parties: Where the Data Controller engages a Third Party, it shall ensure that it enters into a contract with the Third Party, which includes the requirements identified by Data Protection Legislation and shall include, at a minimum, provisions to:

(a) ensure that Personal Data are only Processed on the Smart Meter Data System, and/or subsequently Processed, on the documented instructions of the Data Controller, and in accordance with the Data Controller's Legal Basis under Clause 6.2 or 6.3, as applicable;

(b) ensure that the Third Party commits to only Processing Personal Data for the period specified by the Data Controller, and commits to cease access, delete or return the Personal Data (as the Data Controller requires) to the Data Controller, and delete all other copies of Personal Data, at the end of this period;

(c) ensure that the Third Party undertakes to only use other service providers in the course of Processing Personal Data as have been specifically communicated to, and/or approved by (as the case may be), the Data Controller;

(d) ensure that the Third Party commits to implementing technical and organisational measures to allow it to facilitate and ensure compliance with Final Customer rights under this Code;

(e) ensure that the Third Party commits to implementing appropriate technical and organisational measures to ensure the confidentiality, integrity and availability, of Personal Data;

(f) ensure that the Third Party commits to ensuring the storage and Processing of Personal Data within the European Economic Area, and/or commits to other limitations on any transfers of Personal Data to a third country or international organisation outside the European Economic Area in accordance with Data Protection Legislation;

(g) ensure that the Third Party commits to notifying the Data Controller without undue delay after becoming aware of a Personal Data Breach;

(h) ensure that the Third Party commits to retaining, and making available to the Data Controller on request, all information and records necessary to demonstrate its compliance with the obligations outlined in this Clause; and

(i) ensure that the Third Party commits to entering into a contract with any subsequent Third Party acting on its behalf that includes clauses containing the obligations equivalent to this Clause.

6.11. Notwithstanding the appointment or usage of a Third Party, the Data Controller will remain liable for compliance with its obligations under the Code.

6.12. Confidentiality: The Data Controller shall ensure that it shall only allow:

(a) authorised individuals (including staff) to Process Personal Data on or received from the Smart Meter Data System, and that such authorised individuals have committed themselves to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality, before Processing Personal Data; and

(b) authorised Systems to be used for Processing Personal Data and/or connecting to the Smart Meter Data System.

6.13. Notification of Personal Data Breaches: The Data Controller shall ensure that, where it becomes aware of a Personal Data Breach affecting Personal Data on, or received from, the Smart Meter Data System, that it notifies the Code Compliance Officer within 72 hours of the Data Controller's awareness of the Personal Data Breach. Where an incident occurs out of normal Working Hours, the 72 hours will commence from the start of the next Working Day.

6.14. Limitations on usage:

(a) the Data Controller shall ensure that it does not conduct any of the following activities using Personal Data accessed on the Smart Meter Data System:

(i) direct marketing to the Final Customer; and

(ii) profiling of a Final Customer, on the basis of Personal Data, including Consumption Data, accessed on the Smart Meter Data System; and

(b) the provisions of Clause 6.14(a) shall not apply to the extent that the Data Controller has received the Consent of the Final Customer for these specific Processing activities.

6.15. Good Industry Practice: The Data Controller shall maintain technical and organisational measures, including working arrangements, in accordance with Good Industry Practice, as is necessary to demonstrate compliance with its respective obligations under Clause 6.

7 Additional obligations on the Data System Provider

7.1. Where a Party is the DSP, with respect to Personal Data Processed both on the Smart Meter Data System and for the administration of users, it shall undertake such Processing as a Data Controller.

7.2. Where the Party is the DSP, it shall have the following additional obligations with respect to Personal Data.

7.3. Legal Basis: The DSP shall only Process Personal Data on the Smart Meter Data System for the following purposes:

(a) pursuant to a Licence obligation incumbent on the DSP; or

(b) for any other purpose as defined in the Schedule 2: Access Arrangements.

7.4. Transparency: The DSP shall ensure that it puts in place a Privacy Statement(s) for users of the Smart Meter Data System, including User Personnel and Final Customers, which should include the information specified by Data Protection Legislation, and at a minimum encompass the following:

(a) the identification of the DSP, and its contact details;

(b) information on the purposes of the Processing of Personal Data on the Smart Meter Data System by the DSP, as well as the applicable Legal Basis;

(c) information on the time periods in respect of which the DSP shall Process Personal Data from the Smart Meter Data System;

(d) information on the categories of users of the Smart Meter Data System who may have access to Personal Data, including Consumption Data, on the Smart Meter Data System;

(e) information on the categories of any other Third Parties and service providers (including Sub-Processors) involved in Processing Personal Data as part of the provision and delivery of the Smart Meter Data System;

(f) information on the purposes for which access to Personal Data Processed on the Smart Meter Data System may occur, including for the administration of users of the Smart Meter Data System, and for which it may subsequently be used;

(g) information for the Final Customer about their right to object or withdraw Consent (as the case may be) to Processing of their Personal Data on the Smart Meter Data System, and the process by which the Final Customer may object or withdraw Consent, if appropriate; and

(h) information for the Final Customer about their other rights under the Code or Data Protection Legislation, as well as any limitations to these rights in line with Data Protection Legislation.

7.5. User Personnel Rights: The following provisions apply to Personal Data Processed on the Smart Meter System, including for the purposes of the administration of User Personnel's Personal Data on the Smart Meter Data System, that:

(a) the DSP shall ensure that the Smart Meter Data System includes technical and organisational measures to allow User Personnel to access their individual Personal Data; and

(b) the DSP shall ensure that it maintains technical and organisational measures on the Smart Meter Data System to facilitate User Personnel's Data Subject Rights over their Personal Data.

7.6. Final Customer Rights: The following provisions apply to Personal Data of Final Customers, including Consumption Data, Processed on the Smart Meter Data System:

(a) the DSP shall ensure that the Smart Meter Data System includes technical and organisational measures to allow Final Customers to access their Personal Data, including Consumption Data and the Access Log; and

(b) the DSP shall ensure that it maintains technical and organisational measures on the Smart Meter Data System to facilitate Final Customers' other Data Subject Rights, in addition to other rights under this Code, over their Personal Data, including Consumption Data.

7.7. Data Retention: The following provisions apply to the DSP with respect to Personal Data Processed on the Smart Meter Data System:

(a) Processing of Personal Data on the Smart Meter Data System: The DSP shall ensure it shall only Process Personal Data for determined retention periods in line with the usage, including Processing, of such Data by users on the Smart Meter Data System.

(b) Processing for the purposes of the administration of users on the Smart Meter Data System: The DSP shall ensure that its shall only Process Personal Data for the purposes of the administration of users for determined retention periods.

(c) The DSP shall maintain a Data Retention Policy for the purposes of compliance with this Clause.

7.8. Confidentiality: The DSP shall ensure that it shall only allow:

(a) authorised individuals (including staff) to Process Personal Data on or received from the Smart Meter Data System, and that such authorised individuals have committed themselves to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality, before Processing Personal Data; and

(b) authorised Systems to be used for Processing Personal Data and/or connecting to the Smart Meter Data System.

7.9. Data breach notification: The DSP shall ensure that, where it becomes aware of a Personal Data Breach affecting Personal Data Processed on the Smart Meter Data System, that it notifies the Code Compliance Officer within 72 hours of the Data Controller's awareness of the Personal Data Breach. Where an incident occurs out of normal Working Hours, the 72 hours will commence from the start of the next Working Day.

7.10. International Data Transfers: The DSP shall ensure that:

(a) with respect to any Personal Data Processed on the Smart Meter Data System, such data is only stored using databases, platforms and other technology within the EEA; and

(b) notwithstanding Clause 7.10(a), with respect to any access provided to the Smart Meter Data System to any of its staff or Third Parties, including Data Processors outside the EEA, the DSP shall comply with any limitations for transfers of

Personal Data to a third country or international organisation outside the EEA, in accordance with Data Protection Legislation.

7.11. Service Provider Contracts: The DSP shall ensure that, where a service provider, including a Data Processor, is used, that it shall enter into a contract with the Third Party, which includes the requirements identified by Data Protection Legislation and shall include, at a minimum, provisions to:

(a) ensure that Personal Data are only Processed on the Smart Meter Data System, and/or subsequently Processed, on the documented instructions of the DSP, and in accordance with the Data Controller's Legal Basis under Clause 6.2;

(b) ensure that the service provider commits to only Processing Personal Data for the period specified by the DSP, and commits to cease to access, delete or return the Personal Data (as the DSP requires) to the DSP, and delete all other copies of Personal Data, at the end of this period;

(c) ensure that the service provider undertakes to only use other service providers (including Sub-Processors) in the course of Processing Personal Data as have been specifically communicated to, and/or approved by (as the case may be), the DSP;

(d) ensure that the service provider commits to implementing technical and organisational measures to allow it to facilitate and ensure compliance with Final Customer rights under this Code;

(e) ensure that the service provider commits to implementing appropriate technical and organisational measures to ensure the confidentiality, integrity and availability, of Personal Data;

(f) ensure that the service provider commits to ensuring the storage and Processing of Personal Data within the European Economic Area, and/or commits to other limitations on any transfers of Personal Data to a third country or international organisation outside the European Economic Area in accordance with Data Protection Legislation;

(g) ensure that the service provider commits to notifying the DSP without undue delay after becoming aware of a Personal Data Breach;

(h) ensure that the Third Party commits to retaining, and making available to the DSP on request, all information and records necessary to demonstrate its compliance with the obligations outlined in this Clause; and

(i) ensure that the Third Party commits to entering into a contract with any subsequent Third Party acting on its behalf that includes clauses containing the obligations equivalent to this Clause.

7.12. Good Industry Practice: The DSP shall maintain technical and organisational measures, including working arrangements, in accordance with Good Industry Practice, as is necessary to demonstrate compliance with its respective obligations under Clause 6.

8 Data Processor: Obligations on the Data Processor

8.1. Where a Party or Other User is a Data Processor for the purposes of Personal Data Processed via the Smart Meter Data System, it undertakes that it shall comply with the obligations in this Clause before requesting (including Processing) Personal Data from the Smart Meter Data System.

8.2. Legal Basis: The Data Processor shall ensure, before accessing, including Processing, Personal Data from the Smart Meter Data System, that:

(a) The Data Processor is Processing the Personal Data from the Smart Meter Data System as required for the provision of services to a Data Controller (Party or Other User).

(b) The Data Processor is Processing the Personal Data from the Smart Meter Data System as required for a purpose as defined in Schedule 2: Access Arrangements, where the appropriate Data Controller has been defined.

8.3. Data Retention: The Data Processor shall only access or Process Personal Data for the relevant time period for which it is authorised as specified in Clause 8.2, or otherwise authorised by the Data Controller to which it provides services (as the case may be).

8.4. Consumer rights: Where the Data Processor receives a request from a Final Customer in relation to their Data Subject Rights, or other rights under this Code, the Data Processor shall provide the Final Customer with information on how they may access and exercise their rights in relation to Personal Data on the Smart Meter Data System, including, as relevant:

(a) to the procedure identified by the Data Controller as required to access such rights over their Personal Data; and

(b) to the procedure identified by the DSP as required to exercise such rights on the Smart Meter Data System.

8.5. International Data Transfers: The Data Processor shall ensure that, with respect to any Personal Data Processed on the Smart Meter Data System, that the Data Processor shall ensure that:

(a) with respect to any Personal Data Processed from the Smart Meter Data System, such data is only stored using databases, platforms and other technology within the EEA; and

(b) notwithstanding Clause 7.10(a), with respect to any access provided by the Data Processor to any of its staff or Third Parties, including Sub-Processors, outside the EEA, the Data Processor shall:

(i) only do so with the Panel's approval; and

(ii) where providing access to staff or a Third Party located outside of the EEA, comply with any limitations for transfers of Personal Data to a third country or

international organisation outside the EEA, in accordance with Data Protection Legislation.

8.6. Responsibility for Third Parties: Where the Data Processor engages a Third Party, it shall enter into a contract with the Third Party, which includes, at a minimum, provisions to:

(a) ensure that it only allows access to Third Parties as required for a purpose for which it is authorised as specified in Clause 8.2 or otherwise required for the legal basis applicable to a Party or Other User to which it provides services;

(b) ensure that Personal Data are only Processed on the Smart Meter Data System, and/or subsequently Processed, on the documented instructions of the Data Processor and with the prior written authorisation of the Data Controller;

(c) ensure that the Third Party commits to only Processing Personal Data for the period specified by the Data Processor, and commits to cease access, delete or return the Personal Data (as the Data Controller requests) to the Data Processor, and delete all other copies of Personal Data, at the end of this period;

(d) ensure that the Third Party undertakes to only use other service providers in the course of Processing Personal Data as have been specifically communicated to, and/or approved by (as the case may be), the Data Processor and the Data Controller;

(e) ensure that the Third Party commits to implementing technical and organisational measures to allow it to facilitate and ensure the Data Controller's compliance with Final Customer rights under this Code;

(f) Ensure that the Third Party commits to implementing appropriate technical and organisational measures to ensure the confidentiality, integrity and availability, of Personal Data;

(g) ensure that the Third Party commits to ensuring the storage and Processing of Personal Data within the European Economic Area, and commits to other limitations on any transfers of Personal Data to a third country or international organisation outside the European Economic Area in accordance with Data Protection Legislation;

(h) ensure that the Third Party commits to notifying the Data Processor without undue delay after becoming aware of a Personal Data Breach;

(i) ensure that the Third Party commits to retaining, and making available to the Data Processor on request, all information and records necessary to demonstrate its compliance with the obligations outlined in this Clause; and

(j) ensure that the Third Party commits to entering into a contract with any subsequent Third Party acting on its behalf that includes clauses containing the obligations equivalent to this Clause.

8.7. Notwithstanding the appointment or usage of a Third Party, the Data Processor must notify the Data Controller and receive approval for any sub-Processing by Third Parties engaged by the Data Processor under 7.6(b).

8.8. Notwithstanding the appointment or usage of a Third Party, the Data Processor will remain liable for compliance with its obligations under the Code.

8.9. Confidentiality: The Data Processor shall ensure that it shall only allow:

(a) authorised individuals (including staff) to Process Personal Data on or received from the Smart Meter Data System, and that such authorised individuals have committed themselves to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality, before Processing Personal Data; and

(b) authorised Systems to be used for Processing Personal Data and/or connecting to the Smart Meter Data System.

8.10. Notification of Personal Data Breaches: The Data Processor shall ensure that, where it becomes aware of a Personal Data Breach affecting Personal Data on, or received from, the Smart Meter Data System, that it notifies the Code Compliance Officer within 72 hours of the Data Processor's awareness of the Personal Data Breach, in addition to notifying the Data Controller under procedures agreed with the Data Controller. Where an incident occurs out of normal Working Hours, the 72 hours will commence from the start of the next Working Day.

8.11. Limitations on usage: The Data Processor shall ensure that it does not conduct any of the following activities using Personal Data accessed on the Smart Meter Data System:

(a) direct marketing to the Final Customer; and

(b) profiling of a Final Customer, on the basis of Personal Data, including Consumption Data, accessed on the Smart Meter Data System.

8.12. Good Industry Practice: The Data Processor shall maintain technical and organisational measures, including working arrangements, in accordance with Good Industry Practice, as is necessary to demonstrate compliance with its respective obligations under Clause 8.

8.13. Responsibility for obligations: The provisions of Clause 8 shall apply regardless of whether or not the Data Processor is appointed as a Third Party for any of the Parties or Other Users.

9 Assessments

9.1. Each Applicant shall submit the following information to the Code Compliance Officer, in accordance with its Entry Assessment under Schedule 6: Assessments:

(a) its internal data protection risk assessment, including as a minimum details of internal policies and procedures in place to mitigate data protection risks

associated with obligations under this Code (such as a Data Retention Policy, completed Data Protection Impact Assessments, completed legitimate interest assessments, Privacy Statements provided to Final Customers, terms and conditions provided to Final Customers, and other documents to be identified by the Privacy Controls Framework);

(b) information on whether it has suffered any Personal Data Breaches or it has been subject to any Personal Data Breaches reportable to the DPC (and, if so, the nature of such incidents);

(c) evidence of any arrangements with any Third Parties that contain the clauses referred to in Clauses 6.10, 7.11 or 8.6, as applicable;

(d) evidence of the collection of Consent from Final Customers, as applicable;

(e) information on the Legal Bases on which it relies to Process, or otherwise access, Personal Data from the Smart Meter Data System;

(f) evidence that it has completed an up-to-date and relevant DPC Self-Assessment Checklist, available through the DPC's website, including through providing a completed copy of this completed checklist and evidence of the implementation of the controls it identifies as being met; and

(g) evidence that it has appropriate technical and organisational data protection controls reflective of the risks applicable to its organisation.

9.2. Each user shall maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the user to demonstrate its compliance with its obligations under this Schedule 5: Data Privacy.

9.3. Each user shall complete an Annual Self-Assessment in accordance with Schedule 6: Assessments.

9.4. Each Applicant shall cooperate with the Code Compliance Officer, including by providing the necessary evidence as requested the Code Compliance Officer, in the course of an Entry Assessment.

9.5. Each user shall cooperate with the Code Compliance Officer, including by providing the necessary evidence as requested the Code Compliance Officer, in the course of an Ad-Hoc Assessment.

10 Additional Provisions

10.1. The Code Manager shall ensure that the Data Access Register contains a record of the purposes and Legal Basis that users and Third Parties that are entitled to access Data, including Consumption Data, in accordance with Schedule 2: Access Arrangements.

