An Coimisiún um Rialáil Fóntais
Commission for Regulation of Utilities

Smart Meter Data Access Code

Proposed Decision on the Smart Meter Data Access Code

Consultation Paper

Reference:	CRU/202387	**Date Published:**	14/07/2023	**Closing Date:**	15/09/2023

The Exchange, Belgard Square North, Tallaght, Dublin 24, Ireland
T +353 1 4000 800 | F +353 1 4000 850 | www.cru.ie

CRU Draft Strategic Plan 2022-24

Our Mission

- Protecting the public interest in water, energy and energy safety.

Our Vision

- Safe, secure and sustainable supplies of energy and water, for the benefit of customer now and in the future

Our Strategic Priorities

- Ensure Security of Supply
- Drive a Low Carbon Future
- Empower and Protect Customers
- Enable our People and Organisational Capacity

Executive Summary

The National Smart Metering Programme ("NSMP") involves the nation-wide replacement of over two million older analogue meters over a six-year period. Smart Meters are the next generation of electricity meters that will deliver benefits for consumers, the environment, and the economy.

The new technology installed in smart meters provides consumers with more information about their energy use, which enables consumers to make better choices about their electricity consumption. This accurate information will lead to more accurate billing by suppliers and will also help suppliers to create new smart services and products, such as Time-of-Use[1] tariffs and Smart Pay-As-You-Go[2] tariffs. Customers will then have more options to choose the most suitable tariff product that matches their energy requirements.

Smart meters remove the need for physical meter readings and estimated billing which can result in bill shocks for customers when their actual usage of electricity is not captured correctly. With smart meters, the information is sent electronically from the customer's smart meter to their

[1] At present, customers with a day/night meter can get access to tariffs that enable them to save money by shifting some of their electricity consumption from daytime to night-time, when energy is cheaper. The NSMP will extend access to these "Time of Use" (ToU) tariffs to all electricity consumers

[2] Smart Pay-As-You-Go (Smart PAYG) is a model of prepayment that will provide customers with smart meters the opportunity to pay up-front for their energy without the need for an additional meter or device in the home.

respective supplier and their actual electricity consumption is used to calculate the bill. Furthermore, accurate energy usage information during the day will enable customers to be more efficient in their energy usage and encourage them to use certain appliances outside of peak times which will help customers to save money.

Smart meters can also allow for faults to be found quicker and the network to be managed more efficiently. As a result of this, there can be reduced network costs that can be passed back to customers through reduced bills. The development of a Smart Grid[3], facilitating better network planning and improving network resilience can all be achieved by shifting electricity usage away from peak times which smart metering provides. It removes the need for less efficient and more expensive electricity generation at peak times and increases the use of renewable generation on the electricity grid. This helps to achieve decarbonisation targets and an overall reduction in electricity consumption.

Key to the above will be access to the data in the smart meter and the rules around that access. The development of a Smart Meter Data Access Code ('the Code') will provide for this.

In July 2022, the CRU published a consultation paper on the draft version of the Code. The purpose of the consultation was firstly to introduce stakeholders to the draft rules around smart meter data access and to receive feedback to help inform the CRU on how to finalise these set of rules.

Following the publication of the consultation paper, it became evident that some matters discussed in the paper, combined with undrafted sections in the Code, required further clarification and discussion with various industry stakeholders. This proposed decision paper seeks to clarify the matters discussed in the consultation paper and updates the Code to a near to final version. The paper also sets out the CRU's response to the comments received to the consultation paper.

Within this proposed decision, the CRU is seeking views from suppliers, industry groups, customer interest groups, members of the public and all other interested parties on the latest draft of the Code.

The purpose of this proposed decision paper is to inform policy decisions primarily around the governance model that the CRU will aim to include in the finalised version of the Code and CRU final decision paper.

[3] A smart grid is an electricity network enabling a two-way flow of electricity and data whereby smart metering is often seen as a first step

The proposed decision explores the following topics:

- A recommended governance and enforcement option
- The type of data available in the Smart Meter Data System
- Data security and privacy responsibilities on all parties to the Code
- Licence change proposal and considerations.
- Next steps

An updated draft of the Code has also been included with this proposed decision paper. This proposed decision paper is written with reference to the updated draft Code, and both should be reviewed together to get a complete view of what is being proposed.

One of the main focuses of the Code is the efficient governance and enforcement of its terms, which is discussed in Section 2.4.3 of this proposed decision paper. In the July 2022 consultation paper, six options for governance and enforcement were presented, with a CRU preferred option, Hybrid Model being proposed which the CRU believed would be the most effective way of implementing the code.

Based on the consultation feedback received, it became clear to the CRU that the preferred Hybrid Model required further review and as a result, the CRU are now proposing the ESBN ring-fenced option to manage and administer the Code.

The proposed model would enable the CRU to delegate the role of Code Manager to an already established entity with experience in processing meter data and handling meter data requests in the Irish electricity market. The Code Manager role includes reviewing each data access application and sending a recommendation, where necessary, to a Code Panel. This Code Panel is proposed to be made up of both industry and consumer representation with an appointed independent Chair and will include a Security Sub-Committee to decide on matters such as accession / suspension of Parties to the Code, access of Parties to the Code / Users to smart meter data, and approval of new user categories and new data items under the Code. Combined with an independent body delegated to perform the Code Compliance Officer role which includes onboarding parties to accede to the Code, assessing Parties to the Code / Users before access to smart meter data is provided, and carrying out audits on all parties under the Code, including the Code Manager, the CRU consider this option would be the most balanced way of implementing the Code.

The type of data that will be available in the Smart Meter Data System that is also presented in this consultation. The Code now includes a Data Glossary which describes the data items available in the Smart Meter Data System. The CRU believes the Data Glossary will assist both eligible parties and interested parties with their data requirements i.e., what type of smart meter

data these parties plan to request access to. These data requests will aim to be included in a Data Access Register, to be developed by the Code Manager, which determines the user category, the type of smart meter data that parties will be requesting access to and the method of how they will access the smart meter data from the Smart Meter Data System.