10.2. The Security Sub-Committee shall maintain a Privacy Controls Framework [to be developed] in accordance with Schedule 10: Security Sub-Committee, which shall

establish examples of evidence for a user to demonstrate procedures required under Schedule 5: Data Privacy, in accordance with Good Industry Practice.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 6: Assessments

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Schedule 6: Assessments

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD Mon YYYY		n.n

1 Definitions

Term	Acronym	Definition
Access Agreement		Means an Agreement by which an organisation that is not a Party can access the Smart Meter Data System.
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or c) where a new User Category or Data Item is issued.
Annual Self-Assessment		Means a self-assessment questionnaire issued to all users on an annual basis to identify the extent to which, since the last occasion on which a Self-Assessment was carried out in respect of that Other User or Party, there has been any Material Change in the arrangements that the Other User has in place to comply with its obligations under the Code or in the quantity of Consumption Data being accessed by the Other User or Party.
Applicant		Means any person who applies to be admitted as a Party, subject to and in accordance with the Code.
Assessment Report		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.

Term	Acronym	Definition
Assessment Response		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.
Assurance Status		Has the meaning given to that expression in Clause 3.9 of Schedule 6: Assessments.
Assurance Strategy		Has the meaning given to that expression in Clause 7.8 of the Main Body.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code.
Consumption Data		Means, in respect of a premises, the quantity of electricity or gas measured by the Smart Meter as having been supplied to the relevant premises.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Data Item		Means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for which are defined and controlled in the Data Access Register.

Term	Acronym	Definition
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, as defined in Schedule 2: Access Arrangements.
Entry Assessment		Means an assessment conducted on all Applicants prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
Event of Breach		Has the meaning given to that expression in Clause 21 of the Main Body.
Legal Basis, Legal Bases		Has the meaning as defined in Data Protection Legislation.
Material Change, Materially Changed		Means a change to a Party's Systems or processes which is of such a type or magnitude as to raise the reasonable expectation of an impact on that Party's ability to meet its obligations under this Code.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.

Term	Acronym	Definition
Personal Data Breach		Has the meaning as defined in Data Protection Legislation.
Privacy Controls Framework	PCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Remedial Plan		Means a document describing how a failure to comply with this Code will be remedied by the Party or Other User in question, and how the risk of future failures is to be mitigated.
Schedule		Means a Schedule to this Code.
Security Controls Framework	SCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Security Incident		Means an actual or potential impact on the confidentiality, integrity or availability of Smart Meter Data or a System.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Smart Meter Data		Has the meaning as defined in Statutory Instrument 37 of 2022. ***Potentially to be replaced by the definition in the final legislation***
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time in accordance with Schedule 9: Panel.
System(s)		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise

Term	Acronym	Definition
		processing electronic communications, including all hardware, software, firmware and Data associated therewith.
User Category		A Category of user as defined in Schedule 2: Access Arrangements.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.

2 Introduction

2.1. This Schedule sets out the process by which entities under the Code will be subject to assessments performed by the Code Compliance Officer.

2.2. This includes:

(a) The process for conducting Entry Assessments, Annual Self-Assessments and Ad-Hoc Assessments on Parties, Other Users and the DSP;

(b) The process for conducting performance assessments on the DSP and Code Manager, as appropriate, and;

(c) The process for approving and agreeing Remedial Plans and mitigating actions with respect to relevant entities under the Code.

2.3. This Schedule must be read in conjunction with Clause 6, Clause 7 and Clause 12 of the Main Body, Schedule 2: Access Arrangements, Schedule 4: Data Security, and Schedule 5: Data Privacy and Schedule 9: Change Management.

3 Entry Assessment

3.1. In order to become a user of the Smart Meter Data System, and receive access to Smart Meter Data, a Party or Other User ('Applicant') must first successful complete an Entry Assessment in accordance with Clause 7 of the Main Body.

3.2. The Entry Assessment shall be carried out by the Code Compliance Officer on receipt of a request from the Code Manager in accordance with the procedure specified in Clause 7 of the Main Body.

3.3. During the course of the Entry Assessment, the Applicant shall provide the information

specified in Clause 4.2 of Schedule 4: Data Security and Clause 9.1 of Schedule 5: Data Privacy.

3.4. The Code Compliance Officer shall use such information to complete an objective assessment of the Applicant's ability to manage data security and data protection risks and achieve compliance with Schedule 4: Data Security and Schedule 5: Data Privacy. The Code Compliance Officer shall conduct a review of:

(a) the information specified in Clause 4.2 of Schedule 4: Data Security and Clause 9.1 of Schedule 5: Data Privacy; and

(b) any other information specified as evidence in the Privacy Controls Framework or Security Controls Framework to demonstrate procedures required under Schedule 4: Data Security and Schedule 5: Data Privacy.

3.5. Following completion of its assessment, the Code Compliance Officer shall produce a report ('Assessment Report') setting out its conclusions and recommendations. The Code Compliance Officer shall provide this report to the Applicant who will be asked to agree or comment on the conclusions and recommendations in a response document ('Assessment Response'), as soon as reasonably practicable, and in any event by no later than such date as the Code Compliance Officer may specify.

3.6. Where the Code Compliance Officer identifies deficiencies with an Applicant's compliance as identified in its Assessment Report, the Code Compliance Officer shall liaise with the Applicant in relation to which mitigating actions are required in order for it to demonstrate appropriate data security and data privacy controls to meet the requirements of Schedules 4 and 5, under the Entry Assessment process. The Applicant shall commit to these controls in its Assessment Response.

3.7. If the Code Compliance Officer does not gain the necessary level of assurance that the Applicant's information security and data protection arrangements are sufficiently robust, this will be communicated to the Applicant. It shall be responsibility of the Applicant to propose and carry out mitigating actions to resolve the issues identified by the Code Compliance Officer.

3.8. Following the Applicant's completion of, or commitment to, mitigating actions to the satisfaction of the Code Compliance Officer, the Code Compliance Officer shall provide its updated Assessment Report to the Security Sub-Committee, detailing its findings and the mitigating actions (if any) conducted or committed to by the Applicant.

3.9. Following the receipt of the Assessment Report and Assessment Response, the Security Sub-Committee shall promptly consider the Assessment Report and (having regard to any advice of the Code Compliance Officer) set the Assurance Status of the Applicant, in relation to its compliance with each of its obligations under Schedules 4 and 5.

3.10. The Security Sub-Committee shall set the Assurance Status of the Applicant as one of the following:

(a) Approved;

(b) Approved, subject to the Applicant taking mitigating actions proposed in the Assessment Report or both taking such steps and being subject to an Ad-Hoc Assessment by such date that the Sub-Committee may specify; or

(c) Deferred; and

(i) The Applicant having first taken such steps as it proposed to take in its Entry Assessment Response; and

(ii) The Sub-Committee, having determined that it is satisfied on the evidence of the Ad-Hoc Assessment; that such steps have been taken.

4 Ad-Hoc Assessment

4.1. The Panel reserves the right to subject any Party or Other User or the DSP to an Ad-Hoc Assessment where proposed by the Code Compliance Officer.

4.2. Following a report from the Code Compliance Officer of a Security Incident, including a Personal Data Breach, the Panel will determine whether this warrants an additional Ad-Hoc Assessment under the Assurance Strategy referred to in Clause 7.8 of the Main Body.

4.3. The Panel may approve the Code Compliance Officer to undertake an Ad-Hoc Assessment where the following occurs:

(a) A change in security, privacy or compliance risks with respect to a particular Party or Other User or the DSP is identified by the Panel;

(b) Following a Security Incident with respect to a particular Party or Other User or the DSP;

(c) Event of Breach has occurred with respect to a particular Party or Other User or the DSP;

(d) a Party or Other User requests to be placed within a new User Category or requests access to a new Data Item to which it did not previously have access;

(e) a Party or Other User requests an amendment to their Access Agreement;

(f) a Party is expelled or withdraws from the Code in accordance with Schedule 8: Party Exit;

(g) an Other User's Access Agreement is terminated in accordance with Schedule 8: Party Exit.

4.4. The Code Compliance Officer shall use such information to complete an objective assessment of the Party or Other User's (or the DSP's) ability to manage data security

and data protection risks and achieve compliance with Schedule 4: Data Security and Schedule 5: Data Privacy. The Code Compliance Officer shall conduct a review of:

(a) the information specified in Clause 4.2 of Schedule 4: Data Security and Clause 9.1 of Schedule 5: Data Privacy;

(b) any other information specified as evidence in the Privacy Controls Framework or Security Controls Framework to demonstrate procedures required under Schedule 4: Data Security and Schedule 5: Data Privacy;

(c) sample checks on the Party or Other User's (or the DSP's) Processing of Smart Meter Data.

4.5. Following completion of its assessment, the Code Compliance Officer shall produce a report setting out its conclusions and recommendations. The Code Compliance Officer shall provide this report to the Party or Other User or the DSP who will be asked to agree or comment on the conclusions and recommendations in its Assessment Response, as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify.

4.6. If the Code Compliance Officer does not gain the necessary level of assurance that the Party or Other User's (or the DSP's) information security and data protection arrangements are sufficiently robust, this will be communicated to the Party or Other User or the DSP. It shall be responsibility of the Party or Other User to propose and carry out mitigating actions to resolve the issues identified by the Code Compliance Officer.

4.7. Where the Code Compliance Officer identifies deficiencies with a Party or Other User's (or the DSP's) compliance as identified in its Assessment Report, the Code Compliance Officer shall liaise with the Party or Other User (or the DSP) in relation to which mitigating actions are required in order for it to demonstrate appropriate data security and data privacy controls to meet the requirements of Schedules 4 and 5, under the Entry Assessment process.

4.8. In its Assessment Response, which should be provided to the Security Sub-Committee, the Party or Other User (or the DSP) should:

(a) Indicate whether the Party or Other User or the DSP accepts the relevant findings of the Code Compliance Officer;

(b) provide an explanation of the actual or potential non-compliance that has been identified;

(c) outline any mitigating actions that the Party or Other User or the DSP proposes to take in order to remedy and/or mitigate the actual or potential non-compliance; and

(d) identify a timetable within which the Party or Other User or the DSP proposes to take those steps.

4.9. Following the completion of the Assessment Response, the Code Compliance Officer shall be responsible for providing the Assessment Response and its Assessment Report to the Security Sub-Committee.

4.10. Following the receipt by it of the Assessment Report and Assessment Response, the Security Sub-Committee shall promptly consider both documents and (having regard to any advice of the Code Compliance Officer) set the Assurance Status of the Party or Other User or the DSP, in relation to its compliance with each of its obligations under Schedule 4: Data Security and Schedule 5: Data Privacy.

4.11. The Sub-Committee shall set the Assurance Status of the Party or Other User as one of the following:

(a) Approved;

(b) Approved, subject to the Party or Other User or the DSP taking steps it proposes to take in its Assessment Response; or both taking such steps and being subject to an Ad-Hoc Assessment by such date that the Sub-Committee may specify.

(c) Deferred; and

(i) The Party or Other User or the DSP having first taken such mitigating actions as it proposes to take in its Assessment Response or Remedial Plan; or

(ii) The Sub-Committee having determined that it is satisfied, on the evidence of the Ad-Hoc Assessment; that such steps have been taken; or

(d) Rejected; and

(i) The Party or Other User or the DSP shall have an Ad-Hoc Assessment to address any issues identified by the Code Compliance Officer and not adequately addressed in the response submitted to the Security Sub-Committee.

4.12. The Security Sub-Committee shall, to the extent to which it considers appropriate, in relation to a Party or Other User or the DSP which has produced an Assessment Response that sets out any steps that it proposes to take to:

(a) liaise with the Party or Other User or the DSP as to the nature and timetable of such steps;

(b) either accept the proposal to take those steps within that timetable or seek to agree with the Party or Other User or the DSP such alternative steps or timetable as the Security Sub-Committee may consider appropriate; and

(c) take advice from the Code Compliance Officer.

4.13. On the request of the Security Sub-Committee, the Code Compliance Officer will formulate the mitigating actions identified into a Remedial Plan for the Party or Other

User or the DSP to complete. The arrangements in the Remedial Plan shall be subject to the approval of the Security Sub-Committee.

4.14. Where a Remedial Plan requires any mitigating actions to be conducted by the Party or Other User or the DSP, the Party or Other User or the DSP shall report to the Security Sub-Committee on:

(a) taking the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be);

(b) on completion of those steps in accordance with the agreed timetable; and

(c) on any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

5 Annual Self-Assessment

5.1. All Parties, Other Users, and the DSP, shall be required to complete an annual Data Security and Data Privacy Assessment (Annual Self-Assessment). The scope of this assessment will be based on the User Category or if the DSP, with details provided within the Assurance Strategy.

5.2. Where in accordance with the requirements of the Code, a Party or Other User or the DSP is subject to an Annual Self-Assessment in any year, the Party or Other User or the DSP shall:

(a) carry out the Annual Self-Assessment during in accordance with the Annual Self-Assessment form; and

(b) ensure the Annual Self-Assessment is documented and is submitted to the Code Compliance Officer for review by no later than the date which is 12 months after the date of the completion of the previous Entry Assessment or (if more recent) Annual Self-Assessment.

5.3. The Annual Self-Assessment will require each Party or Other User, and the DSP, to:

(a) self-certify (based on reasonable enquiry) that it continues to meet the requirements to be a Party to the Code or under its Access Agreement, and to access the Smart Meter Data System since the last year in its annual Data Security and Data Privacy Assessment or Entry Assessment was conducted;

(b) document any changes to standards, Systems or processes that may impact the security or integrity of any Data that the Party or Other User or the DSP has made since submission of its last assessment, or that it plans to make in the next 12 months; and

(c) self-certify (based on reasonable enquiry) the categorisation of risk associated with any and all such changes.

5.4. For the purposes of Clause 5.3, the Code Compliance Officer shall develop and maintain an Annual Self-Assessment form, which shall be approved by the Security Sub-Committee.

5.5. The Code Compliance Officer shall review the assessment shall be carried out by a User within 10 Working Days of its receipt, to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that Party or Other User.

5.6. Where the Code Compliance Officer identifies deficiencies with a Party or Other User's (or the DSP's) compliance as identified in its Annual Self-Assessment, the Code Compliance Officer shall liaise with the Party or Other User or the DSP in relation to which mitigating actions are required in order for it to demonstrate appropriate data security and data privacy controls to meet the requirements of Schedules 4 and 5.

5.7. Following its review, the Code Compliance Officer shall produce a Self-Assessment Report considering the Party or Other User's (or the DSP's) ability to manage data security and data protection risks and achieve compliance with Schedule 4: Data Security and Schedule 5: Data Privacy and submit the Self-Assessment Report to the Security Sub-Committee.

5.8. Following the receipt of the Self-Assessment Report, the Security Sub-Committee shall promptly consider it and (having regard to any advice of the Code Compliance Officer) and set the Assurance Status of the Party or Other User or DSP, in relation to its compliance with each of its obligations under Schedule 4 or Schedule 5.

5.9. The Sub-Committee shall set the Assurance Status of the Party, Other User or the DSP as one of the following:

(a) Approved;

(b) Deferred; or

(c) the Party or Other User or the DSP shall have an Ad-Hoc Assessment to address any issues identified by the Code Compliance Officer.

6 Assessment of the Code Manager

6.1. In accordance with Clause 7.10 of the Main Body, the Panel may subject the Code Manager to an assessment of the performance of its responsibilities under the Code, including as set out in Clause 10 of the Main Body.

6.2. The Code Compliance Officer shall outline the circumstances in which such an assessment may be conducted in its Assurance Strategy, which shall be approved by the Panel.

6.3. Where it undertakes such an assessment, the Code Compliance Officer shall produce an Assessment Report.

6.4. The Code Manager shall do all such things as may be reasonably requested by the Panel or the Code Compliance Officer, for the purposes of facilitating an assessment of the Code Manager's compliance with its obligations under the Code.

6.5. Following the receipt of the Assessment Report, the Panel shall promptly consider it and (having regard to any advice of the Code Compliance Officer) identify if any mitigating actions are needed, and shall agree these actions with the Code Manager and/or Code Compliance Officer, as appropriate.

7 Assessment of the DSP

7.1. In accordance with Clause 7.10 of the Main Body, the Panel may subject the DSP to an assessment of the performance of its responsibilities under the Code, including as set out in Clause 12 of the Main Body.

7.2. The Code Compliance Officer shall outline the circumstances in which such an assessment may be conducted in its Assurance Strategy, which shall be approved by the Panel.

7.3. Where it undertakes such an assessment, the Code Compliance Officer shall produce an Assessment Report.

7.4. The DSP shall do all such things as may be reasonably requested by the Panel or the Code Compliance Officer, for the purposes of facilitating an assessment of the DSP's compliance with its obligations under the Code.

7.5. Following the receipt of the Assessment Report, the Panel shall promptly consider it and (having regard to any advice of the Code Compliance Officer) identify if any mitigating actions are needed, and shall agree these actions with the DSP and/or the Code Compliance Officer, as appropriate.

8 Miscellaneous

8.1. Each Party or Other User shall do all such things as may be reasonably requested by the Security Sub-Committee or the Code Compliance Officer, for the purposes of facilitating an assessment of that Party or Other User's compliance with its obligations under Schedule 4 or 5 or any Remedial Plan.

8.2. A Party or Other User shall provide the Code Compliance Officer, at its request, with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of that Party or Other User as are used for, and such persons engaged by that Party or Other User to carry out or are authorised to carry out, any activities related to its compliance with its obligations under Schedules 4 and 5; and

(ii) such cooperation as may reasonably be requested by the Code Compliance Officer carrying out such an assessment in accordance with this Schedule.

8.3. Where a Party disagrees with any decision made by the Security Sub-Committee in relation to its Assurance Status, it may appeal that decision to the Panel and the determination of the Panel shall be final and binding for the purposes of the Code.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 7: Panel

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Schedule 7: Panel

Version 0.1

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD-Mon-YY		n.n

1 Definitions

Term	Acronym	Definition
Alternate		Means another natural person who may be appointed by a Panel Member or the Panel Chair to act as their alternate.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code. Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.
Code Website		Means the dedicated website established by the Code Manager for the purposes of this Code.
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Competition and Consumer Protection Commission		Means the Competition and Consumer Protection Commission within the Republic of Ireland
Data Protection Commission	DPC	Means the commissioner as defined in the Data Protection Legislation.
Data Systems Operator	DSP	Means the legal entity responsible for the maintenance and

Term	Acronym	Definition
		administration of the Smart Meter Data System, as defined in Schedule 2: Access Arrangements.
Department		Means the Department of the Environment, Climate and Communications within the Republic of Ireland.
Deputy Chair		Shall have the meaning as per Clause 3.2.
Distribution Systems Operator	DSO	Means the legal entity holding the Distribution System Operator Licence.
Elected Member		Has the meaning given to that expression in Clause 1.1 of Annex 1.
Electricity Supplier		Has the meaning as defined in the as defined in Statutory Instrument 426 of 2014.
Electricity Supplier Party		Means a Party that is an Electricity Supplier.
Extraordinary Panel Meeting		Any meeting of the Panel that meets to discuss any business it deems urgent and can be convened on such notice (but in any event not less than one hour's notice) as the Panel Chair considers appropriate, and such that, where practicable within the time available, as many Panel Members as possible may attend but subject to the quoracy provisions of Clause 5.4.
Interim Election		Means the process that applies in respect of a Panel Member being removed from office in accordance with Clause 1.1 of Annex 1.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.

Term	Acronym	Definition
Panel Chair		Has the meaning given to that expression in Clause 3.1.
Panel Chair Appointee		Shall have the meaning as per Clause 3.8.
Panel Meeting		Shall have a meaning as per Clause 5.1 to 5.3.
Panel Member(s)		Has the meaning given to that expression in Clause 8.8 of the Main Body.
Panel Proceedings		Shall have the meaning as per Clause 5.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Framework Agreement) and that has not ceased to be bound by the Code.
Party Category		Means one of the following categories of Party: (a) the DSO; (b) Electricity Suppliers; (c) the TSO; and (d) the SMO.
Related Persons		Means, in relation to an individual: a) any member of that individual's immediate family (including parent, partner and children); b) any person in partnership with that individual or a member of that individual's immediate family; c) any employer of that individual or a member of the individual's immediate family; d) any Affiliate or related undertaking of such employer; and e) any related undertaking of that individual or a member of that individual's immediate family.

Term	Acronym	Definition
Scheduled Election		Means an Election that occurs in accordance with the process described in Clause 4.4.
Secretariat		Means the allocated role to perform those tasks and functions expressly ascribed to it under the Code and any other tasks and functions as the Panel may assign to the Secretariat from time to time.
Single Market Operator	SMO	Means the entity responsible for administering the market functions of the single electricity market (SEM).
Smart Meter Data Access Arrangements		Means such arrangements (including all necessary systems, contracts, processes, procedures, resources, products, and facilities) required to establish, procure, or otherwise have in place under or pursuant to the Code in connection with the provision of services, whether on behalf of or to Parties or otherwise.
Transmission Systems Operator	TSO	Means the legal entity responsible for conveying electricity on the high voltage electricity network (the 'Transmission System') and for the operation and development of that system.
Voting Group		Means, in respect of each Party Category with a right to vote, each Party that falls into that Party Category collectively with that Party's Affiliates (if any) who also fall into that Party Category.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.

2 Introduction

2.1. This Schedule sets out the requirements and processes for:

(a) the appointment of Panel Members;

(b) vacation of Panel Members; and

(c) the Panel Proceedings.

3 Panel Appointments

Panel Chair

3.1. The Commission shall appoint the Panel Chair in accordance with such process as the Commission may determine, as modified from time to time by the Commission; provided that such process as modified must be designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party, Other User or class of Parties or Other Users;

(b) the Panel Chair is appointed for a three-year term (following which they can be reappointed);

(c) the Panel Chair is remunerated at a rate to be determined by the Commission;

(d) the Panel Chair's appointment is subject to Clause 3: Panel Appointments and terms equivalent to those set out in Clauses 4: Vacation of Panel Members; and

(e) provision is made for the Panel Chair to continue in office for a reasonable period following the end of their term of office in the event of any delay in appointing their successor.

3.2. The Panel Chair shall preside at every meeting of the Panel. If the Panel Chair is unable to be (or is not) present at a meeting, a person selected by a simple majority of the attending Panel Members shall act as the Panel Chair for that meeting (Deputy Chair).

Electricity Supplier Member(s)

3.3. There shall be two (2) Electricity Supplier Members elected in accordance with Annex 1, below.

Distribution Systems Operator Member

3.4. The Distribution Systems Operator (DSO) Member shall be one person nominated by the DSO by notice to the Code Manager, who shall not be the Data Systems Provider (DSP) Member. The DSO may replace such person from time to time by prior notice to the Code Manager.

Transmission Systems Operator Member

3.5. The Transmission Systems Operator (TSO) Member shall be one person nominated by

the TSO by notice to the Code Manager. The TSO may replace such person from time to time by prior notice to the Code Manager.

Single Market Operator Member

3.6. The Single Market Operator (SMO) Member shall be one person nominated by the SMO by notice to the Code Manager. The SMO may replace such person from time to time by prior notice to the Code Manager.

Data Systems Provider Member

3.7. The DSP Member shall be one person nominated by the DSP by notice to the Code Manager, who shall not be the DSO Member. The DSP may replace such person from time to time by prior notice to the Code Manager.

Panel Chair Appointee

3.8. Where at any time:

(a) no person is currently appointed as a Panel Member pursuant to this Clause; and

(b) the Panel Chair (having consulted with the other Panel Members) considers that there is a class or category of person having an interest in the Smart Meter Data Access Arrangements whose interests are not adequately represented in the composition of the Panel at that time, and whose interests would be better represented if a particular person were appointed as an additional Panel Member,

The Panel Chair may (having consulted with the other Panel Members) appoint that particular person as a Panel Member by notice to the Code Manager. The Panel Chair may (having consulted with the other Panel Members), at any time thereafter by notice to the Code Manager, remove that person from the office of Panel Member.

4 Vacation of Panel Members

4.1. Each Panel Member may resign their office by 10 Working Days' notice in writing to the Panel.

4.2. Each Panel Member nominated by or elected in respect of Electricity Suppliers shall be appointed for a maximum term of two years.

4.3. Each Panel Member:

(a) may be removed from office by a Panel decision if they fail to attend (either in person or via their Alternate) two consecutive Panel meetings without good reason;

(b) for Electricity Supplier members, shall be removed from office as the result of a vote of no-confidence by Electricity Supplier Parties, which shall require the support of at least 75% of the Electricity Supplier Parties who cast a vote, on the

basis that each Electricity Supplier Party gets one vote (such vote to be organised by the Code Manager where requested by an Electricity Supplier Party);

(c) shall be removed from office where so directed by the Commission; and

(d) shall automatically be removed from office if they are unable to discharge their duties.

4.4. Subject to earlier removal from office of a Panel Member in accordance with Clauses 4.3, and without prejudice to their ability to stand for re-election, each Elected Member shall retire (at which point their office shall become vacant).

5 Panel Proceedings

Meetings

5.1. The Panel shall hold meetings at such times as it may decide or the Panel Chair may direct, but in any event shall meet when necessary to meet its responsibilities under the Code.

5.2. Each meeting of the Panel shall be convened by the Code Manager on at least 5 Working Days' notice (or such shorter period as the Panel Chair may approve).

5.3. Each Panel meeting shall be held at the venue and/or via the electronic means determined by the Panel from time to time.

Voting and Quorum

5.4. The quorum for a Panel meeting shall be 50% of the total number of Panel Members but excluding from such number any and all who have been excluded from the meeting by the Panel Chair due to a conflict of interest.

5.5. Should a quorum not be achieved in accordance Clause 5.4, or where the Panel Chair is not present and a Deputy Chair has not been agreed in accordance with Clause 3.2, the Panel Meeting shall not proceed and its business deferred until the next scheduled meeting or an Extraordinary Panel Meeting as determined by the Panel Chair.

5.6. Subject to Clause 5.8, each Panel Member shall be entitled to attend, and to speak and vote at, every meeting of the Panel.

5.7. Each decision of the Panel shall be by simple majority of those Panel Members attending the relevant meeting.

5.8. The Panel Chair shall not cast a vote as a Panel Member but shall have a casting vote on any matter where votes are otherwise cast equally in favour of and against the relevant motion, provided that where any person other than the Panel Chair is chair of a Panel Meeting they shall not have a casting vote.

5.9. A resolution in writing signed by or on behalf of all the Panel Members shall be as valid and effective as if it had been passed at a meeting of the Panel duly convened and held. Such a resolution may be signed in any number of counterparts.

Meeting Notice and Papers

5.10. Each meeting that the Panel determines, or the Panel Chair directs, is to be held shall be convened by the Code Manager. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Panel may approve). Such notice must be given to:

(a) the Panel Members (and any appointed Alternates);

(b) each of the persons referred to in Clauses 3 and 5.17;

(c) the Parties; and

(d) any other person that the Panel determines, or the Panel Chair directs, should be invited to the meeting.

5.11. The notice of each Panel meeting shall contain or be accompanied by the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and supporting papers.

5.12. The accidental omission to give notice of a meeting to, or the non-receipt of notice of a Panel meeting by, a person entitled to receive notice shall not invalidate the proceedings of that meeting.

5.13. Any Party shall be entitled to send a representative to attend a Panel Meeting provided that Party gives the Code Manager at least 3 Working Days' notice in advance of such meeting (or such shorter period of notice as the Panel Chair may approve). Such a representative shall be entitled to attend and (at the Panel Chair's invitation) speak at (but in no circumstances vote at) the meeting.

5.14. The Panel Chair may (at their discretion on grounds of confidentiality) exclude from any part of a Panel Meeting persons admitted pursuant to Clauses 5.13 or 5.17.

5.15. The Panel Chair may exclude a Panel Member from part of a Panel meeting where the Panel Chair considers that the matters under discussion present a conflict of interest for the Panel Member.

5.16. The Panel Chair may also exclude the Code Manager from part of a Panel meeting where the Panel Chair considers that the matters under discussion present a conflict of

interest for the Code Manager.

Attendance by other persons

5.17. A representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Panel:

(a) the Department;
(b) the Commission;
(c) the Data Protection Commissioner;
(d) the Competition and Consumer Protection Commission
(e) the Code Manager, separate from the Secretariat function; and
(f) the Code Compliance Officer.

5.18. The Panel Chair may invite other representatives from other organisations to attend and speak (but not vote) at each Panel Meeting as they deem necessary.

Minutes

5.19. The Code Manager shall circulate copies of the minutes of each Panel meeting to each person who was entitled to receive a notice of that meeting, as soon as practicable (and in any event within 5 Working Days) after the relevant meeting has been held. The Panel may determine that certain parts of a meeting are confidential, in which case those matters will not be included in the minutes circulated to persons other than the Panel , the Department and the Commission.

5.20. If any Panel Member disagrees with any item of the minutes, they shall notify the Code Manager of those items with which they disagree, and the Code Manager shall incorporate those items upon which there is disagreement into the agenda for the next following meeting of the Panel.

5.21. The Code Manager shall maintain a record of all resolutions voted on by the Panel, indicating how each Panel Member voted on each resolution, and shall make such record available on request to any Party.

5.22. The Code Manager shall publish on the Code Website a summary of the business conducted at each Panel Meeting.

Alternates

5.23. Each Panel Member may, from time to time by notice in writing to the Code Manager, appoint another natural person to act as their alternate (an “Alternate”). The Panel Chair must appoint a person to act as their Alternate.

5.24. Each such Alternate must, before their appointment as such can become valid, have provided the confirmations referred to in Clause 9.9 of the Main Body.

5.25. Where a Panel Member does not attend a Panel Meeting, the Panel Member's Alternate shall be entitled to attend (and count, in their capacity as Alternate, towards the quorum at) that meeting, and to exercise and discharge all the functions, powers and duties of the Panel Member at that meeting.

5.26. Each Panel Member may, by notice in writing to the Code Manager, remove or replace the person appointed from time to time by that Panel Member as their Alternate. An Alternate shall immediately cease to be an Alternate on the occurrence of any of the events set out in Clause 4: Vacation of Panel Members in respect of the Alternate. Where an Alternate's appointor ceases to be a Panel Member for any reason, the Alternate's role as such shall also cease.

5.27. Unless the context otherwise requires, any reference in this Code to a Panel Member shall be construed as including a reference to that Panel Member's Alternate.

Conflicts of interest

5.28. Given the duty of each Panel Member to act independently, as set out in Clause 8.11 to 8.15 of the Main Body, conflicts of interest should not regularly arise.

5.29. Notwithstanding Clause 5.28 where a decision of the Panel will have particular consequences for a particular Party or class of Parties, each Panel Member shall consider whether that decision presents a conflict of interest (whether because such Party or Parties comprise Related Persons of the Panel Member or otherwise).

5.30. Where a Panel Member considers that a decision does present a conflict of interest, the Panel Member shall absent themselves from the Panel Meeting for that decision and abstain from the vote regarding that decision. Furthermore, where the Panel Chair considers that a decision does present a conflict of interest for a Panel Member, the Panel Chair may require the Panel Member to themself from the Panel Meeting for that decision and to abstain from the vote regarding that decision.

Annex 1: Election of Elected Members

1 General

1.1. The process set out in this Clause shall apply in respect of the election of each Elected Member. This process shall apply in respect of Elected Member vacancies arising by virtue of a Panel Member's retirement in accordance with Clause 4.4 (a Scheduled Election), or a Panel Member being removed from office in accordance with Clauses 1.1(e), 1.1(p)(ii) or 1.1(q)(iii) (an Interim Election) of this Annex. In each case, the following process shall apply:

(a) each Elected Member is to be elected by a Party Category as described in Clause 8.8 of the Main Body.

(b) each Voting Group within a Party Category is entitled to cast one vote in the election of the Panel Member(s) to be elected by that Party Category;

(c) the Code Manager shall publish on the Website and send to each Party within the relevant Party Category an invitation for nominations for candidates for the role of Elected Member for that Party Category;

(d) in the case of Scheduled Elections, the invitation for nomination of candidates shall be published and sent by the Code Manager at least 35 Working Days ahead of the date on which the relevant Panel Member's term of office expires;

(e) in the case of Interim Elections, the invitation for nomination of candidates shall be published and sent by the Code Manager by no later than 5 Working Days after the date on which the relevant Panel Member was removed from office;

(f) the invitation for nomination of candidates shall request nominations within 15 Working Days after the date of the invitation;

(g) the eligible candidates for election shall be those persons who are (at the time of their nomination) capable of becoming and remaining Panel Members in accordance with Clauses 8.9 of the Main Body and Clause 4: Vacation of Panel Members, and whose nominations (whether nominated by themselves or a third party) are received by the Code Manager within the period of time set out in the request for nominations;

(h) where the Code Manager receives a nomination for a candidate that the Code Manager does not consider to be an eligible candidate in accordance with Clause 1.1(g) of this Annex, the Code Manager shall notify that person that this is the case as soon as reasonably practicable after receipt of the nomination (and, in any event, by no later than 2 Working Days following the expiry of the period of time set out in the request for nominations);

(i) where a candidate disputes the Code Manager's notification under Clause 1.1(h) of this Annex, the candidate shall have 2 Working Days following receipt of such notification to refer the matter to the Panel Chair for final determination (which

determination shall be made by the Panel Chair by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations);

(j) 6 Working Days following the expiry of the period of time set out in the request for nominations, the Code Manager shall give notice to each Party within the relevant Party Category of the names of each eligible candidate (together with any supporting information provided to the Code Manager with their nomination);

(k) at the same time as the Code Manager issues such notice, where there are more eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category, the Code Manager shall invite the Voting Groups comprising that Party Category to vote for their preferred eligible candidate;

(l) each such Voting Group shall be entitled to cast one vote, and shall cast such vote by means of a system established by the Panel which ensures that each Voting Group casts only one vote, and which allows 10 Working Days following the invitation pursuant to Clause 1.1(k) of this Annex for such vote to be cast;

(m) the successful candidate or candidates elected as a result of the votes cast in accordance with Clause 1.1 of this Annex shall be determined in accordance with Clause 1.1(q) of this Annex;

(n) the Code Manager shall not publish details of the votes cast by each Voting Group, but shall disclose such details to the Panel Chair for scrutiny;

(o) as soon as reasonably practicable following the election of an Elected Member in accordance with this Clause 1.1 of this Annex, the Code Manager shall publish on the Code Website and notify each Party of the identity of the person who has been so elected; and

(p) each person elected as a Panel Member in accordance with this Clause 3.3 shall commence their office as a Panel Member:

(i) in the case of Scheduled Elections, simultaneously with the retirement of the relevant Panel Member; or

(ii) in the case of Interim Elections, simultaneously with the notification by the Code Manager pursuant to Clause 1.1(o) of this Annex.