For parties with licence obligations, the CRU are considering modifications with respect to the DSO licence that would be necessary to primarily reflect the role of the Data Systems Provider (DSP). The CRU are also considering license changes to other licensed entities in relation to the Code. These are detailed in Section 3 “License Considerations”.

Public/ Customer Impact Statement

The number of homes and business with smart meters is increasing. Smart meters allow customers to access smart services and tariffs, which give customers greater information on their energy usage. With a smart meter, customers will have more accurate information and more control over the way they use energy. The additional knowledge and control can help customers to save more on their electricity bills by moving energy use to times of the day when electricity is cheaper.

Access to smart meter data will be important when developing the smart services being made available to customers. The rules around this access will be set out in the Smart Meter Data Access Code. Suppliers and others must sign up to the rules of this code before they can access smart meter data. They will then be able to use the data to provide services to customers and to help operate the electricity network. This will in turn help Ireland meet our climate action targets.

The smart meter data will also allow suppliers and others to provide new smart services and tariffs to customers. Customers with a smart meter installed can already access their own smart meter data. This data is provided by ESB Networks, who operate the electricity distribution network and metering systems. Customers that want to get their smart meter data can set up an Online Account[4] on the ESB Networks website. Customers can see detailed information on when they use electricity. This information can help customers find the best smart tariff for to them and when they engage with energy suppliers.

Consumption graph example covering a 24-hour period for a customer registered with ESB Networks Online Account

[4] Customers with smart meters can now access details of the electricity they have consumed and exported within their ESB Networks Online Account.

You can view a graphical representation of this usage and export data, which you can also download in a Harmonised Downloadable File (HDF). Only you have access to your data.
The data is shown in kilowatts and is available for each half hour in a 24-hour period. ESB Networks updates this data regularly and it may take 36-48 hours for data to appear on your online account.

Table of Contents

Glossary of Terms and Abbreviations

Abbreviation or Term	Definition or Meaning
CEP	Clean Energy Package
CCO	Code Compliance Officer; the delegated entity with responsibility for the development and maintenance of all Code Compliance and Assurance documentation and provisions.
Code, The Code	Specifies the updated Smart Meter Data Access Code (abbreviated as SMDAC)
Code Manager	The legal entity with responsibility for the governance, maintenance and operation of the Code.
Code Panel	The panel set up for decision-making purposes; Parties to the Code and Users are represented on this committee. The CRU is proposed to be a non-voting member. DPC and consumer representation will be invited to become non-voting members.
CRU	Commission for Regulation of Utilities as established pursuant to the Electricity Regulation Act, 1999 or any successor body.
Data Controller	As defined in Data Protection Legislation
Data Processor	As defined in Data Protection Legislation
DPC	Data Protection Commission
Data Protection Legislation	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, General Data Protection Regulation (GDPR) and any other implementing legislation within Ireland, including the Data Protection Acts 1988 to 2018.
DECC	The Department of the Environment, Climate and Communications
DSP	Data System Provider - legal entity responsible for the maintenance and administration of the Smart Meter Data System
DSO	Distribution System Operator
EC Implementing Regulation, Implementing Regulation	EU Implementing Regulation 2023/1162 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data, having regard to Article 24 of EU Directive 2019/944.
EEA	The European Economic Area which includes EU countries and also Iceland, Liechtenstein and Norway.
Eligible Party / Parties	means an entity offering energy-related services to final customers, such as suppliers, transmission and distribution system operators, delegated operators and other third parties, aggregators, energy service companies, renewable energy communities, citizen energy communities and balancing service providers, as far as they offer energy related services to final customers.
GDPR Checklist	A checklist to evidence compliance with Data Protection Legislation provided by the Data Protection Commission (DPC)

Other User	Legal entity that has access to the Smart Meter Data System by virtue of an Access Agreement, without being a Code Party.
Party, Party to the Code	Legal entity 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
SMO	Single Market Operator
Smart Meter Data System	The infrastructure and Smart Meter Data System (data hub) operated by the DSO, and all interfaces, including portals or interfaces to allow access to Smart Meter Data and any other Data associated with the Smart Meter.
SSC	Security Sub-Committee set up to deal with complex data access requests, new user categories and breaches of the Code. This committee sits with the Code Panel and is made up of data security / privacy expertise from industry.
TSO	Transmission System Operator
User, Data System User	Party that has completed the Entry Process and is entitled to access Smart Meter Data on the Smart Meter Data System, by virtue of being a Code Party and having an Access Arrangement- that includes an approved data privacy and security assessment

1. Introduction

1.1 Background

The Department of the Environment, Climate and Communications (DECC) has progressed the transposition of the Clean Energy Package (CEP) which comprises eight legislative acts on the energy performance of buildings, renewable energy, energy efficiency, governance and electricity market design. A revised Directive on common rules for the internal market for electricity (EU) 2019/944 ("IMED")[5] will be one of the key drivers for the evolution of the electricity markets in the next decade.

That Directive includes the following provisions for a competent authority on Smart Meter Data to be established:

- Encourage the electricity market in Ireland to optimise the use of electricity to promote energy efficiency and empower customers.
- Ensure that the smart meter deployment assists the active participation of the customer within the electricity market.
- Require the DSO to implement and publish the functions and technical details of smart meters.
- Ensure smart meters are able to communicate, exchange data and provide output for customer energy management purposes.
- Monitor smart meter deployment to be able to track the delivery of benefits to customers.

The authority will also be responsible for defining rules for access to, and processing of, data from smart meters. The CRU has been designated as the competent authority with responsibility for this.

Smart meter data is a key building block for the clean energy transition and is fundamental to enabling customers and market actors to access and provide the opportunities the CEP envisages. Given the nature of the Data Protection Legislation and the need to ensure that data is secure and only processed where appropriate, an updated draft version of the Smart Meter

[5] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU

Data Access Code has been developed for this proposed decision. This work needs to be progressed in 2023 to ensure the activities envisaged under the CEP are possible.

The aim of the Code is to ensure customers interests and their respective smart meter data are protected and secure and to maintain transparency in terms of its implementation and management. The Code also proposes to validate an established basis for market participants, including the DSO, to use smart meter data for network planning, real time grid management and information provision purposes.