(q) As a result of the process set out in Clause 1.1 of this Annex:

(i) where there are the same number of eligible candidates for a Party Category as there are positions to be filled as Elected Members for that Party Category, all of the eligible candidates shall be elected as Elected Members;

(ii) where there are more eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category, the eligible candidate(s) that received the most votes in accordance with Clause 1.1(l) of this Annex shall be elected as Elected Members (and, in the case of a tie, the Code Manager shall determine the Elected Member by drawing lots, to be witnessed by the Panel Chair); or

(iii) where there are fewer eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category (including where there are no eligible candidates), the Commission will (at its discretion) be entitled to nominate an Elected Member for that Party Category. Where this Clause 1.1(q)(iii) of this Annex applies, the Panel shall be entitled (at any time

thereafter) to determine that a further Interim Election should be held in accordance with Clause 1.1 of this Annex in respect of that Party Category.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 8: Party Exit

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Schedule 8: Party Exit

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD-Mon-YYYY		n.n

1 Definitions

Term	Acronym	Definition
Access Agreement		Means an Agreement by which an organisation that is not a Party can access the Smart Meter Data System.
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or c) where a new User Category or Data Item is issued.
Change of Supplier		Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code.

Term	Acronym	Definition
		Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Data Item		Means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for which are defined and controlled in the Data Access Register.
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data Processor		Has the meaning as defined in Data Protection Legislation.
Data Protection Legislation		Means the GDPR and any other implementing legislation with the Republic of Ireland, including the Data Protection Act 2018, and, in each case, all regulations, statutes and instruments made thereunder as may be amended from time to time.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, in accordance with Clause 12 of the Main Body.

Term	Acronym	Definition
Electricity Industry Arrangements		Means any regulatory multilateral code or agreement, or obligations, maintained pursuant to one or more Licence Condition.
Electricity Supplier		Has the meaning as defined in the as defined in Statutory Instrument 426 of 2014.
Event of Breach		Has the meaning given to that expression in Clause 21 of the Main Body.
Final Customer		Means a natural or legal person who receives, or wishes to receive, a supply of energy at any premises in the Republic of Ireland, in accordance with Statutory Instrument (SI) 37 of 2022.
Meter Point Reference Number	MPRN	Means, in respect of a Smart Meter System, the supply meter point reference number allocated by the relevant Party to the premises at which the supply of gas is recorded by that Smart Meter System.
Metering Point		Has the meaning as defined in the Irish Electricity Retail Market Glossary of Terms https://rmdservice.com/glossary-of-terms
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Personal Data		Has the meaning as defined in the GDPR, as applicable to Data Processed on the Smart Meter Data System. This includes the Data

Term	Acronym	Definition
		Items marked as Personal Data within Appendix A: Data Glossary of the Code.
Processing (including Process, Processed)		Has the meaning as defined in Data Protection Legislation.
Registered Supplier		Means, in respect of a Metering Point and at any time, the Electricity Supplier recorded against that Metering Point in the MRSO at that time.
Replacement Supplier		Means a supplier appointed by means of a direction by the Commission under its customer protection protocols.
Schedule		Means a Schedule to this Code.
Smart Meter Data		Has the meaning as defined in Statutory Instrument 37 of 2022. ***Potentially to be replaced by the definition in the final legislation***
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Smart Meter System		Means an electronic System that can measure energy consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication, as defined in Statutory Instrument 426 of 2014, and that connects to the Smart Meter Data System.
Sub-Processor, Sub-Processing		Has the meaning as defined in Data Protection Legislation.
Supplier of Last Resort	SoLR	Means, in respect of each premises supplied by a failing Electricity Supplier, the Supplier directed to supply gas and/or electricity to that premises by the Commission under

Term	Acronym	Definition
		the Commission's customer protection protocols.
System(s)		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith.
Third Party		A natural or legal person that accesses or uses Data (including but not limited to Consumption Data) on behalf of a Party or Other User, without themselves being a Party or Other User.
Withdrawal Date		Means the time and date on which a Party wishes to withdraw from this Code, as specified in its Withdrawal Notice.
Withdrawal Notice		Means a notice given by a Party in accordance with Clause 4 of Schedule 8: Party Exit indicating that Party's wish to withdraw from this Code.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.

2 Introduction

2.1. This Schedule sets out the process with which a Party must comply to enable an orderly exit from this Code.

2.2. This includes:

(a) expulsion from this Code following an Event of Breach;

(b) considerations for Parties seeking to exit the Code voluntarily; and

(c) management of Supplier of Last Resort (SoLR) Process to facilitate the transfer of responsibilities under this Code from the existing Electricity Supplier to the Replacement Supplier.

2.3. This Schedule must be read in conjunction with Clause 21 and Clause 22 of the Main Body, which describe the instances where Parties may be expelled from the Code, in addition to Clause 11 and Clause 12 of the Main Body and Schedule 5: Data Privacy, which describe the obligations in place on the Code Compliance Officer, Data Systems Provider and Parties respectively in relation to exit from the Code.

3 Expulsion of Parties

3.1. As set out in Clause 22.1 of the Main Body, a Party cannot be expelled from this Code unless the Commission has approved such expulsion.

3.2. The Panel shall coordinate any proposed expulsion from this Code with any concurrent process under the other Electricity Industry Arrangements and/or any enforcement action by the Commission.

3.3. Subject to Clauses 3.1 and 3.2, the Panel may expel a Party from this Code by written notice to that Party where that Party is subject to an ongoing Event of Breach.

3.4. Where notice of expulsion is served on a Party pursuant to Clause 3.3, the Code Manager shall promptly confirm the expulsion (and the effective date of expulsion) to:

(a) all Parties;

(b) the Code Compliance Officer;

(c) the DSP;

(d) the code managers of any other Electricity Industry Arrangements to which the expelled Party is or was party; and

(e) the Commission.

3.5. Following receipt of a notification from the Code Manager in accordance with Clause 3.4:

(a) The Code Compliance Officer shall provide the Code Manager with support in identifying that no Metering Points are registered and no gaining Metering Points to be gained due to Change of Supplier process prior to a Party's exit from the Code, and that Data, including Personal Data, received from the Smart Meter Data System has been deleted, as described in Clause 12 of the Main Body; and

(b) The DSP shall ensure that the Party is removed from access to the Smart Meter Data System, as described in Clause 11.6(l)(i) of the Main Body;

(c) The Code Manager shall ensure that the Party is removed from the Data Access Register.

4 Voluntary Exit by Parties

4.1. Subject to Clause 4.3, each Party shall be entitled to initiate its own withdrawal from this Code by giving notice in writing (known as a Withdrawal Notice) to the Code Manager.

4.2. The Withdrawal Notice shall specify the time and date on which the Party wishes to withdraw from this Code (known as the Withdrawal Date), being not less than 28 days after the date of the Withdrawal Notice.

4.3. A Party may not withdraw from the Code if, as at 17.00 hours on the day which is 2 Working Days prior to the Withdrawal Date:

(a) such Party has not deleted and declared deletion of any Data, including Personal Data, received from the Smart Meter Data System, in accordance with Schedule 5: Data Privacy;

(b) the Commission has not approved the withdrawal from the Code; and/or

(c) where such Party is an Electricity Supplier, it continues to be the Registered Supplier in respect of any MPRNs.

4.4. Following receipt of a Withdrawal Notice from a Party, the Code Manager shall check that the Party is eligible to withdraw, as described in Clause 4.3. Where the Party is eligible to withdraw, the Code Manager shall accept the Withdrawal Notice and promptly notify the organisations listed in Clause 3.4 of the withdrawing Party's intention to withdraw from the Code on the agreed Withdrawal Date.

4.5. Following receipt of a notification from the Code Manager in accordance with Clause 4.4:

(a) The Party shall issue a self-declaration, no later than required by Clause 4.3, that:

(i) the Party has demonstrated that Data, including Personal Data, received from the Smart Meter Data System has been deleted in accordance with Schedule 5: Data Privacy, unless otherwise needed in accordance with that Schedule; and

(ii) no Metering Points are registered and no gaining Metering Points to be gained due to Change of Supplier process prior to a Party's exit from the Code; and

(b) The Party shall evidence the controls identified in Clause 4.5(a) are in place, in accordance with Schedule 5: Data Privacy;

(c) The Code Compliance Officer shall provide the Code Manager with support in identifying that the controls issued in the Party's self-declaration under Clause 4.5(a) are in place, as described in Clause 11 of the Main Body;

(d) The DSP shall ensure that the Party is removed from access to the Smart Meter Data System, as described in Clause 12 of the Main Body; and

(e) The Code Manager shall ensure that the Party is removed from the Data Access Register.

4.6. Provided the requirements of Clause 4.3 are satisfied, with effect from the Withdrawal Date, the withdrawing Party shall cease to be a Party in accordance with Clause 22 of the Main Body of this Code.

4.7. Where the requirements of Clause 4.3 are not satisfied in respect of a Party, then that Party shall not withdraw from this Code, and Clause 4.6 shall not apply. If the Party still wishes to withdraw, it must serve another Withdrawal Notice and the requirements of Clause 4.3 will be reassessed.

4.8. Where a Party withdraws from this Code in accordance with Clause 4.6, the Code Manager shall promptly confirm such withdrawal to the organisations listed in Clause 3.4.

5 Exit for Other Users

5.1. Other Users shall be entitled to terminate their access to the Smart Meter Data System by providing a Withdrawal Notice to the Code Manager.

5.2. The Withdrawal Notice shall specify the time and date on which the Other User wishes to terminate their access, being no less than 28 days after the date of the Withdrawal Notice.

5.3. An Other User may not terminate its agreement if, as at 17.00 hours on the day which is 2 Working Days prior to the Withdrawal Date:

(a) the Other User has not deleted and declared deletion of any Data, including Personal Data, received from the Smart Meter Data System, in accordance with Schedule 5: Data Privacy; and/or

(b) the Panel has not approved the withdrawal from the Code.

5.4. Following receipt of a Withdrawal Notice from an Other User, the Code Manager shall check that the Party is eligible to withdraw, as described in Clause 4.3. Where the Other User is eligible to withdraw, the Code Manager shall accept the Withdrawal Notice and promptly notify the organisations listed in Clause 3.4 of the Other User's intention to withdraw from the Code on the agreed Withdrawal Date.

5.5. Following receipt of a notification from the Code Manager in accordance with Clause 5.4:

(a) The Other User shall issue a self-declaration, no later than required by Clause 5.3, that the Other User has demonstrated that Data, including Personal Data, received from the Smart Meter Data System has been deleted in accordance with Schedule 5: Data Privacy, unless otherwise needed in accordance with that Schedule; and

(b) The Other User shall evidence the controls identified in Clause 5.5(a) are in place, in accordance with Schedule 5: Data Privacy;

(c) The Code Compliance Officer shall provide the Code Manager with support in identifying that the controls issued in the Other User's self-declaration under Clause 5.5(a) are in place, as described in Clause 11 of the Main Body;

(d) The DSP shall ensure that the Other User is removed from access to the Smart Meter Data System, as described in Clause 12 of the Main Body; and

(e) The Code Manager shall ensure that the Other User is removed from the Data Access Register.

5.6. Provided the requirements of Clause 5.3 are satisfied, with effect from the Withdrawal Date, the Other User will cease to be entitled to have access to the Smart Meter Data System.

5.7. Where the requirements of Clause 5.3 are not satisfied in respect of an Other User, then that Other User shall not withdraw from this Code, and Clause 5.6 shall not apply. If the Other User still wishes to withdraw, it must serve another Withdrawal Notice and the requirements of Clause 5.3 will be reassessed.

5.8. Where an Other User terminates its agreement in accordance with Clause 5.6, the Code Manager shall promptly confirm such termination I to the organisations listed in Clause 3.4.

5.9. Where an Other User's Access Agreement has been terminated in accordance with Clauses 21 and 23 of the Main Body, the Panel will terminate the Access Agreement by written notice to that Other User where that Other User is subject to an ongoing Event of Breach.

5.10. Where notice of termination is served on an Other User pursuant to Clause 5.9, the Code Manager shall promptly confirm the termination (and the effective date of termination) to:

(a) the Code Compliance Officer, and;

(b) the DSP;

5.11. Following receipt of a notification from the Code Manager in accordance with Clause 5.10:

(a) The Code Compliance Officer shall provide the Code Manager with support in identifying that Data, including Personal Data, received from the Smart Meter Data System has been deleted, as described in Clause 7 of this Schedule 8: Party Exit; and

(b) The DSP shall ensure that the Other User is removed from access to the Smart Meter Data System, as described in Clause 12 of the Main Body;

(c) The Code Manager shall ensure that the Other User is removed from the Data Access Register.

6 Supplier of Last Resort Process

6.1. Where a Supplier of Last Resort is appointed in respect of premises, they shall become, from the date and time set out by the direction of the Commission, responsible for all obligations assigned to the Registered Supplier as set out within the Code.

6.2. The Supplier of Last Resort shall be responsible for providing information to the Final Customer around the use of their Personal Data, in accordance with Schedule 5: Data Privacy, connected to the Commissions direction and the activities of the Replacement Supplier.

7 Exit Arrangements

7.1. This Clause shall apply to the access, receipt and Processing of Data, including Smart Meter Data, from the Smart Meter Data System.

7.2. Each Party and Other User shall ensure that, following receipt of its request for withdrawal, or notification of its expulsion or the termination of its Access Agreement, from the Code Manager under Schedule 8: Party Exit or otherwise:

(a) It issues a self-declaration in accordance with Clause 4.5(a) or 5.5(a);

(b) It conducts and evidences that Data, including Personal Data, received from the Smart Meter Data System has been deleted from its Systems, including its Data Processors', Sub-Processors' and Third Parties' Systems, and/or returned to the Data Systems Provider (at its request) unless permitted to be retained for determined periods and purposes in accordance with this Schedule;

(c) It provides any such documents or evidence to the Code Compliance Officer, at its request, and otherwise shall cooperate with the Code Compliance Officer in accordance with Clauses 7.3 to 7.5;

7.3. Each Party or Other User shall cooperate with the Code Compliance Officer as required for any investigation that the Code Compliance Officer requests in accordance with:

(a) A Party's withdrawal from the Code, under Schedule 8: Party Exit;

(b) A Party's expulsion from the Code, under Schedule 8: Party Exit; or

(c) The termination of an Other User's Access Agreement.

7.4. For the purposes of Clause 7.3 the Code Compliance Officer's investigation may encompass identifying the information specified in Clause 11.6(l) of the Main Body.

7.5. At the request of the Panel, the Code Compliance Officer may conduct an Ad-Hoc Assessment of a Party or Other User in the course of its investigation under Clause 7.3, in particular, where:

(a) The declaration issued in accordance with Clause 4.5(a) or Clause 5.5(a) of Schedule 8: Party Exit is either not received or suspected to be false, in the opinion of the Panel;

(b) That the evidence provided by the Party and Other User under Clause 7.2 is not satisfactory to demonstrate its obligations under Schedule 8: Party Exit.

7.6. Each Party and Other User shall comply with its obligations under this Schedule and shall remain obligated to comply with its obligations under this Schedule until the time that its withdrawal or expulsion is effective under Clause 22 (or Clause 23 if an Other User) of the Main Body.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 9:
Change Management

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Schedule 9: Change Management

Version 0.1

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD-Mon-YY		n.n

1 Definitions

Term	Acronym	Definition
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or c) where a new User Category or Data Item is issued.
Alternative Modification Proposal		Has the meaning given to that expression in Clause 18.1.
Anonymous Data		Means Data which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
Change Proposal	CP	Means a proposal to change a subsidiary document to the Code and Schedules, in accordance with this Schedule 9: Change Management.
Change Register		Means the register established and maintained by the Code Manager which contains all current and past Modification Proposals, as further described in Clause 5 of Schedule 9: Change Management.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.