1.1.1 Scope of Requirements

DECC has completed the transposition of Articles 19 – 24 of the IMED, and the CRU is now the designated competent authority, providing the legislative basis for the Code. It will not be possible for the market operator to collect and disseminate some classes of smart meter data to other actors in the market without the Code being in place.

Under the regulations, the CRU shall:

- Specify the point at which smart meter data shall no longer be considered personal data,
- Establish a clear definition of non-personal data, with respect to smart meter data, in accordance with relevant EU and national data protection legal framework, that may be stored by eligible parties without the requirement for customer consent,
- Specify the purposes for which the DSO shall collect and process smart meter data,
- Specify the rights of access to smart meter data for final customers and third parties acting on their behalf,
- Specify the basis for the provision of smart meter data to suppliers. SEMO and the TSO
- Specify the smart meter data that may be transferred to eligible parties and the conditions under which this data may be stored by those parties,
- Require that suppliers obtain each final customers consent before that customer is switched to a dynamic electricity price contract,
- Specify the rules for the use of smart meter data by the DSO for its systems planning and operational purposes, and
- Specify the manner in which eligible parties are to have access to smart meter data and the reasonable and duly justified charges which shall be payable by the eligible parties.

The Code will establish which entities can access customers' smart meter data, and in what cases, without prior agreement with the customer, as per the legal bases prescribed in Article 6 of GDPR. It will also define the purposes for which customers' personal data can be used by ESB Networks in its role as the Distribution Network Operator, by Energy Suppliers who are providing a service to customers, other parties such as SEAI, the CSO for research purposes and other actors in the energy market whose role is set out in the CEP. This will include aggregators and demand side response providers. The intention is for the Code to validate an established basis for market participants, including the DSO, to use meter data for network planning, real time grid management and information provision purposes.

The CRU will provide advice and guidance on how Smart Meter Data will be treated, some of which may be personal data, in the context of the wider regulatory framework (including Data Protection Legislation) and how best to enable the energy market to process this data to enable the opportunities in the CEP to be realised.

1.1.2 Responses to the Consultation

The CRU published its consultation paper (CRU202265) on the draft version of the Smart Meter Data Access Code on 6 July 2022. The CRU received 11 responses to the consultation:

- Bord Gais Energy
- Digital Rights Ireland
- Economic and Social Research Institute
- Electric Ireland
- Electricity Association of Ireland
- Energia
- ESB Networks
- PrePayPower
- Retail Market Design Service
- Sustainable Energy Authority of Ireland
- UCD Energy Institute

The CRU plans to publish the responses a short time after this Proposed Decision is published.

1.1.3 Related Documents

By way of background to this consultation paper, the following list of documents is of relevance:

- CRU Information Paper on Phase 2 Scope of the NSMP[6]
- Statutory Instrument 37 of 2022 – EU (Internal Market in Electricity) Regulation 2022[7]
- CRU Consultation on the draft version of the Smart Meter Data Access Code[8]
- Draft version of the Smart Meter Data Access Code[9]

Information on the CRU's role and relevant legislation can be found on the CRU's website at **www.cru.ie**

1.1.4 Structure of Paper

- **Section 1** contains background information and scope of requirements in relation to this proposed decision.
- **Section 2** presents the proposed option on governance and enforcement and provides the data types that will be available for access; The CRU's proposed decision to the consultation responses received, with regard to the remaining questions posed in the consultation paper, are also included.
- **Section 3** looks at the proposed license modifications considered for the Code.
- **Section 4** sets out the next steps in the proposed decision process.

1.1.5 Responding to this Proposed Decision

Responses to this proposed decision should be returned by email or post by close of business on the 15th of September 2023 and marked with the reference CRU/202387.

Please forward submissions on this paper (preferably in electronic format) to:

Retail & Smart Metering Team

Commission for Regulation of Utilities

The Exchange

Belgard Square North

Tallaght

Dublin 24

E-mail: smartmetering@cru.ie

---

[6] CRU21074-CRU-Information-Paper-on-Phase-2-Scope-of-the-NSMP (Page 10)
[7] S.I. No. 37 of 2022 -EUROPEAN UNION (INTERNAL MARKET IN ELECTRICITY) (NO. 2) REGULATIONS 2022
[8] CRU202265-Consultation on the Draft Version of the Smart Meter Data Access Code
[9] CRU202265a-Draft Version of the Smart Meter Data Access Code

2. Smart Meter Data Access Code

The main objective of the Code is to ensure customer interests and their respective smart meter data are protected and secure and to maintain transparency in terms of implementing and managing the Code. For the DSO and Suppliers, the Code's aim is to facilitate their obligations, as set out in their respective DSO and Supplier licenses. Third parties' obligations will be set out by contractual agreement with the customer or an agreement process within the Code.

The updated draft of the Code, which has been published alongside this proposed decision paper, includes a main body outlining the terms and accompanying schedules and appendices which form part of the Code. These are subject to amendment or modification where necessary. The CRU is keen to highlight that this updated draft of the Code will be addressed in this proposed decision to assist in the final version of the Code and the CRU decision paper.

One of the main topics outlined in this proposed decision paper is the proposed governance and enforcement option which would apply to all users of the Code. The CRU will also consider the implementation steps for the proposed governance model that would be required ahead of a final version of the Code.

The sections and schedules of the attached Code that have now been updated or drafted are as follows:

- Definitions and Interpretation (Section 4);
- Categories of Parties and Data Access (Section 5);
- Becoming a Party (Section 6);
- Compliance (Section 7);
- Code Panel (Section 8);
- Security Sub-Committee and Other Sub-Committees (Section 9);
- Code Manager (Section 10);
- Code Compliance Officer (Section 11);
- Data Systems Provider (Section 12);
- Change Management (Section 15);
- Data Security and Data Privacy Obligations (Section 17);
- Force Majeure (Section 18);
- Disputes (Section 19);
- Derogations (Section 20);
- Events of Breach and Consequences of Breach (Section 21);

- Ceasing to Be A Party (Section 22);
- Ceasing to Be an Other User (Section 23);
- Interpretations (Schedule 1);
- Access Arrangements (Schedule 2);
- Accession (Schedule 3);
- Data Security (Schedule 4);
- Data Privacy (Schedule 5);
- Assessment (Schedule 6);
- Code Panel (Schedule 7);
- Party Exit (Schedule 8)
- Change Management (Schedule 9);
- Security Sub-Committee (Schedule 10);
- Data Glossary (Appendix 1)

The following sections detail the sections and schedules of the Code that were initially consulted on, with a summary of the consultation, stakeholder response and the CRU proposed decision, where possible. The newly drafted sections and schedules of the Code, previously undrafted, are also discussed in this proposed decision paper.