Term	Acronym	Definition
Code Website		Means the dedicated website established by the Code Manager for the purposes of this Code.
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Commission Modification Proposal		Means a Commission-Approved Modification Proposal as set out in 9.3.
Cross Industry Change Arrangements		Means those arrangements established in accordance with Clause 4.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code.
Code Objectives		Has the meaning given to that expression in Clause 2 of the Main Body.
Competition and Consumer Protection Commission		Means the Competition and Consumer Protection Commission within the Republic of Ireland.
DAR Change		Has the meaning of 3.4 of Schedule 9: Change Management.
DAR Release		Means a package of one or more approved DAR Change Proposals which is implemented in accordance with 27.1 of Schedule 9: Change Management.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these)

Term	Acronym	Definition
		embodied in any medium (whether tangible or electronic).
Data Access Register	DAR	Means a register that describes what each Party or Other User is entitled to access on the Smart Meter Data System, the Legal Basis for such access, and the purposes for such access.
Data Item		Means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for which are defined and controlled in the Data Access Register.
Data Protection Commission	DPC	Means the commissioner as defined in the Data Protection Legislation.
Data Protection Impact Assessment	DPIA	Has the meaning as defined in Data Protection Legislation.
Data Systems Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, as defined in Schedule 2: Access Arrangements.
Electricity Industry Arrangements		Means any regulatory multilateral code or agreement, or obligations, maintained pursuant to one or more Licence Condition.
Final DAR Change Proposal Report		Has the meaning given to that expression in Clause 27.10.
Final Modification Report		Has the meaning given to that expression in Clause 20.2.
Good Industry Practice		Means, in respect of a person, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced organisation engaged in a similar type of undertaking as that person under the same or similar circumstances, complying with all applicable laws, codes of professional conduct,

Term	Acronym	Definition
		relevant codes of practice, Irish, European and other relevant standards.
Housekeeping Modification Proposal		Means a Modification Proposal which satisfies the requirements of Clause 24.
Housekeeping Modification Report		Means a written report on a Housekeeping Modification Proposal, as described in Clause 24 of Schedule 9: Change Management.
Modification		A modification, revision, amendment, supplementation, extension, consolidation or replacement to the provisions of the Code which is accepted and implemented in accordance with this Schedule 9.
Modification Path		Means one of the three modification paths followed by a Modification Proposal, being either a Commission-Approved Modification, a Self-Governance Modification or a Housekeeping Modification.
Modification Proposal	MP	Means the term applied to a Modification proposed in accordance with Clause 15 of the Main Body and this Schedule 9.
Modification Proposal Plan		Means, in respect of a Modification Proposal, a plan produced in accordance with Clause 9.5.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Personal Data		Has the meaning as defined in the GDPR, as applicable to Data

Term	Acronym	Definition
		Processed on the Smart Meter Data System. This includes the Data Items marked as Personal Data within Appendix A: Data Glossary.
Preliminary DAR Change Proposal Report		Means a report which satisfied the requirements of Clause 27.5.
Preliminary Modification Report		Means the written report on a Modification Proposal prepared by the Code Manager in accordance with Clause 19.
Processing		Has the meaning as defined in Data Protection Legislation.
Proposer		Means a person who submits a Modification Proposal or DAR Change Proposal.
Provisional DAR Change Proposal Report		Has the meaning given to that expression in Clause 27.6.
Release Plan		Means the document of that name published by the Code Manager in accordance with Clause 26.
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Self-Governance Modification		Means a Modification Proposal which is a Panel approved change.
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time in accordance with Schedule 7: Panel.
Systems		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic

Term	Acronym	Definition
		communications, including all hardware, software, firmware and Data associated therewith.
Test Environments		Means the testing environments as described in the Test Plan.
Test Phase(s)		Means each phase of testing as set out in the DSP Test Plan.
Test Plan		Has the meaning given to that expression in Clauses 26.1 and 26.2.
Test Strategy		Means the document produced by the Code Manager setting out the Testing objectives and approach to coordinating testing activities between the DSP, Parties and Other Users.
User Category		A Category of user as defined in Schedule 2: Access Arrangements.
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.
Working Group		Means a group of persons, established by the Panel, for the purposes set out in Schedule 7: Panel and Schedule 9: Change Management.
Working Group Terms of Reference		Means the document produced by the Responsible Sub-Committee and published on the Code Website for the Working Group to operate in accordance with.

2 Introduction

2.1. With the exceptions set out in Clauses 15.1 and 15.2 of the Main Body, this Schedule sets out the process for changing this Code. A change to this Code may only be made in accordance with this Schedule. This includes changes to the Schedules.

2.2. Each change to this Code must commence with a Modification Proposal made in accordance with the provisions of this Schedule.

2.3. Modification Proposals will be expected to focus on an issue that the Proposer seeks to address and/or an outcome they wish to effect, rather than necessarily on the detail of a potential solution. Where Modification Proposals do contain a proposed solution, that will not preclude the Code Manager from exploring and developing solutions which may better fulfil the Proposer's intention and/or the Code Objectives more generally.

3 Process overview

3.1. Whilst each Modification Proposal submitted in accordance with Clause 7 will follow a process that is particular to its requirements, there are six stages to the process, as follows (subject to Clause 3.3):

(a) submission and acceptance of the Modification Proposal (Clauses 7 and 8);

(b) initial assessment of the Modification Proposal (Clauses 9 and 10);

(c) only as needed, further development of the Modification Proposal (Clause 11), impact assessment by the Code Compliance Officer, Data Systems Provider (DSP), Parties and/or Other Users (Clauses 12, 13 and/or 14), and/or referral in accordance with any established Cross Industry Change Arrangements (Clause 15);

(d) production of the Preliminary Modification Report and consultation on such report (Clauses 19 and 20);

(e) approval or rejection of the Modification Proposal (Clauses 21 to 23); and

(f) implementation and release of the Modification Proposal (Clauses 25 and 26).

3.2. The Panel is the body responsible for making the decision (or for making recommendations to the Commission as the case maybe) on whether to approve a Modification Proposal. The Panel may consult with or delegate responsibility for a specific Modification Proposal, group of Modifications Proposals or any such Modification Proposals that impacts any identified part of the Code, Schedules and/or Appendices, to:

(a) an existing Sub-Committee; or

(b) where a Sub-Committee does not exist, form a Sub-Committee in accordance with Clause 9 of the Main Body form such.

3.3. In the case of a Housekeeping Modification Proposal a shortened process shall apply, as set out in Clause 23.

3.4. In the case of any Change Proposals impacting Data Access Register (a "DAR Change") the Change Proposal shall follow the process set out in Clause 27.

4 Establishing Cross Industry Change Arrangements

4.1. The Code Manager shall establish from time-to-time (in accordance with the Panel's directions), together with relevant managers of other Electricity Industry Arrangements that are subject to regulatory change, Cross Industry Change Arrangements to manage the interaction between this Code and other Electricity Industry Arrangements for specific cross industry changes.

4.2. The Code Manager shall agree the terms of reference for the Cross Industry Change Arrangements with the managers of the other Electricity Industry Arrangements. Such terms of reference must include:

(a) constituency of the group, including details of the organisations required to participate;

(b) high-level details of the provisions that will be considered by the Cross Industry Change Arrangements;

(c) the process for determining the matters outlined in Clause 4.3; and

(d) how and when any meetings are to be convened.

4.3. The core roles of the Cross Industry Change Arrangements shall be to:

(a) provide its views on whether a potential change to one Electricity Industry Arrangement is likely to have an impact on the other Electricity Industry Arrangements or on the parties and stakeholders of those arrangements;

(b) determine whether a potential change to one Electricity Industry Arrangement is likely to require a parallel or consequential change to another Electricity Industry Arrangement; and

(c) where Clause 4.3(b) applies, determine which Electricity Industry Arrangement is to be used as the lead-code for the change.

4.4. Where it is determined that this Code is to be used as the lead for a Modification Proposal, then:

(a) the Code Manager shall progress the Modification Proposal in accordance with this Code;

(b) the Code Manager shall coordinate with the managers of the other affected Electricity Industry Arrangements so that they can manage the processes under their arrangements in parallel with the process under this Code;

(c) the Modification Proposal shall only be approved if both,

(i) the Modification Proposal is approved in accordance with this Code; and

(ii) the associated consequential changes under the other Electricity Industry Arrangements are all approved in accordance with those other arrangements; and

(d) if the Modification Proposal is approved in accordance with this Code, but one or more of the associated consequential changes under the other Electricity Industry Arrangements are not approved in accordance with those other arrangements, then the Panel may, within 30 days of the decision or other determination which triggered the application of this sub-clause, refer the Modification Proposal and all associated consequential changes to the Commission for a decision.

4.5. Where it is determined that another Electricity Industry Arrangement is to be used as the lead for a Modification Proposal, then the Code Manager shall progress that Modification Proposal in accordance with this Code, but subject to the following:

(a) the Code Manager shall progress the Modification Proposal in parallel with the change under the lead-code, and as far as practicable subject to the timetable determined under the lead-arrangement;

(b) the Panel shall have regard to the change under the lead-arrangement but make its decision under Clause 21 based on an assessment of the consequential change to this Code only;

(c) the Modification Proposal shall only be approved if both,

(i) the Modification Proposal is approved in accordance with this Code; and

(ii) the associated change to the lead Electricity Industry Arrangement is approved in accordance with that arrangement; and

(d) if the change to the lead Electricity Industry Arrangement is approved, but the consequential change under this Code is not approved, then the manager (or other relevant body) under the lead Electricity Industry Arrangement may refer the decision in respect of the consequential change under this Code to the Commission; provided that such referral must be made within 30 days after the later of the approval under the lead arrangement or the rejection under this Code.

5 Change Register

5.1. The Code Manager shall establish and maintain a register of all current and past Modification Proposals (referred to as the Change Register).

5.2. The Code Manager shall determine the content of the Change Register.

5.3. Where submission of a Modification Proposal is accepted under Clause 8, the Code Manager shall assign a unique identifier to the Modification Proposal, and add the Modification Proposal to the Change Register.

5.4. The Code Manager shall publish the Change Register on the Code Website.

5.5. The Code Manager shall also publish on the Code Website details of changes and proposed changes to other Electricity Industry Arrangements which are related to or may have an impact on this Code, and details of other matters which may affect this Code, with due consideration to other Electricity Industry Arrangements.

6 Preliminary advice and assistance

6.1. The Code Manager shall provide advice and assistance to any interested person, consistent with Good Industry Practice, which shall include:

(a) assistance with the development of Modification Proposals and/or exploration of other possible remedies to address issues raised;

(b) explanation of the operation and effect of this Code, including this Schedule 9: Change Management; and

(c) acting as a 'critical friend' in the provision of support to any person with an interest in this Code, particularly with respect to under-represented Parties and Other Users, small market participants and consumer representatives.

7 Submitting a Modification Proposal

7.1. Any Party or Other User, and the Code Manager, may submit a Modification Proposal (referred to as a Proposer), regardless of whether or not they are a Party.

7.2. The Code Manager may prescribe what information will be required to support the Modification Proposal, in accordance with Good Industry Practice. The Code Manager shall set out the requirements, and publish accompanying guidance on the submission and treatment of Modification Proposals, on the Code Website.

7.3. Modification Proposals must be submitted using the submission form published by the Code Manager on the Code Website.

8 Acceptance of a Submitted Modification Proposal

8.1. Except in the case of a Commission Modification Proposal, or where otherwise directed by the Panel, the Code Manager may refuse to accept submission of a Modification Proposal if the Code Manager considers that one of more of the following apply:

(a) the proposal is incomplete or insufficiently clear;

(b) the proposal and/or issue that it seeks to address is not materially different from or could appropriately form part of an active Modification Proposal that has not yet been decided upon;

(c) the proposal concerns matters that are outside the scope of this Code; or

(d) the proposal has no reasonable prospect of being approved.

8.2. If the Code Manager refuses to accept submission of a Modification Proposal, it shall write to the Proposer, copying in the Panel, setting out the reasons for refusal, and offering assistance (where reasonably practicable) to address the reasons given (such that the proposal could be re-submitted).

8.3. The Panel may, independently or on the application of any person, overrule a decision by the Code Manager to refuse submission or progression of a Modification Proposal, based on the same criteria as apply under Clause 8.1.

8.4. Where submission of a Modification Proposal is accepted by the Code Manager, unless it is clear that the scope of the proposal is limited to the provisions of this Code, the Code Manager shall refer the Modification Proposal for discussion with other Electricity Industry Arrangement managers under the Cross Industry Change Arrangements for consideration in accordance with Clause 4.3.

8.5. The Code Manager may revisit its consideration of a Modification Proposal under this Clause 8 if new evidence or analysis is available, whether as a result of an impact assessment or otherwise. Despite its earlier acceptance of the Modification Proposal, if the Code Manager reasonably believes that any of the criteria in Clauses 8.1(b), 8.1(c), or 8.1(d) now apply, the Code Manager may determine that the Modification Proposal should not progress any further and Clause 8.2 shall apply.

9 Initial assessment

9.1. For each Modification Proposal accepted under Clause 8, the Code Manager shall undertake an initial assessment of the proposal in accordance with the requirements of this Clause 9, and the Panel's standing instructions regarding timetable and criteria.

Modification Paths

9.2. The Code Manager shall make the initial determination of which approval route (referred to as a Modification Path) each Modification Proposal will follow, being:

(a) a Commission-Approved Modification;

(b) a Self-Governance Modification; or

(c) a Housekeeping Modification.

9.3. Commission-Approved Modifications are for those Modification Proposals which satisfy one or more of the following criteria:

(a) the Modification Proposal has been raised by the Commission or as a result of a direction by the Commission;

(b) the Modification Proposal concerns the governance of this Code; or

(c) as a consequence of Clauses 4.4(d) or 4.5(d).

9.4. The Code Manager may seek an informal view from the Commission regarding the most appropriate Modification Path.

9.5. The Code Manager shall draft the initial Modification Proposal Plan for each Modification Proposal, and may make amendments to each such plan from time to time (in each case subject to Clause 9.7).

9.6. The Modification Proposal Plan for each Modification Proposal shall set out:

(a) the timetable and priority of the Modification Proposal;

(b) whether the Modification Proposal is:

(i) sufficiently developed to warrant it going straight to the Preliminary Modification Report stage; or

(ii) in need of further development by the Code Manager, and/or of an impact assessment by the Parties and Other Users and/or the DSP and/or the Code Compliance Officer;

(c) whether the Modification Proposal has other Electricity Industry Arrangement impacts such that it needs to be progressed in conjunction with other Electricity Industry Arrangement managers under the Cross Industry Change Arrangements; and

(d) whether, in the opinion of the Code Compliance Officer, a Data Protection Impact Assessment is required on any change in Processing activities impacted by the Modification Proposal.

9.7. In determining the prioritisation and timetable to be followed in respect of each Modification Proposal, the Code Manager shall:

(a) (subject to (b) below) determine a reasonable timetable, having regard to the Modification Proposal's complexity (including where a Data Protection Impact Assessment is to be carried out), importance relative to other ongoing Modification Proposals and time-sensitivity; and

(b) in the case of Commission Modification Proposals, determine a timetable consistent with any relevant timetable issued by the Commission;

10 Initial Assessment Report

10.1. For each Modification Proposal accepted under Clause 8, the Code Manager shall report to the Panel on the outcome of the Code Manager's initial assessment under Clause 9, and providing the Panel with the proposed Modification Proposal Plan.

10.2. The Code Manager’s initial determination under Clause 9 of the applicable Modification Path and Modification Proposal Plan shall apply unless and until over-turned by:

(a) the Code Manager, who shall keep the relevant issues under consideration, and who may make changes as circumstances dictate; and/or

(b) the Panel, when considering the report provided under this Clause 10 or following an application for a Modification Proposal (but the Panel cannot overrule the Commission and, where delegated to a Sub-Committee, the Sub-Committee cannot overrule the Panel); and/or

(c) the Commission, at its own volition or (where the issue has previously been determined by the Panel) following the application of a Modification Proposal.

11 Modification Proposal development

11.1. This Clause 11 only applies to a Modification Proposal where its Modification Proposal Plan provides that further development of the Modification Proposal by the Code Manager is required.

11.2. The Code Manager shall further analyse and develop the Modification Proposal in accordance with the Modification Proposal Plan.

11.3. Where the Code Manager and/or Panel deems that the Modification Proposal requires further analysis and development, the Panel shall establish a group of persons (a Working Group). Such Working Groups shall be formed and operate in accordance with terms of reference as agreed by the Panel and published on the Code Website (the "Working Group Terms of Reference").

11.4. Where the Modification Proposal affects access to Data, the Code Manager shall request the opinion of the Code Compliance Officer as to whether a Data Protection Impact Assessment is required with respect to any Processing activities impacted by a Modification Proposal.

11.5. Where the Code Compliance Officer determines that Data Protection Impact Assessment is required, the Code Compliance Officer shall conduct such a Data Protection Impact Assessment for the consideration of the Security Sub-Committee and the Panel.

11.6. The Security Sub-Committee and, where applicable, the Panel shall consider any risks identified by the Data Protection Impact Assessment and their effects on the Modification Proposal with escalation to the Panel for a decision on the implementation of any mitigating actions.

11.7. The Proposer shall retain control of the legal text of the Modification Proposal, and no variations can be made to the legal text without the Proposer's approval. Where the Proposer does not wish to vary the legal text of its Modification Proposal, the Code Manager may raise an Alternative Modification Proposal.

12 DSP impact assessments

12.1. This Clause 12 only applies to a Modification Proposal where its Modification Proposal Plan provides that an impact assessment from the DSP is required.

12.2. Where required, the Code Manager shall request an impact assessment from the DSP, in accordance with the Modification Proposal Plan.

12.3. Where requested to do so by the Code Manager, the DSP shall, within 5 Working Days of a request, confirm whether the DSP considers that the Modification Proposal would be likely to have an impact on the services it provides.

12.4. Where the Code Manager requests further assessment, the DSP shall:

(a) within 15 Working Days of a request, unless otherwise agreed with the Code Manager, provide a preliminary assessment of the scope, cost and likely timescales for changes to its Systems which would be necessary as a result of the Modification Proposal being approved, together with confirmation of the cost and timescales of providing a detailed impact assessment; and

(b) within 40 Working Days (or in accordance with such other timetable as the Code Manager may agree) provide a detailed impact assessment of the scope, cost and timescales for making the changes to the Systems the DSP uses (or its sub-contractors use) to provide the services it provides in its capacity as the DSP which would be necessary as a result of the Modification Proposal being approved.

12.5. Where the response to DSP impact assessments identifies the need to coordinate testing activities between the DSP and Parties and Other Users (should the Modification Proposal be approved for implementation), the Code Manager shall create a Code Test Strategy, setting out the testing objectives and approach to coordinating testing activities between the DSP and Parties and Other Users.

13 Code Compliance Officer Impact Assessment

13.1. This Clause 13 only applies to a Modification Proposal where its Modification Proposal Plan provides that an impact assessment from the Code Compliance Officer is required.

13.2. The Code Manager shall request an impact assessment from the Code Compliance Officer, in accordance with the Modification Proposal Plan.

13.3. Where requested to do so by the Code Manager, the Code Compliance Officer shall, within 5 Working Days of a request, confirm whether the Code Compliance Officer considers that the Modification Proposal would be likely to have an impact on the services it provides.

13.4. Where the Code Manager requests further assessment, the Code Compliance Officer shall, within 15 Working Days of a request, unless otherwise agreed with the Code

Manager, provide a preliminary assessment of the scope, cost and likely timescales for changes to the service, including any systems, processes and products, which would be necessary as a result of the Modification Proposal being approved, together with confirmation of the cost and timescales of providing a detailed impact assessment.

14 Party and Other User impact assessments

14.1. This Clause 14 only applies to a Modification Proposal where its Modification Proposal Plan provides that an impact assessment from the Parties and Other Users (or one or more classes of Parties or Other Users) is required.

14.2. The Code Manager shall consult with and seek impact assessments from the Parties and Other Users (or one or more classes of Parties or Other User) in accordance with the Modification Proposal Plan.

15 Consultation with other Electricity Industry Arrangement Managers

15.1. This Clause 15 only applies to a Modification Proposal where its Modification Proposal Plan provides that other code managers are to be consulted on the Modification Proposal, in accordance with the Cross Industry Change Arrangements.

15.2. The Code Manager shall consult with other Electricity Industry Arrangement managers in accordance with the Cross Industry Change Arrangements, in accordance with the Modification Proposal Plan.

15.3. The Code Manager shall progress the Modification Proposal subject to Clause 4.4 or 4.5 (as applicable in accordance with the Cross Industry Change Arrangements).

16 Compliance with Modification Proposal Plan

16.1. The Panel, the Panel, the Code Manager, the DSP, the Code Compliance Officer and each Party and Other User shall (insofar as within its reasonable control) complete any and all of the respective tasks assigned to them in respect of a Modification Proposal in accordance with the Modification Proposal Plan applying to that Modification Proposal.

17 Withdrawing a Modification Proposal

17.1. The Proposer may withdraw support for a Modification Proposal on notice to the Code Manager at any time prior to publication of the proposal's Final Modification Report.

17.2. As soon as is reasonably practicable after receiving such notice, the Code Manager shall notify the Parties and Other Users that the Proposer has withdrawn support for the Modification Proposal.

17.3. Where, within 10 Working Days of the Code Manager issuing a withdrawal notice, the Code Manager receives notice from an individual or organisation that it is prepared to adopt the Modification Proposal, that individual or organisation shall become the Proposer for the Modification Proposal. The Code Manager may also choose to adopt a Modification Proposal that would otherwise be withdrawn, and the Change Register will be updated to reflect the new Proposer following the adoption.

17.4. Unless adopted under Clause 17.3, the Modification Proposal shall be withdrawn on the expiry of the notice period under that Clause, and the Change Register updated accordingly.

17.5. Where one or more Commission Modification Proposals have been raised, the Commission may issue a direction under this Clause 17.5 that requires the withdrawal of those Commission Modification Proposals and of any related Alternative Modification Proposals. Where the Commission so directs, such Modification Proposals shall be deemed to have been withdrawn under this Clause 17 and shall not be capable of being adopted under Clause 17.3.

17.6. Where a Modification Proposal is withdrawn which already has an Alternative Modification Proposal associated to it, the Alternative Modification Proposal is not automatically withdrawn by the same notice and will continue to be progressed in accordance with the published Modification Proposal Plan.

18 Alternative Modification Proposals

18.1. Any person may raise an alternative proposal (referred to as an Alternative Modification Proposal) to be progressed alongside an existing Modification Proposal, subject to the following:

(a) an Alternative Modification Proposal must be raised before publication of the Preliminary Modification Report for the Modification Proposal (and the Code Manager can refuse to accept a proposed Alternative Modification Proposal if its acceptance would prevent the Code Manager completing the Preliminary Modification Report in accordance with the Modification Proposal's timetable);

(b) the Code Manager may refuse a proposed Alternative Modification Proposal on the same grounds as apply to Modification Proposals under Clause 8.1;

(c) the Code Manager may refuse a proposed Alternative Modification Proposal on the grounds it is not seeking to address the same (or similar) issues as the Modification Proposal; and

(d) the Code Manager may refuse a proposed Alternative Modification Proposal on the grounds that it is not substantively different from the existing Modification Proposal and/or its existing Alternative Modification Proposals.

18.2. There is no restriction on the number of Alternative Modification Proposals that can be

raised in relation to a Modification Proposal.

18.3. Refusal by the Code Manager to accept an Alternative Modification Proposal does not prevent the Proposer submitting a new Modification Proposal.

18.4. Each Alternative Modification Proposal shall be subject to the same process as applies to the Modification Proposal in respect of which the Alternative Modification Proposal was raised. Except where the context otherwise requires, references in this Code to Modification Proposals shall be deemed to include reference to its Alternative Modification Proposal(s).

18.5. The decision of the Panel in respect of the original Modification Proposal and its Alternative Modification Proposal(s) shall be made at the same time, and on the basis that no more than one of the changes can be approved by the Panel.

19 Preliminary Modification Report

19.1. Save for those exceptional circumstances to which Clauses 11, 12, 13 and/or 14, apply, Modification Proposals will progress from their initial assessment under Clauses 9 and 10 to the Preliminary Modification Report phase (as described in this Clause 19).

19.2. In the Preliminary Modification Report phase, the Code Manager shall prepare a written report on the Modification Proposal (referred to as a Preliminary Modification Report).

19.3. The Preliminary Modification Report for each Modification Proposal shall set out:

(a) a description and analysis of the Modification Proposal;

(b) the proposed legal text to change this Code in order to give effect to the Modification Proposal;

(c) the proposed implementation date(s) for the implementation of the Modification Proposal;

(d) for Self-Governance Modifications, the business case for the Modification Proposal, and the Code Manager's recommendation as to whether or not the Modification Proposal should be approved;

(e) for Commission-Approved Modifications, an assessment of the Modification Proposal against the Code Objectives, and the Code Manager's recommendation as to whether or not the Modification Proposal should be approved;

(f) for Housekeeping Modifications, the business case for the Modification Proposal, and the Code Manager's recommendation as to whether or not the Modification Proposal should be approved;

(g) where relevant, the assessment of the DSP as to whether implementation of the Modification Proposal would require changes to its Systems, and (if so) the likely cost of such changes, and the time period required for the design, build and delivery of the changes;

(h) where relevant, the outcome of any Code Compliance Officer impact assessment and/or Data Protection Impact Assessment undertaken by the Code Compliance Officer;

(i) where relevant, the outcome of any Party and Other User impact assessment undertaken by the Party or Other User; and

(j) where relevant, a summary of any input given by other Electricity Industry Arrangement managers.

20 Industry consultation

20.1. The Code Manager shall publish the Preliminary Modification Report for each Modification Proposal and consult with Parties and Other Users, the DSP and Code Compliance Officer and other interested persons regarding such report in accordance with the applicable Modification Proposal Plan.

20.2. Following such consultation, the Code Manager shall produce an updated version of the Preliminary Modification Report (referred to as the Final Modification Report) which covers those matters required to be covered in the Preliminary Modification Report, and also reports on the outcome of the consultation, setting out a summary of the consultation submissions and the Code Manager's response to such submissions.

21 Determination by the Panel

21.1. In respect of each Final Modification Report, the Code Manager shall arrange for the relevant Panel to determine whether to approve the Modification Proposal. Modification Proposals that are not approved are deemed rejected, unless the Panel defers its decision pending any further analysis, impact assessment and/or consultation.

21.2. The relevant Panel shall make its determination in respect of each Modification Proposal based on whether:

(a) in the case of Commission-Approved Modifications, the approval of the Modification Proposal would better facilitate the Code Objectives than not approving the Modification Proposal; or

(b) in the case of Self-Governance Modifications, the business case for approving the Modification Proposal (which may or may not specifically refer to the Code Objectives) has been made.

21.3. The relevant Panel must record the outcome of its determination (based on the criteria above), and (if applicable) the reasoning for its divergence from the Code Manager's recommendation.

21.4. Decisions of the Panel shall be made by a simple majority vote.

22 Approval or rejection of a Modification Proposal

22.1. The effect of the determination under Clause 21 in respect of each Modification Proposal shall be (unless Clause 4.5 applies):

(a) in the case of Commission-Approved Modifications, a recommendation to the Commission that the Modification Proposal be approved or rejected; or

(b) in the case of Self-Governance Modifications, to approve or reject the Modification Proposal (subject to appeals under Clause 23).

22.2. In the case of each Commission-Approved Modification, the Commission will determine whether to approve or reject the Modification Proposal.

22.3. If the Commission considers that it is unable to form an opinion in relation to the approval or rejection of an Commission-Approved Modification, the Commission may issue a direction to the Panel specifying any additional steps that the Commission requires in order to form such an opinion (including drafting or amending the proposed legal text, revising the proposed implementation timetable, and/or revising or providing additional analysis and/or information). Where the Commission issues a direction to the Panel pursuant to this Clause 22.3:

(a) the vote under Clause 21 shall be null and void;

(b) the Panel shall (in accordance with any directions given by the Commission) determine the additional steps to be undertaken and the timetable for those steps; and

(c) the Code Manager shall update the Change Register, and progress the Modification Proposal in accordance with the Panel's determination.

23 Appeal of Self-Governance Modifications

23.1. Any Party or Other User materially impacted by the outcome of the decision under Clause 22 in respect of a Self-Governance Modification, may (within 10 Working Days following the notification of that decision) appeal the decision to the Panel, providing such any evidence and additional information not previously considered when the Panel made its decision.

23.2. Where the Panel delegates to a Sub-Committee, if the decision under Clause 22 in respect of a Self-Governance Modification differs from the recommendation of the Code Manager, then the decision will automatically be referred to the Panel, unless the Code Manager considers that the reasons provided by the relevant Panel are of themselves sufficient for it to change its own recommendation. In such cases, the revision to the recommendation and specifically the reasons for it will be recorded by the Code Manager.

23.3. For each decision appealed to the Panel under Clause 23.1, the Panel will then determine whether to approve or reject the Modification Proposal. Accordingly, where the Panel's determination is that the Modification Proposal is to be rejected (where it has previously been approved) the Modification Proposal shall be cancelled and not implemented (or, if already implemented, shall be reversed).

23.4. The Panel may, in respect of appeals under this Clause 23:

(a) dismiss the appeal if it is brought for reasons that are trivial or vexatious, or has no reasonable prospect of success; or

(b) send the Modification Proposal to a Sub-Committee if the Panel considers that it is unable to form an opinion in relation to the approval or rejection of the Modification Proposal.

24 Housekeeping Modification Proposals

24.1. A Housekeeping Modification Proposal can only be used to correct an error, inconsistency or factual change, including:

(a) updating names, addresses (including email addresses) listed in this Code;

(b) correcting minor typographical or grammatical errors;

(c) correcting formatting and consistency errors, such as Clause or Clause numbering; or

(d) updating out of date references to other documents or Clauses.

24.2. The Code Manager will follow a process for Housekeeping Modifications that is particular to its requirements, and in accordance with the following four-stage process (which applies instead of the process described elsewhere in this Code Schedule):

(a) acceptance of the Housekeeping Modification Proposal;

(b) assessment of the Housekeeping Modification Proposal;

(c) production of the Housekeeping Final Modification Report; and

(d) approval or rejection of the Housekeeping Modification Proposal.

Acceptance

24.3. Any Party or Other User may submit a Housekeeping Modification Proposal.

24.4. The Code Manager may refuse to accept the Housekeeping Modification Proposal, if the Code Manager considers that:

(a) the proposal is incomplete or insufficiently clear; or

(b) the proposal does not meet the criteria set out in Clause 24.1.

24.5. If the Code Manager decides that the scope of the Housekeeping Modification Proposal goes beyond the criteria set out in Clause 24.1, then it will re-consider acceptance and progression of the Modification Proposal (as a non-Housekeeping Modification Proposal), in accordance with Clause 8.

24.6. If the Code Manager refuses to accept submission of a Housekeeping Modification Proposal it shall write to the Proposer, setting out the reasons for refusal and offering assistance (where reasonably practicable) to address the reasons given (such that the proposal could be re-submitted).

Assessment

24.7. An assessment will be carried out by the Code Manager, who will assess the impacted products and re-confirm the suitability of the submitted Housekeeping Modification Proposal to be a Housekeeping Modification Proposal.

24.8. Housekeeping Modification Proposals will follow the Housekeeping Modification Path.

24.9. The Code Manager will determine Housekeeping Modification Proposals. If the Code Manager's determination is appealed, then the Panel will be the Panel to determine the Housekeeping Modification Proposal.

Housekeeping Modification Report

24.10. The Code Manager will prepare a written report on the Housekeeping Modification Proposal (referred to as the Housekeeping Modification Report).

24.11. The Housekeeping Modification Report will set out:

(a) description of the Housekeeping Modification Proposal;

(b) the proposed legal text to change this Code in order to give effect to the Housekeeping Modification Proposal;

(c) the proposed implementation date of this Housekeeping Modification Proposal; and

(d) the Code Manager's recommendation as to whether or not the Housekeeping Modification Proposal should be approved.

Industry Consultation

24.12. The Code Manager shall publish the Housekeeping Modification Report on the Code Website and clearly state the Objection Deadline by which objections shall be made, which shall be no more than 20 Working Days from publication. The publication will allow

Parties and Other Users, the DSP and the Code Compliance Officer and other materially impacted persons to review the proposed Housekeeping Modification Proposal, and if necessary, raise an objection to the change being made under this Clause 24. The Code Manager will not decide on a Housekeeping Modification Proposal if (before the Deadline) one or more objections is raised by a Party of Other User, the DSP, the Code Compliance Officer, the Competition and Consumer Protection Commission, the Data Protection Commission or the Commission.

Determination by the Code Manager

24.13. The Code Manager shall determine if the Housekeeping Modification Proposal shall be approved based on the business case for approving the Housekeeping Modification Proposal (which may or may not specifically refer to the Code Objectives).

24.14. If one or more objections is received as referred to in Clause 24.12, or the Code Manager does not approve the Housekeeping Modification, then the Housekeeping Modification Proposal will be rejected, and the Code Manager may consider whether the change should be accepted as a standard Modification Proposal as described in Clause 8.

24.15. The Code Manager shall within 1 Working Day after it has made its determination, update the Housekeeping Modification Report (recording its decision) and send this to the Commission, Panel, each Party and Other User and publish it on the Code Website .

24.16. Approved Housekeeping Modification Proposals shall be implemented by the Code Manager in the next scheduled release under Clause 24.

25 Implementation

25.1. Modification Proposals that are approved in accordance with Clauses 21 and 22 (or in accordance with another Electricity Industry Arrangement where Clause 4.5 applies) shall be implemented by the Code Manager.

25.2. The Code Manager shall establish release dates for the approved Modification Proposals in accordance with the implementation dates approved as part of the Modification Proposal.

25.3. These release dates will be consistent with, but not necessarily be limited to, any scheduled release dates of revisions to the DSP's Systems. Changes to this Code which are unrelated to System changes may be made independently of System update release dates, but (for example) to coincide with the beginning of the financial year or a deadline imposed by impending regulations.

25.4. The implementation of changes to this Code that necessitate System changes shall be subject to successful testing of those System changes.

25.5. The implementation dates approved as part of the Modification Proposal can only be changed via a further Modification Proposal or via direction of the Panel (for Self-Governance Modifications and Housekeeping Modifications) and the Commission (for Commission-Approved Modifications), and subject to the normal requirements with respect to impact assessments, etc.

26 Release Management

26.1. The Code Manager shall set out a Release Plan for each release date which will detail, as a minimum:

(a) the plan for making updates to this Code as a result of Modification Proposals approved for that release date, including details of when pre-release information will be published;

(b) where changes are required to DSP systems, details of the DSP Test Plan set out by the DSP, including details of relevant DSP Test Phases and planned interactions with Parties and Other Users;

(c) a plan for the implementation of any mitigating actions identified by the Data Protection Impact Assessment in relation to the Modification Proposal conducted by the Code Compliance Officer, as approved by the Panel;

(d) where changes are required to systems maintained by the Code Manager (such as the Code Website), details of the Test Plan set out by the Code Manager, including details of relevant Test Phases and planned interactions with Parties and Other Users of those systems;

(e) details of any new training or guidance requirements identified and the plan for delivery; and

(f) details of any planned communications and engagement with impacted Parties and Other Users to support the delivery of the Release Plan.

26.2. The DSP shall provide all relevant information required by the Code Manager to produce and publish the Release Plan. This includes:

(a) the DSP's plan for the design, build and testing of any changes to its Systems;

(b) the DSP's plan (referred to as a DSP Test Plan) detailing the proposed activities in testing and implementing changes to its Systems, including:

(i) Required DSP Test Phases and Test Environments;

(ii) planned timescales and schedules for each DSP Test Phase;

(iii) where relevant, confirmation that the plan aligns with the Code Test Strategy set out by the Code Manager;

(iv) entry and exit criteria for each DSP Test Phase;

(v) the approach to the use of Test Data in each DSP Test Phase;

(vi) details of key personnel relevant to the plan and associated roles and responsibilities;

(vii) any risks, issues, assumptions or dependencies identified in the development of the plan; and

(viii) the approach to managing defects identified in testing including associated acceptance criteria for resolving defects; and

(c) details of any restricted or confidential information in the DSP Test Plan that should not be shared with Parties and Other Users as part of the Release Plan.

26.3. The DSP shall take reasonable steps to deliver changes to its systems and processes in accordance with the Release Plan and shall notify the Code Manager, in a timely manner, of any risks, issues or dependencies that may impact its ability to deliver in accordance with the Release Plan.

26.4. The Code Manager shall publish the Release Plan (and any subsequent updates to that Release Plan) on the Code Website.

26.5. Where a Modification Proposal is approved for implementation on a date for which a Release Plan has already been published by the Code Manager, the Code Manager shall update the Release Plan and publish the updated version on the Code Website.

27 Data Access Register Changes

27.1. The Code Manager shall publish a timetable for the submission, approval and implementation (DAR Release) of DAR Changes.