Sections 13, 14, and 16 which cover Costs, Annual Budget and Cost Recovery, Usage Charges and Limitations of Liability are still under consideration, pending a final decision on a governance framework.

2.1 Definitions and Interpretations

This section and schedule detail the list of general interpretations and definitions provided in the Code. The glossary of terms and abbreviations used in the Code is provided on page 6.

2.1.1 Smart Meter Data

The Smart Meter Data definition is taken from Statutory Instrument 37 of 2022, transposed from Article 23 of EU Directive 2019/944:

“a) metering and consumption data, and

(b) data required for customer switching, demand response and other services,”

This definition adequately covers data coming in and out of the smart meter.

2.1.2 Smart Meter Data System

The Smart Meter Data System is the data hub or repository developed to collect and make available smart meter data. The role responsible for developing this data repository is defined as the Data Systems Provider under the Code. This role is obligated to ensure that the Smart Meter Data System is secure and compliant with relevant data protection legislation and that it provides the access interfaces required to access smart meter data.

2.1.3 Data Systems Provider

The Data Systems Provider (DSP) is defined as the legal entity that is responsible for the maintenance and administration of the Smart Meter Data System i.e., the hub, infrastructure, and access interfaces / portals. The DSP also ensures the smart meter data is available to access and process. This signifies that the DSO will be the legal entity providing data that will populate the Smart Meter Data System, which is being purposely built by the DSO to hold large volumes of all data from smart meters.

In the July 2022 consultation paper, CRU aimed to avoid confusion with the introduction of the DSP role by referencing the DSO, as the legal entity to perform the role, throughout the paper. However, in the stakeholder responses received for the consultation, it was noted that the DSP and DSO are two separate roles as set within the Code. The CRU confirms the separation of DSP and DSO roles are necessary for the purposes of collecting and making available smart meter data (DSP) and accessing and processing the smart meter data (DSO).

Furthermore, the inclusion of the DSP role will require a licence modification to the DSO licence which is discussed in Section 3 License Considerations.

2.1.4 Personal / Non – Personal Data

In terms of the smart meter data that is available in the Smart Meter Data System, a Data Glossary is now available which contains the data that will be accessible from Day 1 of the Code going live. This glossary is considered to meet the definition of smart meter data, but CRU is aware that, subject to legislative changes and /or approval, additional smart meter data items may become available at a later time. This glossary is included as an appendix to the Code and will be discussed in Section 2.2.

As per Article 4 in GDPR legislation, personal data is defined as any data which are related to an identified or identifiable natural person[10]. The data glossary will highlight whether a data item is considered personal or non-personal with regard to smart meter data only. As an example, it has already been determined, through engagement with the DPC, that the Meter Point Registration Number (MPRN), which tells the location of a customer's premises at which the smart meter is installed, is considered personal data. Therefore, when MPRN data is included with datasets that are being requested to access, the dataset is defined as personal in relation to smart meter data.

The CRU notes that non-personal data is defined in Article 3 of EU Regulation 2018/1807 as data other than personal data[11] i.e., data that does not originally refer to an identified / identifiable natural person or data that initially was personal and subsequently rendered anonymous. With respect to that definition, under the Code, any access request or application for anonymous or aggregated smart meter data i.e., data that contains non-personal data e.g., no MPRN data included, the dataset is therefore defined as non-personal with respect to smart meter data.

[10] 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) – Article 4 Definitions (1) - 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[11] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union – Article 3 Definitions (1) - 'data' means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679

2.2 Categories of Parties and Data Access

2.2.1 Summary of consultation position

The categories of parties and their respective eligibility to access smart meter data were discussed in the consultation. Those parties with licence obligations i.e., DSO, TSO, SMO and Suppliers, are obliged to become a Party to the Code and are automatically eligible to become a Data Systems User (User) to access smart meter data.

For those who are not eligible to become a Party to the Code i.e., Other Users, third parties such as price comparison websites, data aggregation and response companies and electricity undertakings, the Central Statistics Office (CSO), the Sustainable Energy Authority of Ireland (SEAI) and universities for research purposes, an access agreement is required to allow access to smart meter data from the Smart Meter Data System.

For customers, they are not required to become a Party to the Code, nor will they be subject to the obligations set within the Code. Customers can access their smart meter data via the DSO or their respective supplier. The DSO has launched a customer online account[12] which will allow customers with smart meters installed to access their respective smart meter data. A Harmonised Downloadable File (HDF[13]) is also available on this customer online account which enables customers to download and share their smart meter data with suppliers or third parties. Customers can also access their smart meter data by providing consent to a third party to access the data on their behalf e.g., price comparison websites.

The Access Arrangements schedule primarily concerns a third party and explains how such a third party can apply to become an Other User to the Code and access smart meter data. There will be a requirement on third parties to complete information security and data protection assessments before any access to smart meter data will be permitted. The Code Manager is responsible for assessing each application against criteria, as approved by the Code Panel. The criteria include validating the third party's identity, verifying the third party meets the expected characteristics for the requested category of User, and confirming the specific smart meter data being requested is consistent with the category of User allowed in the Data Access Register. Once assessment for the application is complete, the Code Manager determines if the application will be approved or rejected. For an approved third-party application, the DSP is

[12] ESB Networks Online Account

[13] Harmonised Downloadable File is a web-based means of providing consumption and export data in a standard harmonised downloadable format to the customer.

notified to provide smart meter data access to the third party. In the case where an application is rejected, the third party can appeal the decision to the Code Panel.

The Data Access Register will include the list of User Categories, the smart meter data they are permitted access to, and the mechanism used to access the relevant smart meter data. It is important to note that twenty-four-hour, day, peak and night register, half-hourly interval, event, and instrumentation data will be stored and available in the Smart Meter Data system. A comprehensive data dictionary, outlining each data item contained in the Smart Meter Data System will be provided for the Code. The CRU encourages industry and interested parties to outline their respective data requirement expectations in their response to this proposed decision paper.

The CRU also discussed how access to the Smart Meter Data System could be provided and presented three options under consideration:

- Portal Access – seen as a method for customer access and requests for smaller amounts of data.
- Connected Systems – allows for large volumes of data to be accessed and applicable to entities with API capabilities on their respective systems.
- Whole File Transfer – caters for third parties requesting bulk data in a single transfer.

The CRU asked respondents on their views on the most suitable way to access smart meter data and what type of smart meter data they expected to have access to.

2.2.2 Summary of responses

Respondents were generally supportive of the options provided in the consultation paper but noted the lack of information on what specific smart meter data is available in the Smart Meter Data System as the reason use cases were not submitted.

Several respondents suggested that the flexibility of all three options being provided is necessary to facilitate the various requests for smart meter data. Some responses expressed strong views on extra layers of security and validations i.e., multi-factor authentication being applied to the portal access system. Some respondents suggested access to smart meter data could be achieved by the customer sharing or uploading their respective smart meter data, via a downloadable HDF, to a supplier or third-party site.

A majority of responses highlighted the default bi-monthly day/night/peak smart meter data reads requested and approved in Market Change Request (MCR)1208[14] as a use case for the smart

[14] Market Change Request 1208

meter data Suppliers would be expected to receive. Most respondents expect to access the twenty-four-hour, day, peak and night register, half-hourly interval, event, and instrumentation data that is recorded by a smart meter for various reasons i.e., to fulfil licence obligations and for research purposes. The responses in general agree that it is important the access to customer smart meter data is secure and used appropriately and that any data request needs to be justified with a valid legal basis as defined in relevant data protection legislation.

2.2.3 The CRU's proposed decision

As mentioned previously, the CRU is including a Data Glossary which provides the data items that are available in the Smart Meter Data System, a description of each item and guidance on how each data item is classified as personal or non-personal smart meter data. This glossary is considered to cover the definition of smart meter data as provided in S.I. 37 of 2022. The data glossary is included with the updated Code, as an appendix.

The CRU would like to highlight that the data items available in the Smart Meter Data System will not be used for billing and reconciliation purposes. The following flow diagram sets out the separate data flows for access to the Smart Meter Data System and for billing via the Retail Market System.

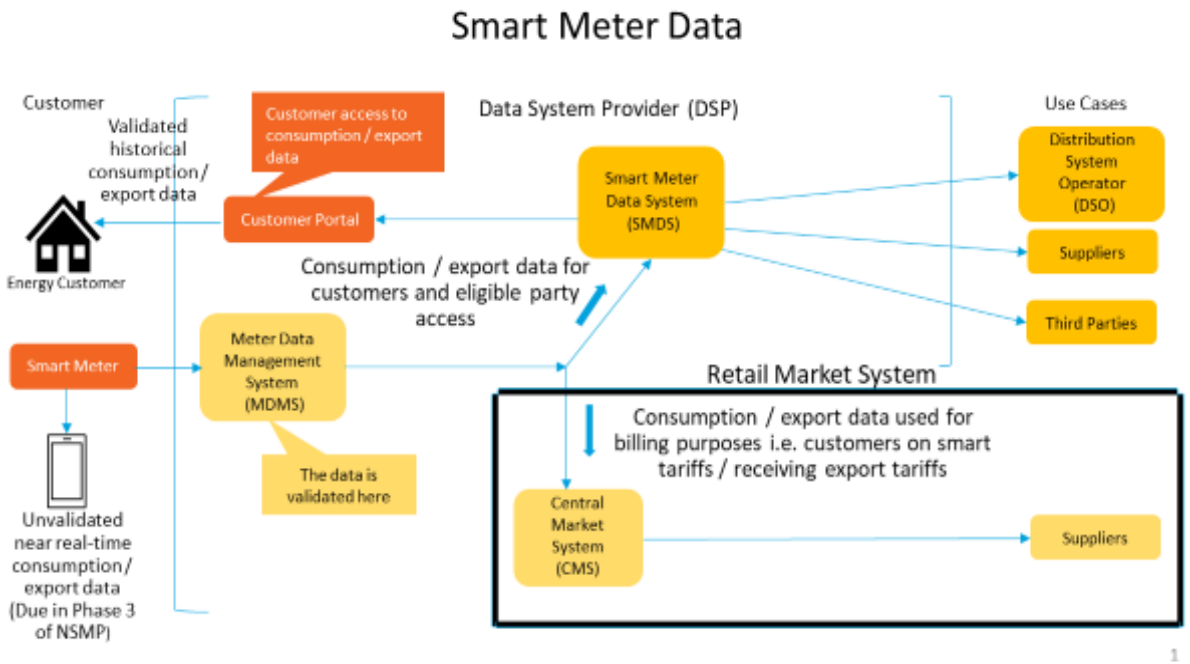

Figure 1 – Overview of the Smart Meter Data System and Retail Market System.

As shown in the figure above, the smart meter data is validated in the Meter Data Management System and then sent to the Smart Meter Data System where it is stored and presently made

available to customers through the online customer portal. The smart meter data is also sent through the Retail Market System, in the instances where customers have signed up to smart tariffs, opted in to access smart services or are availing of export tariffs, to suppliers for billing purposes.

The data that is currently available in the Smart Meter Data System is validated historical consumption and export data for customer access only. Customers will be able to view their consumption / export data in graphical form on the DSO online customer portal. They can also download their consumption / export data in CSV file format which empowers customers to share their respective data with suppliers and third parties to both fully understand their consumption behaviour and to see what suitable tariffs there are available to them.

The CRU would like to note that the rights of customers, in terms of their smart meter data, will be clearly specified in the final version of the Code to meet legislative requirements. These rights include:

- Accessing their own validated historical consumption / export data via an online interface, and at a certain point in the future accessing their near real-time consumption data via an application on their phone or in-home display.
- Accessing a data access log which will show them who is / had accessed their validated historical consumption / export data, the permission used to access their data and the type of data shared.
- Giving consent to allow an eligible party to access their validated historical consumption / export data on their behalf for a specified time period.
- Revoking consent to an eligible party accessing their validated historical consumption / export data.