Submitting a DAR Change Proposal

27.2. The Code Manager, DSP and any Party or Other User may submit a DAR Change Proposal. Such submission should be made using the submission form published by the Code Manager on the Code Website.

Acceptance of a DAR Change Proposal

27.3. Upon receipt of a DAR Change Proposal, the Code Manager shall review the DAR Change Proposal and, within 5 Working Days either:

(a) where the request is incomplete, insufficiently clear or outside the scope of a DAR Change Proposal, reject the DAR Change Proposal; or

(b) accept the DAR Change Proposal.

27.4. Where the Code Manager rejects a DAR Change Proposal, they may request additional

information or supporting information required for this to be accepted and may accept the DAR Change Proposal on receipt of an updated submission.

Preliminary DAR Change Proposal Report and Consultation

27.5. The Code Manager shall publish the Preliminary DAR Change Proposal Report for each DAR Change Proposal and consult with Users, the DSP and Code Compliance Officer and other interested persons.

Provisional DAR Change Proposal Report and SSC Minded-to Opinion

27.6. Following such consultation, the Code Manager shall produce an updated version of the Preliminary DAR Change Proposal Report (referred to as the Provisional DAR Change Proposal Report) which covers those matters required to be covered in the Preliminary DAR Change Proposal Report, and also reports on the outcome of the consultation, setting out a summary of the consultation submissions and the Code Manager's response to such submissions.

27.7. In respect of each Provisional DAR Change Proposal Report, the Code Manager shall arrange for the Security Sub-Committee at its next scheduled meeting to determine its minded-to view on whether each DAR Change Proposal should be approved for implementation or rejected.

Ad-Hoc Assessment for a new User Category

27.8. Where the Security Sub-Committee is minded-to approve a DAR Change Proposal that creates a new User Category, the Code Manager will advise the Code Compliance Officer which shall conduct an Ad-Hoc Assessment on the Party, Parties and Other User(s) within the User Category seeking to access the Smart Meter Data System, in accordance with the process in Clause 3 of Schedule 2: Access Arrangements.

Data Protection Impact Assessment

27.9. The Security Sub-Committee may instruct the Code Compliance Officer to conduct a Data Protection Impact Assessment on implications of the DAR Change Proposal for access to Smart Meter Data, in accordance with Clause 3.13 of Schedule 2: Access Arrangements.

Determination by the Security Sub-Committee

27.10. Following 27.8 and/or 27.9, the Code Manager shall produce an updated version of the Provisional DAR Change Proposal Report (referred to as the Final DAR Change Proposal Report) which covers those matters required to be covered in the Provisional DAR Change Report, and also reports on the outcome of 27.8 and/or 27.9, as applicable, setting out a summary of the Code Compliance Officer’s findings.

27.11. In respect of each Final DAR Change Proposal Report, the Code Manager shall arrange for the Security Sub-Committee to determine whether to approve the DAR Change Proposal. DAR Change Proposals that are not approved are deemed rejected.

27.12. DAR Change Proposals approved by the Security Sub-Committee shall be implemented by the Code Manager in the next scheduled DAR Release, unless another more suitable date is agreed by the Security Sub-Committee.

27.13. The Code Manager will notify Parties and Other Users of approved DAR Change Proposal.

Adding or Removing Data Items from the Data Access Register

27.14. Where a DAR Change Proposal, that either adds or removes a Data Item, is approved, the Code Manager shall, in accordance with the release date agreed by the Security Sub-Committee under 27.12:

(a) update its Data Access Register detailing access to the relevant Data Items;

(b) update its Data Glossary under Appendix 1 with the relevant Data Items; and

(c) notify the DSP, which shall update its Data Dictionary with the relevant Data Item(s) and provide access to the appropriate Parties and Other Users on the Smart Meter Data System as per Section 12 of the Main Body.

Adding a new User Category

27.15. Where a DAR Change Proposal that introduces a new User Category is approved, the Code Manager, with input from the Code Compliance Officer and DSP as may be required, shall:

(a) Develop the proposed criteria to be used in assessing an application to become a user for the new User Category in accordance with Clause 7 of Schedule 2: Access Arrangements;

(b) Identify the purpose for which Parties and Other Users in this new category should be entitled to access and use the Data;

(c) Identify the Data Items that the new User Category should be entitled to access, including, as applicable, Personal Data and Anonymous Data; and

(d) Develop the proposed approach for delivering assurance to mitigate risks relating to information security and data protection for this new category.

27.16. Where a DAR Change Proposal, that adds a new User Category, is approved, the Code Manager shall, in accordance with the DAR release date agreed by the Security Sub-Committee under 27.12:

(a) add the new User Category to the Data Access Register; and

(b) notify the DSP, which shall provide access to the appropriate Parties and Other User(s) on the Smart Meter Data System, as per Section 12 of the Main Body.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Schedule 10:
Security Sub-Committee

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Schedule 10: Security Sub-Committee

Version n.n

DD Month YYYY

DOCUMENT HISTORY

Modification Proposals included in this version	Modification Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD Mon YYYY		n.n

1 Definitions

Term	Acronym	Definition
Ad-Hoc Assessment		Means an assessment on a user which may be conducted on an ad-hoc basis by the Code Compliance Officer in accordance with Schedule 6: Assessments, such as with respect to: a) a risk with respect to a particular user or type of Processing activity is discovered by the Panel; b) following a Security Incident or Event of Breach that affects a particular user; and/or c) where a new User Category or Data Item is issued.
Annual Self-Assessment		Means a self-assessment questionnaire issued to all users on an annual basis to identify the extent to which, since the last occasion on which a Self-Assessment was carried out in respect of that Other User or Party, there has been any Material Change in the arrangements that the Other User has in place to comply with its obligations under the Code or in the quantity of Consumption Data being accessed by the Other User or Party.
Assessment Report		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.
Assessment Response		Has the meaning given to that expression in Clause 3.5 of Schedule 6: Assessments.
Assurance Status		Has the meaning given to that expression in Clause 3.9 of Schedule 6: Assessments.
Change Proposal	CP	Means a proposal to change a subsidiary document to the Code

Term	Acronym	Definition
		and Schedules, in accordance with Schedule 9: Change Management.
Code, Smart Meter Data Access Code		Means this Smart Meter Data Access Code, including all of the Schedules and Appendices as amended from time to time or otherwise modified in accordance with the Code.
Code Compliance Officer	CCO	Means the responsible authority or delegated authority with responsibility for the maintenance of all Code Compliance and assurance documentation and provisions.
Code Manager		Means the natural or legal person with responsibility for the governance, maintenance and operation of this Code. Clause 10 of the Main Body sets out the tasks and functions of the Code Manager.
Commission, Commission for Regulation of Utilities	CRU	Means the Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Data		Means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Data Protection Commission	DPC	Means the commissioner as defined in the Data Protection Legislation.
Data Protection Impact Assessment	DPIA	Has the meaning as defined in Data Protection Legislation.
Data System Provider	DSP	Means the legal entity responsible for the maintenance and administration of the Smart Meter Data System, in accordance with Clause 12 of the Main Body.

Term	Acronym	Definition
Department		Means the Department of the Environment, Climate and Communications within the Republic of Ireland.
Dispute		Means any dispute or difference (of whatever nature) arising under, out of or in connection with this Code and/or any bilateral agreement.
Distribution System Operator	DSO	Means the legal entity holding the Distribution System Operator Licence.
Elected Member		Has the meaning given to that expression in Clause 3.3 of Schedule 7: Panel.
Entry Assessment		Means an assessment conducted on all Applicants or user prior to entry into the Code or on signing an access agreement (in the case of Other Users) as further described in Schedule 6: Assessments.
Event of Breach		Has the meaning given to that expression in Clause 21 of the Main Body.
Final Customer		Means a natural or legal person who receives, or wishes to receive, a supply of energy at any premises in the Republic of Ireland, in accordance with Statutory Instrument (SI) 37 of 2022.
Good Industry Practice		Means, in respect of a person, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced organisation engaged in a similar type of undertaking as that person under the same or similar circumstances, complying with all applicable laws, codes of professional conduct, relevant codes of practice, Irish, European and other relevant standards.

Term	Acronym	Definition
Licence		The Licence granted by the Commission to the DSO / Electricity Suppliers under the Electricity Regulation Act, 1999.
Major Security Incident		Means, in relation to any System or Smart Meter Data, any event which results, or was capable of resulting, in that System or Smart Meter Data being Compromised to a material extent.
Material Change, Materially Changed		Means a change to a Party's Systems or processes which is of such a type or magnitude as to raise the reasonable expectation of an impact on that Party's ability to meet its obligations under this Code.
Modification Proposal		Means the term applied to a Modification proposed in accordance with Clause 15 of the Main Body and Schedule 9: Change Management.
Modification Report		Has the meaning given to that expression in Schedule 9: Change Management.
National Smart Metering Programme	NSMP	Means the National Smart Metering Programme within the Republic of Ireland.
Other User(s)		A natural or legal person that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Party.
Panel		Means the body established as such in accordance with Clause 8 of the Main Body.
Panel Chair		Has the meaning given to that expression in Clause 3.1 of Schedule 7: Panel.
Panel Member		Has the meaning given to that expression in Clause 8.8 of the Main Body.

Term	Acronym	Definition
Party		A natural or legal person that has agreed to be bound by this Code (pursuant to the Accession Agreement) and that has not ceased to be bound by the Code.
Personal Data Breach		Has the meaning as defined in Data Protection Legislation.
Privacy Controls Framework	PCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Remedial Plan		Means a document describing how a failure to comply with this Code will be remedied by the Party or Other User in question, and how the risk of future failures is to be mitigated.
Risk Treatment Plan		Has the meaning given to that expression in Clause 6.2(d) of Schedule 10: Security Sub-Committee.
Schedule		Means a Schedule to this Code.
Secretariat		Means the allocated role to perform those tasks and functions expressly ascribed to it under the Code and any other tasks and functions as the Panel may assign to the Secretariat from time to time.
Security Controls Framework	SCF	Means the document of that name developed and maintained by the Panel in accordance with Schedule 7: Panel.
Security Incident		Means an actual or potential impact on the confidentiality, integrity or availability of Smart Meter Data or a System.
Security Risk Register		Means a register of data protection and information security risks in relation to the Smart Meter Data System and related Systems, maintained by the Security Sub-Committee.

Term	Acronym	Definition
Security Sub-Committee	SSC	Means the Sub-Committee established in accordance with Clause 9.2 of the Main Body.
Security Sub-Committee Chair		Has the meaning given to that expression in Clause 4.3 of Schedule 10: Security Sub-Committee.
Security Sub-Committee (Supplier) Member		Has the meaning given to that expression in Clause 4.6 of Schedule 10: Security Sub-Committee.
Security Sub-Committee Member		Has the meaning given to that expression in Clause 4.1 of Schedule 10: Security Sub-Committee.
Security Sub-Committee Terms of Reference		Means the terms of reference according to which the Security Sub-Committee shall be formed and shall operate.
Smart Meter Data System		Means the infrastructure and hub operated by the Data System Provider, and all interfaces, including portals or interfaces to allow Final Customers access to Smart Meter Data and any other Data associated with the Smart Meter.
Sub-Committee		Means a Sub-Committee of the Panel established from time to time in accordance with Schedule 9: Panel.
System(s)		Means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith.
Test, Testing		Means carrying out the activities defined in the Test Strategy and/or Test Plan.

Term	Acronym	Definition
Working Day(s)	WD	Means any day other than a Saturday, a Sunday, Christmas Day, St. Patrick's Day, or a day that is a public holiday within Schedule 2 of the Organisation of Working Time Act, 1997.
Working Group		Means a group of persons, established by the Panel, for the purposes set out in Schedule 7: Panel and Schedule 9: Change Management.

2 Introduction

2.1. This Schedule sets out the establishment, membership proceedings and duties and powers of the Security Sub-Committee.

3 Establishment of the Security Sub-Committee

3.1. The Panel shall establish a Sub-Committee in accordance with the requirements of this Schedule, to be known as the Security Sub-Committee, which shall act on behalf of the Panel.

3.2. Save as expressly set out in this Schedule, the Security Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Clause 9 of the Main Body.

4 Membership of the Security Sub-Committee

4.1. The Security Sub-Committee shall be composed of the following persons (each a Security Sub- Committee Member):

(a) the Security Sub-Committee Chair (as further described in Clause 4.3);

(b) Two (2) Security Sub-Committee (Supplier) Members (as further described in Clause 4.6);

(c) a representative of the DSO (as further described in Clause 4.7);

(d) a representative of the SMO (as further described in Clause 4.7); and

(e) a representative of the TSO (as further described in Clause 4.7).

4.2. Each Security Sub-Committee Member must be an individual (and cannot be a body

corporate, association or partnership). No one person can hold more than one office as a Security Sub-Committee Member at the same time.

Security Sub-Committee Chair

4.3. The Security Sub-Committee Chair shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party, Other User or class of Parties or Other Users;

(b) the Security Sub-Committee Chair is appointed for a three-year term (following which they can apply to be re-appointed);

(c) the Security Sub-Committee Chair is remunerated at a rate to be determined by the Commission;

(d) the Security Sub-Committee Chair's appointment is subject to Clause 9.9 of the Main Body, and to terms equivalent to Clause 8.10 of the Main Body;

(e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of their term of office in the event of any delay in appointing their successor; and

(f) where the Security Sub-Committee Chair's appointment (and for the purposes of this Clause and Clause 4.4 all references to appointment shall encompass re-appointment) is to take effect on or after the date this Clause 4.3 comes into force, the Panel shall:

(i) notify the Commission of the appointment it proposes to make;

(ii) not make the appointment unless and until the Commission has confirmed in writing that they do not object to the appointment being made; and

(iii) ensure that the terms of the appointment include terms which provide for the Panel to terminate the appointment where directed to do so by the Commission pursuant to Clause 4.4 and from such date or within such period as may be specified in the Commission's direction.

4.4. The Commission may, in respect of any Security Sub-Committee Chair appointment which takes effect on or after the date Clause 4.3(f) comes into force, direct the Panel to terminate the appointment of the Security Sub-Committee Chair where the Commission considers it necessary to do for the purposes of preserving the integrity of, and in the interests of maintaining, the security of the NSMP.

Security Sub-Committee (Supplier) Members

4.5. Each of the Security Sub-Committee (Supplier) Members shall (subject to any directions to the contrary made by the Commission for the purpose of transition on the incorporation of this Schedule into this Code):

(a) be appointed in accordance with Clause 4.6, subject to compliance by the appointed person with Clause 9.9 of the Main Body;

(b) retire two years after their appointment (without prejudice to their ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Clause 8.10 of the Main Body for which the purpose of those Clauses shall be read as if references to "Elected Member" were to "Security Sub-Committee (Supplier) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

4.6. Each of the Security Sub-Committee (Supplier) Members shall (subject to Clause 4.7) be appointed in accordance with a process that is otherwise the same as that by which Elected Members are elected under Annex 1 of Schedule 7: Panel (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Schedule 7: Panel were to the corresponding provisions set out in or applied pursuant to this Clause.

Security Sub-Committee (DSO, SMO & TSO) Members

4.7. Each of:

(a) the DSO;

(b) the SMO; and

(c) the TSO,

may nominate one person to be a Security Sub-Committee Member by notice to the Code Manager from time to time. The each may replace its nominee from time to time by prior notice to the Code Manager. Such nomination or replacement shall be subject to compliance by the relevant person with Clause 9.9 of the Main Body.

Membership Requirements

4.8. The following shall apply in respect of all candidates nominated or re-nominated for election as a Security Sub-Committee (Supplier) Member:

(a) the Security Sub-Committee may, by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations, reject a candidate (by notifying the candidate of such rejection) where the Security Sub-Committee determines that the candidate does not satisfy one or more of the following requirements:

(i) the candidate must have been nominated by a company or other organisation, and the individual who submitted the nomination on behalf of the organisation must hold a senior position within the organisation;

(ii) the organisation which nominated the candidate must have confirmed that it is satisfied that the candidate has the relevant security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated; and

(iii) the candidate must have sufficient security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;

(b) a candidate who is rejected under 3.8(a) above shall not (subject to 3.8(c) below) be an eligible candidate for the relevant election;

(c) where a candidate Disputes a rejection notification under 3.8(a), the candidate shall have 3 Working Days following receipt of such notification to refer the matter to the Panel for its final determination of whether the candidate satisfies the requirements set out in 3.8(a); and

(d) where necessary, the Code Manager shall delay giving notice of the names of eligible candidates pending expiry of the time periods set out in 3.8(a) and/or (c) or determination by the Panel under 3.8(c) (as applicable).

5 Proceedings of the Security Sub-Committee

5.1. Without prejudice to the generality of Clause 3 of Schedule 7: Panel as it applies pursuant to Clause 5.2:

(a) a representative of the Department, a representative of the Commission, a representative of the DSP and a representative of the Code Manager (separate from the Secretariat function) shall be:

(i) invited to attend each and every Security Sub-Committee meeting;

(ii) entitled to speak at such Security Sub-Committee meetings without the permission of the Security Sub-Committee Chair; and

(iii) provided with copies of all the agenda and supporting papers available to Security Sub- Committee Members in respect of such meetings; and

(b) the Security Sub-Committee Chair shall invite to attend Security Sub-Committee meetings the Code Compliance Officer, and any other persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters.

5.2. Subject to Clause 5.1, the provisions of Clause 9 of the Main Body shall apply to the proceedings of the Security Sub-Committee, for which purpose that this Clause shall be read as if references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

6 Duties and Power of the Security Sub-Committee

6.1. The Security Sub-Committee shall perform:

(a) the duties and may exercise the powers set out in Clauses 6.2 to 6.8; and

(b) such other duties and may exercise such other powers as may be expressly ascribed to the Security Sub-Committee elsewhere in this Code.