These rights are in addition to those already contained in Articles 12-22 of GDPR legislation, which are also to be set out in the final version of the Code.

The CRU recognises that certain Other Users, like aggregators, energy service companies, renewable energy communities, citizen energy communities, price comparison websites and demand response providers and entities that offer energy related services to customers are considered eligible according to EU legislation and as such, the CRU proposes that these entities are eligible to become Code Parties and that this will be clarified further in the final decision paper. Other Users such as statistic institutes, research institutes and authorities, universities etc. will be subject to an Access Agreement prior to access to smart meter data being granted.

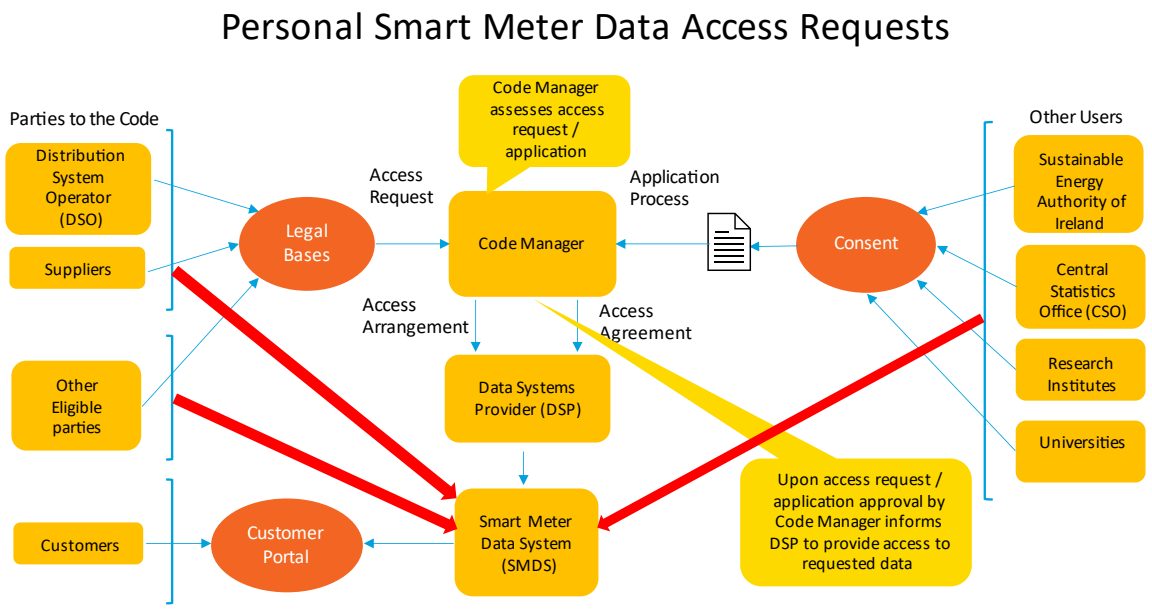

Figure 2. Overview of personal smart meter data requests under the Code

In terms of personal smart meter data, Code Parties, including eligible parties, will need to ensure that one of the legal bases under the remit of GDPR has been obtained prior to access such data. For Other Users and their respective Access Agreement, they will need to ensure that consent from the customer has been collected in order to access personal smart meter data.

Smart Meter Data

The smart meter data items that are currently included in the Data Glossary and stored in the Smart Meter Data System are as follows:

- **30-minute Interval Consumption Data** – this is the validated electricity consumed from the grid recorded and stored every 30 minutes, measured in kilowatts (kW) - 48 values recorded in each 24-hour period.
- **30-minute Interval Export Data** – this is the validated electricity exported to the grid recorded and stored every 30 minutes measured in kW for customers with micro-generation installed – 48 values recorded in each 24-hour period.
- **24-hour Consumption Register Data** – this is the electricity consumed from the grid, snapshot taken daily at midnight and monthly on the first day of the month, measured in kilowatt hours (kWh).
- **24-hour Export Register Data** – this is the electricity exported to the grid, snapshot taken each midnight, measure in kWh for customers with micro-generation installed.

- **Standard Smart Tariff (SST) Day / Peak / Night Consumption Register Data** – this is the electricity consumed from the grid, snapshot taken each midnight, measured in kilowatt-hours (kWh). It is broken down 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 and SST Peak Import Register (kWh) from 5pm to 7pm.
- **Communication Technical Feasible (CTF) Data** – this data establishes the reliability of communications from the smart meter across the telecommunications network. It is used for switching purposes and is measured as a number between 1-4 depending on the communication quality of all meter types, with 1 relating to poor communication requiring manual only readings i.e., conventional meters (24-hr, Day / Night), and 4 being very good communication where remote daily reads are reliable i.e., smart meters.
- **DUoS Group Data** – this a code that represents the distribution use of system tariff applying to the MPRN of a premise. This data is generally used for switching purposes.
- **MPRN - Meter Point Registration Number**. This is the unique identifier for each connection point to the network from the customer home. The MPRN identifies the location of a customer's premises at which the smart meter is installed and also the supplier who has accepted financial responsibility for the energy traded at the connection point. At present, at any time, there will be only one supplier for each MPRN. 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.

The CRU is aware that there is also technical information i.e., event and instrumentation data being recorded by the smart meter. It is the CRU's understanding that this data is considered to be solely useful to the DSO to enable it to manage and monitor smart meters as per its statutory requirement under licence conditions. The CRU will review whether this type of data will need to be covered under the Code to be made available to access and will clarify, in the final decision paper, whether there will be an updated data glossary to reflect this data type.

In Phase 3 of the NSMP, unvalidated near real-time consumption / export data from smart meters will be made available to customers via an in-home display or application on their phone. Combined with the tariff that customers on, this data will seek to provide greater insights into a customer's consumption behaviour and will encourage the customer to become more aware of their consumption throughout a 24-hour period and enable them to change their consumption to different times in the day or night so as to see the savings they could potentially make on their energy bills. This data will be covered in the Code when it becomes available, and the data glossary will be updated to reflect this data type.