Document Development and Maintenance

6.2. The Security Sub-Committee shall:

(a) develop and maintain documents, to be known as the "Security Controls Framework", and a “Privacy Controls Framework” which shall:

(i) set out the appropriate Entry Assessment, Annual Self-Assessment and Ad-Hoc Assessment methodology to be applied to different categories of privacy and security assessments carried out in accordance with Clause 7 of the Main Body, Schedule 4: Data Security and Schedule 5: Data Privacy and be designed to ensure:

(A) that such assessments are proportionate and achieve appropriate levels of assurance in respect of different User Categories and the DSP;

(B) the establishment of the principles and criteria to be applied in the carrying out of any assessment, including principles designed to ensure that assessments take place on a consistent basis across all Parties, Other Users and the DSP;

(C) the provision for determining the timing and frequency of assessments;

(ii) establish examples of evidence for a user to demonstrate procedures required under Schedule 4: Data Security and Schedule 5: Data Privacy, in accordance with Good Industry Practice.

(b) maintain a Security Risk Register, and:

(i) review the Security Risk Register on an annual basis to Identify any new or changed security or privacy risks to the Smart Meter Data System; and

(ii) review the risk register in any event promptly if the Security Sub-Committee considers there to be any Material Change in the level of security or privacy risk(s); and

(iii) consider and update the Security Risk Register with any risks identified by a Data Protection Impact Assessment conducted by the Code Compliance Officer.

(c) ensure that it identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Register; and

(d) develop and maintain a document to be known as the "Risk Treatment Plan", which shall identify the residual security and privacy risks which in the opinion of the Security Sub-Committee remain unmitigated, taking into account the security controls that are in place.

Security Assurance

6.3. The Security Sub-Committee shall:

(a) periodically, and in any event at least once each year, review the requirements and arrangements within Schedule 4: Data Security and Schedule 5: Data Privacy in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;

(b) exercise such functions as are allocated to by the Panel, and comply with the applicable requirements of Schedule 6: Assessments;

(c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of Schedule 4: Data Security and Schedule 5: Data Privacy;

(d) following the Security Sub-Committee's receipt of the Assessment Report and Assessment Response, promptly consider both documents and (having regard to any advice of the Code Compliance Officer) set the Assurance Status of the Party, in relation to its compliance with each of its obligations under Schedule 4: Data Security and Schedule 5: Data Privacy;

(e) consider, and as appropriate, approve any recommendations from the Code Compliance Officer in its Assessment Report or otherwise in relation to a Remedial Plan following an Entry Assessment, Annual Self-Assessment or Ad-Hoc Assessment;

(f) provide advice to the Panel on the security arrangements in place in relation to the design, building and Testing of the Smart Meter Data System;

(g) where the Security Sub-Committee considers that actual non-compliance of a Code Party, Other User or the DSP has occurred with respect to any of the obligations has occurred under Schedule 4: Data Security or Schedule 5: Data Privacy of the Code, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Breach;

(h) provide advice to the Commission in relation to the appointment of the Code Compliance Officer, monitor the performance of the person appointed to that role and provide advice to the Commission in respect of its views as to that performance; and

(i) consider the outcomes and any mitigating actions of a Data Protection Impact Assessment conducted by the Code Compliance Officer, and make recommendations to the Panel.

Security Assurance

6.4. The Security Sub-Committee shall:

(a) provide such reasonable assistance to the Panel as may be requested by them in relation to the causes and management of Security Incidents, including Personal Data Breaches, in accordance with Clauses 6.9 to 6.14;

(b) provide such reasonable assistance to the DSP, Parties and Other Users as may be requested by them in relation to the causes of Security Incidents, including Personal Data Breaches, and the management of vulnerabilities on their Systems;

(c) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to obligations under Schedule 4: Data Security and Schedule 5: Data Privacy, including through attaining the support and advice of the Code Compliance Officer, as appropriate;

(d) provide the Panel and any relevant Sub-Committee with support and advice in relation to any Change Proposal or Modification Proposal which may affect the security of the Smart Meter Data System, or the effective implementation of the security and privacy controls that are identified in Schedule 4: Data Security and Schedule 5: Data Privacy;

(e) advise the Commission of any modifications to the conditions of Licences which it considers may be appropriate having regard to the residual security risks identified from time to time in the Risk Treatment Plan;

(f) respond to any consultations on matters which may affect the security of the Smart Meter Data System or the effective implementation of the security and privacy controls that are identified in Schedule 4: Data Security and Schedule 5: Data Privacy;

(g) provide such further support and advice to the Panel as it may request; and

(h) provide the Commission with such information and documents as it may reasonably request in relation to any matter referred by a Code Party to the Commission for determination.

Modifications

6.5. The Security Sub-Committee shall establish a process under which the Code Manager monitors Change Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:

(a) are likely to affect the requirements of Schedule 4: Data Security and/or Schedule 5: Data Privacy; or

(b) are likely to relate to other parts of the Code but may have a material effect on the security of the Smart Meter Data System,

and the Code Manager shall comply with such process.

6.6. Notwithstanding Schedule 9: Change Management:

(a) the Security Sub-Committee shall be entitled to submit Change Proposals and Modification Proposals in respect of obligations under Schedule 4: Data Security, Schedule 5: Data Privacy, Schedule 6: Assessments and Clause 7 of the Main Body, where the Security Sub-Committee considers it appropriate to do so; and

(b) any Security Sub-Committee Member shall be entitled to submit Change Proposals and Modification Proposals in respect of obligations under Schedule 4: Data Security, Schedule 5: Data Privacy and Clause 7 of the Main Body, where they consider it appropriate to do so (where the Security Sub-Committee has voted not to do so).

6.7. Notwithstanding and subject to the provisions of the Security Sub-Committee Terms of Reference, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

6.8. For the purposes of Schedule 9: Change Management:

(a) written representations in relation to the purpose and effect of a Modification Proposal may be made by:

(i) the Security Sub-Committee; and/or

(ii) any Security Sub-Committee Member (either alone or in addition to any representations made by other Security Sub-Committee Members and/or the Security Sub-Committee collectively); and

(b) notwithstanding Schedule 9: Change Management, the Code Manager shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.

Incident Management: Security Incidents and Personal Data Breaches

6.9. The Code Compliance Officer shall receive notification of a Security Incident or Personal Data Breach, in accordance with the procedures identified in Schedule 4: Data Security and Schedule 5: Data Privacy.

6.10. The Code Compliance Officer shall inform the Security Sub-Committee on receipt of a notification of a Security Incident or Personal Data Breach, in accordance with Clause 6.9.

6.11. The Security Sub-Committee shall request the opinion of the Code Compliance Officer on the severity of the Security Incident, which the Code Compliance Officer shall provide, with due consideration to:

(a) The volume of Systems, Data and/or individuals affected by the Security Incident;

(b) The categories of Data affected by the Security Incident;

(c) The potential level of risk faced by Parties, Other Users, Final Customers and other natural persons; and

(d) Any mitigating actions already in place with respect to the Security Incident.

6.12. Following the Code Compliance Officer's opinion on the severity of the Security Incident:

(a) The Security Sub-Committee and Code Compliance Officer, on behalf of the Panel, shall provide such reasonable assistance to the Panel as may be

requested by them in relation to the causes and management of the Security Incidents, including a Personal Data Breach.

(b) Where a Security Incident, which includes a Personal Data Breach, occurs, the Security Sub-Committee should notify the Panel and the Panel may contact the DPC for its opinion on any mitigating actions to be conducted as a result of the Personal Data Breach.

6.13. Security Incident or Personal Data Breach occurs, the Security Sub-Committee may request the opinion of the DSP as to any mitigating actions required to be conducted as a result of the Security Incident or Personal Data Breach.

6.14. Where a Security Incident or Personal Data Breach occurs, the Security Sub-Committee may request the Panel to notify impacted Parties, Other Users and/or Final Customers, at the recommendation of the Code Compliance Officer.

Major Security Incidents

6.15. Where the Code Compliance Officer receives notification that a Major Security Incident has occurred in accordance with the procedure identified in Schedule 4: Data Security, it shall notify the Security Sub-Committee.

6.16. The Code Compliance Officer and the DSP shall provide their opinions to the Security Sub-Committee on the severity of the Security Incident, which the Code Compliance Officer shall provide, with due consideration to:

(a) The volume of Systems, Data and/or individuals affected by the Security Incident;

(b) The categories of Data affected by the Security Incident;

(c) The potential level of risk faced by Parties, Other Users, Final Customers and other natural persons; and

(d) Any mitigating actions already in place with respect to the Security Incident.

6.17. The Security Sub-Committee shall, on behalf of the Panel:

(a) Provide its opinion as to any mitigating actions required to be conducted as a result of the Major Security Incident, including through consultation with the Code Compliance Officer and the DSP, as appropriate; and

(b) provide such reasonable assistance to the DSP, Parties and Other Users as may be requested by them in relation to the management of the Major Security Incident on their systems.

6.18. Where a Major Security Incident affects the Smart Meter Data System, the Code Compliance Officer and the DSP shall conduct the management of the Major Security Incident and any mitigating actions.

6.19. Where a Major Security Incident affects Systems other than the Smart Meter Data System, the Code Compliance Officer and the Code Manager shall conduct the management of the Major Security Incident and any mitigating actions.

Mitigating Actions

6.20. The Security Sub-Committee shall advise the Panel on any mitigating actions required as a result of the Security Incident, Personal Data Breach or Major Security Incident.

6.21. Following the receipt of the opinion of the Security Sub-Committee under Clause 6.17, the Panel shall require Parties, Other Users and/or the DSP, as appropriate, to give effect to any mitigating actions that it decides to be necessary.

6.22. The Code Compliance Officer shall ensure that it retains a log of any Security Incidents, including Personal Data Breaches, that have occurred, and the mitigating actions taken.

6.23. The DSP shall ensure that it retains a log of any Major Security Incidents that have occurred, and the mitigating actions taken.

6.24. The logs identified in Clauses 6.22 and 6.23 shall not be published or made publicly available.

6.25. The Code Compliance Officer shall maintain a framework methodology to be used to assess Security Incidents and determine appropriate mitigating actions, to be approved by the Security Sub-Committee.

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Smart Meter Data Access Code

Appendix 1: Data Dictionary

An Coimisiún um Rialáil Fóntas
Commission for Regulation of Utilities

Contents

Appendix 1: Data Glossary

Version 0.1

DD Month YYYY

DOCUMENT HISTORY

Change Proposals included in this version	Change Proposal effective Date	Schedule Clauses Modified	Schedule Version if applicable
	DD-Mon-YY		n.n

1 General Interpretation

1.1. This Appendix sets out the Data Glossary, which provides a list of, and relevant information on, the Data Items available on the Smart Meter Data System. This Data Glossary also includes consideration of whether each Data Item constitutes, or may constitute, Personal Data, in accordance with the definitions within Schedule 1: Interpretations.

1.2. All other definitions shall be provided within Schedule 1: Interpretations.

1.3. Personal Data shall have the meaning provided within Data Protection Legislation, as indicated within Schedule 1: Interpretations. As such, any Data Item relating to an identified or identifiable natural person, including a Final Customer, who can be identified, directly or indirectly, in particular by reference to an identifier, can be considered Personal Data.

1.4. The consideration of whether a Data Item is Personal Data shall be central to consideration of the appropriate Legal Basis required for a Code Party or Other User to access the Data Item, in accordance with Clause 5.4 of Schedule 2: Access Arrangements and Clauses and Clauses 6.2 and 6.3 of Schedule 5: Data Privacy.

1.5. The consideration of whether the Data Items indicated in the table in Clause 2 of this Appendix constitute Personal Data is not simply a consideration of whether such Data Items shall constitute identifiers such as a Final Customer's full name, postal address, IP address, MPRN or meter serial number. Data Items considered Personal Data will often be broader than simply personal identifiers, in accordance with the definition within Schedule 1 and as provided by Data Protection Legislation. As such, the determination of whether the Data Items constitute Personal Data shall always be made with consideration towards:

(a) whether the Data Controller or Data Processor Processing the relevant Data Item is capable, using the means likely reasonably to be used and the information available to them, of identifying a Final Customer or other Data Subject;

(b) whether the Data Controller or Data Processor Processing the relevant Data Item is likely to be Processing the Data Items in combination with other information, including identifiers specific to a Final Customer;

(c) whether the Data Item is likely to be used Data Controller or Data Processor Processing the relevant Data Item for the treatment or evaluation of Final Customers or other Data Subjects on an individual basis (such as for billing purpose, providing Final Customer-specific services and tariffs, etc.).

In particular, in most cases, Data Items Processed by a Party or Other User from the Smart Meter Data System are likely to be Processed in combination with other Data Items, including personal identifiers, from the Smart Meter Data System.

1.6. Other Data Items, including information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic) will not be considered Personal Data unless otherwise indicated by this Data Glossary.

1.7. Data Items may be accessed in a format without any connection to individual identifiers or the possibility of Final Customer identification, such as through a request for bulk or Anonymous Data, in accordance with Clause 3.12 of Schedule 2: Access Arrangements. For example, this may be used to analyse trends in consumption data across at a county or national level. In such a case, the relevant Data items will not be considered Personal Data if provided in a bulk or Anonymous Data format, where re-identification is not considered possible in the format in which the Data Items are provided, notwithstanding the table in Clause 2 of this Appendix.

1.8. This Appendix shall be maintained and updated by the Code Manager as Data Items become available and as use cases for Data Items change, in accordance with Clause 27.14 of Schedule 9: Change Management.

2 Smart Meter Data

Term/Data Item	Identifier	Description	Personal Data? (*rationale*)
Interval Data	30-minute Interval Consumption Data - Active Import (kW)	This is the real power consumed from the grid at the premise measured in kiloWatts (kW). Interval Data is recorded and stored in every electricity smart meter (ESM) at 30-minute granularity.	Personal Data *Specific to a Final Customer's device or premise and likely to be used for the treatment of Final Customers on an individual basis*
	30-minute Interval Channel Consumption Data - Active Export (kW)	This is the real power exported to the grid from the premise measured in kiloWatts (kW). Customers with micro-generation equipment installed have the potential to export active energy to the grid. Interval Data is recorded and stored in every ESM at 30-minute granularity.	Personal Data *Specific to a Final Customer's device or premise and likely to be used for the treatment of Final Customers on an individual basis*
Register Data	24-hr Cumulative Active Import Register (KWh) with a snapshot	This is the energy consumed from the grid at the premise measured in kilowatt-hours (kWh). A snapshot of each of the Cumulative Registers is taken daily (at midnight) and monthly (on the first day of the month) and is stored on the ESM for up to 175 days (daily snapshots) or 36 iterations (monthly snapshots) in a first-in, first-out circular buffer	Personal Data *Specific to a Final Customer's device or premise and likely to be used for the treatment of Final Customers on an individual basis*
	24-hr Cumulative Active Export Register (KWh) with a snapshot taken each midnight Midnight Snapshot of	This is the energy exported to the grid from the premise measured in kilowatt-hours (kWh). Only customers with micro-generation equipment installed have the potential to export active energy to the grid.	Personal Data *Specific to a Final Customer's device or premise and likely to be used*

Term/Data Item	Identifier	Description	Personal Data? (*rationale*)
	Standard Smart Tariff (SST) Day / Peak / Night Import Register (KWh)		*for the treatment of Final Customers on an individual basis*
	24-hr Cumulative Active Import Register (KWh) with a snapshot	These are the midnight snapshots of the SST Registers required to deliver the Standard Smart Tariff (SST) and are recorded in every ESM each day. These Cumulative Active Import Registers only measure energy consumption during certain periods of the day as follows: • SST Night Import Register (KWh) from 11pm to 8am • SST Day Import Register (KWh) from 8am to 5pm and from 7pm to 11pm • SST Peak Import Register (KWh) from 5pm to 7pm	Personal Data *Specific to a Final Customer's device or premise and likely to be used for the treatment of Final Customers on an individual basis*

3 Final Customer Attributes Data

Term/Data Item	Identifier	Description	Personal Data? (*rationale*)
Communication Technical Feasible (CTF)	Communication Technical Feasible (CTF)	CTF is a measure of the reliability of communications from the smart meter to the head end system across the communications network	Non-Personal Data *Likely to be general information used across devices, rather than used to evaluate or treat a specific Final Customer*
DUoS Group		DUoS Group is a code which denotes the distribution use of system tariff applying to the MPRN.	Non-Personal Data *Likely to be general information used across devices, rather than used to*

Term/Data Item	Identifier	Description	Personal Data? (*rationale*)
			evaluate or treat a specific Final Customer
MPRN		Meter Point Registration Number. This is the unique identifier for each Service Delivery Point on the network. It applies to each service delivery point where there is a Connection Agreement between the Distribution System Operator (Networks) and a customer or generator. In most cases, this is the point of connection to the network. The MPRN identifies the supplier who has accepted financial responsibility for the energy traded at the service delivery point. At any time, there will be only one supplier for each MPRN. It defines the point at which a metering configuration can stand alone in terms of the accurate recording of consumption. In the case of unmetered supplies, it defines the point on the network where accurate estimates of the consumption can be provided for settlement. Meter Point Reference Number is the unique and unchanging reference Number (MPRN) number of a meter point. The MPRN will include a two-digit code indicating the distribution system to which the Meter Point is connected and a one-digit check digit which is calculated	Personal Data *Specific identifier linked to a Final Customer's premise Likely to be used for the treatment of Final Customers on an individual basis, in combination with other data*