Use Cases

The CRU has been made aware of use cases i.e., data requirements, which are expected to be made available to the relevant eligible party to access on Day 1 of the Code going live.

Suppliers have provided a use case, in the form of a Market Change Request (MCR1208) to allow suppliers access to their respective customers Standard Smart Tariff register data i.e., the default bi-monthly Day/Night/Peak register read to enable suppliers to offer more attractive ToU tariffs to suit the consumption needs of the customer. While the CRU is in favour of providing this access to suppliers, the CRU is also aware of the importance of data protection being adhered to prior to access being granted, given that the smart meter data concerned contains personal data of customers and the purposes for this access likely go beyond billing as is currently set out in licence conditions. As such, while the CRU can determine the purposes for processing personal smart meter data, as per 6.3(e) of S.I. 37 of 2022, it cannot determine the essential means of the processing for those purposes. Furthermore, data controllers, which suppliers are considered to be, must establish that one of the lawful bases under Article 6 of GDPR, apply to the processing of personal smart meter data for each given purpose.

The CRU is aiming to discuss further, with its own legal team and DECC, on potential legislative changes to support this use case with an established lawful basis to access and process this data ahead of the Code go-live date, once the final decision paper for the Code and finalised Code has been published. The CRU will aim to discuss this particular use case further in the final decision paper.

The CRU understands the need for the DSO to access smart meter data for purposes such as network planning and operation, revenue protection and flexibility services and solutions for customers. Similarly, the purposes for processing personal smart meter data can be determined by the CRU but the DSO, as a Data Controller, must establish that one of the GDPR lawful bases apply to each purpose that is specified. The CRU will engage with its own legal team and DECC to see what legislative amendments can be made to support these particular use cases with the intention of delivering this access, on publication of the final decision paper for the Code, prior to the Code being up and running. It is the intention of the CRU to outline these use cases in more detail in the final decision paper.

As discussed previously, the data glossary provided contains the data items that are considered to cover the smart meter definition. However, the CRU is aware of other smart meter data items that may be requested by entities, which are not currently listed in the data glossary. Any new smart meter data item request would need to be assessed by the Code Manager and approved by the Code Panel / Security Sub-Committee before being made available.

Method of Access Workshop

The CRU would like to highlight a workshop that took place in March 2023 for both market participants and interested parties, which included a presentation by the DSP on the method of access to smart meter data.

From the workshop, it was established that the DSP's preferred method of access will be connected systems / an API setup for the majority of requests received to access smart meter data. The CRU notes that market participants and interested parties will need to ensure their IT systems are compliant and / or upgraded, where necessary, to allow access to smart meter data via a connected system. The CRU confirms that the connected system will be the main method of access to smart meter data.

Access to smart meter data with the portal option will only be available to customers. This portal is available to customers through the online customer portal on the DSP website. Customers can currently see their historical consumption and export data in graphical form and can download their smart meter data as a CSV file to use themselves to better understand their daily consumption or to share with their supplier or a price comparison website as examples in order to see tariffs that suit their usage patterns. The CRU is aware that the historical data being currently provided to customers in the online portal is in kilowatts and that work by the DSP is in progress to include the data in kilowatt hours which is the recognised retail market format. This will enable the customer, and their respective supplier / price comparison website they share their data with, to interpret the historical consumption data more efficiently.

It was recognised at the March workshop that there would need to be flexibility in the access mechanism to enable requests to access smart meter data in bulk. A Secure File Transfer (SFTP) access method will be made available, upon approval, to parties who request bulk smart meter data. Given the volume of data included in a request such as this, the smart meter data will need to be aggregated / anonymised before access can be granted.

Access to Smart Meter Data Pre-Code

In terms of accessing customer smart meter data, all market participants and interested parties must adhere to the principles relating to the processing of personal smart meter data contained in GDPR legislation. Articles 5-7 of GDPR[15] set out how parties must provide a lawful basis to

[15] Article 5 GDPR - Principles relating to processing of personal data;
Article 6 GDPR - Lawfulness of processing; Article 7 GDPR - Conditions for consent

process personal smart meter data and ensure that the data is used for specific and legitimate purposes. The CRU is seeking that the approach to granting access to personal smart meter data is seen as non-restrictive as possible, providing the obligations under data protection legislation are met.

The CRU is cognisant of a lawful basis being required by parties prior to requesting personal smart meter data. Once this basis has been established and verified, and in addition to confirmation that respective IT systems are compliant in terms of data security, access to such smart meter data will be granted. For clarification, the CRU confirms that Code Parties, including those considered eligible parties and therefor eligible to become a Code Party, will be required to acquire a legal basis as per Article 6 of GDPR, to access personal smart meter data. The CRU would like to note that Other Users, subject to an Access Agreement, must have evidence of consent collected from the customer prior to access to personal data being granted.

Subject to an industry approved governance framework, the CRU is proposing that some use cases, where personal smart meter data is concerned, will be under consideration to be granted ahead of the Code go-live date, dependent on potential legislative changes being implemented. The CRU considers access to smart meter data is one of the key drivers to achieve climate action plan and decarbonisation targets and by providing access to industry, that is compliant with data protection legislation and shared in a timely manner, will enable said parties to contribute towards these targets and provide to customers more benefits through more attractive smart tariffs and services. The CRU believes access to smart meter data should be as permissive as possible, with respect to data protection requirements.

With this recommendation and pending the publication of the decision paper and final version of the Code, the proposed Code Manager's role, an already established entity (MRSO), would be in a position to facilitate this access to personal smart meter data and log each access arrangement /agreement in the Data Register, which documents the user category, the type of data being requested, the legal basis for processing personal smart meter data and the method of how access will be provided. Once the MRSO has procured the sufficient resources and expertise to fulfil the Code Manager role, the CRU believes the proposed Code Manager would be in a position to assess these requests to personal smart meter data, including confirming data protection compliance and that the IT systems are meeting data security standards. Once these requirements are met, the proposed Code Manager will approve the request and notify the DSP to make the data available. Once the Code is up and running, the Data Register will contain the agreed requests prior to go live. The other entities within the proposed governance model will be procured and set up post the CRU decision paper publication and the CRU recognises the significant timelines involved, estimated to be at least 6 months from publication of the final decision paper, in implementing the proposed governance framework. With this timeframe in

mind, the CRU believes granting access to particular use cases ahead of the Code going live is necessary to enhance the NSMP and its related projects that depend on accessing smart meter data. The CRU understands there will be time required after publication of the final decision paper to enable the MRSO to ensure the adequate resources are in place to assess these data requests and that this needs to be considered.

Similarly, for non-personal smart meter data access requests i.e., smart meter data that is aggregated or anonymised, the CRU is proposing that the proposed Code Manager role would facilitate these access requests from the publication date of the CRU decision paper and final version of the Code and log the access arrangement / agreement in the Data Register. As stated above, the CRU acknowledges the significant time needed to enable the MRSO to procure the necessary resources and expertise to carry out these assessments and as a result, this would need to be considered before access requests can be submitted to the Code Manager. By the time the Code is live, these approved access requests will be documented. The CRU considers the proposed Code Manager would be best placed to assess these non-personal smart meter data requests and upon approval, notify the DSP to make this data available. The CRU believes that, where there is no personal smart meter data involved, there is also merit in publishing anonymised / aggregated non-personal smart meter datasets which the CRU considers as a public good. For smart meter data requests that contains both personal and non-personal data, GDPR requirements would need to be met to allow access to this requested data.

The CRU view this proposal as vital to the reputation of the NSMP in terms of customer sentiment and engagement and see earlier industry access to smart meter data as an important tool in achieving climate action targets and the increase of services being offered to customers with smart meters installed. The CRU would like the data access approach to be shaped in a way to allow as much smart meter data to be shared as is possible within the confines of GDPR requirements, where personal smart meter data is concerned, and that the proposed governance model is seen to be supportive of innovation. With that approach in mind, the CRU is also considering whether amendments to legislation are required to assist with certain use cases, as highlighted above, and will engage with DECC to ascertain what legislative changes are possible in this context.

Question 1: The CRU would welcome any views on the proposal on access to smart meter data ahead of the Code going live.

2.3 Becoming a Party and Compliance

2.3.1 Summary of consultation position

In the consultation paper, the process of how to become a Party to the Code and the expected annual compliance and assurance provisions in place for Users to the Code were discussed.

An entity may apply to become a Party to the Code, provided the necessary criteria is met, and the Code Panel determines to admit the entity as a Party to the Code.

There is a provision in place for the CRU to carry out an annual audit of the Code and that an Assurance Strategy, to define the scope of assurance activities and techniques will need to be developed by the Code Compliance Officer.

Users to the Code are required under the Code to perform annual Information Security and Data Protection assessments. If Users to the Code are found to be non-compliant with the obligations imposed by the Code, as a result of these annual assessments, they may be considered to be in breach of the Code. Users are obligated to notify the Code Manager of any data security or integrity breaches.

The CRU asked respondents on their views on the annual compliance and assurance assessments placed on all Users to the Code.

2.3.2 Summary of responses

Respondents were generally in agreement of annual compliance and assurance assessments but highlighted that these assessments will need to be compatible with existing GDPR legislation.

Several respondents suggested the Code should be a Code of Conduct under Article 40[16] of the GDPR legislation would provide clear guidance to all Users to the Code. Some responses cautioned on the potential doubling up of regulation with both the Code and GDPR compliance obligations.

There were contrasting views on compliance assessments. Some respondents believed that assessments should be varied depending on the User and the type of data being accessed. Other responses felt that compliance by all Users should be of the same standard regardless of the category of User. A memorandum of understanding (MoU) between the Data Protection

[16] Article 40 GDPR – Codes of conduct

Commission and the Code Manager was also proposed in some responses to provide confidence in data protection under the Code.

The majority of responses sought further clarity on the role of the Code Compliance Officer and the development of an Assurance Strategy and welcomed the opportunity to engage with the CRU on how the strategy will be developed.

2.3.3 The CRU's proposed decision

The CRU believes the requirement of privacy and security assessments on all Code governance entities, including Parties to the Code, Other Users and the DSP, during entry to the Code and access arrangements / agreements are essential when considering the processing of smart meter data. The CRU seeks to achieve a balance between adherence to data protection legislation and ensuring the smart meter data is made available to eligible parties to enable them achieve climate action targets, improve the network efficiency, support innovation, and provide new and attractive smart tariffs and services to customers.

It is CRU's understanding that some Parties to the Code are automatically entitled to metering and consumption data, to fulfil licence obligations and for legitimate purposes such as billing. In order to access smart meter data that is considered personal from the Smart Meter Data System, Parties to the Code must demonstrate a legal basis to access personal smart meter data for purposes other than what is contained in their existing licence obligations. The Code Compliance Officer must also receive the necessary assurance around data protection, which includes legal basis for the data that is being requested for access, and security controls that are in place on Parties to the Code respective procedures and systems. This is to mitigate against a new Party to the Code presenting a risk of a data breach or security incident that would compromise the Smart Meter Data System. The same assurance requirements are placed on Other Users, who are not automatically entitled to metering and consumption data.

Given that technology will evolve and that there will be likely be changes to data items being made available on the Smart Meter Data System in the future, the CRU considers that annual assessments on all Code entities should be conducted, as is best practise among other existing codes. The CRU is aware that service providers, such as software providers, will also be subject to these assessments to ensure they do not pose a risk to smart meter data, including metering and consumption data, or data of Code entities' employees.

The CRU is proposing that all security and privacy assessments, including on entry to the Code and on an annual basis, be carried out by the Code Compliance Officer. The assessments are recommended to be structured in accordance with the following schedule, as covered by Section 7 of the Code.

Code entity	**Entry / Year One**	**Annual Basis**	**Ad-hoc (new data item requested, new User Category, investigation purposes)**
Party to the Code (DSO, Suppliers, Eligible Parties)	Entry Assessment	Annual Self-assessment	Ad-hoc assessment
Other User (Third Parties)	Entry Assessment	Annual Self-assessment	Ad-hoc assessment
DSP	Entry Assessment	Annual Self-assessment	Ad-hoc assessment
Service Provider	Due diligence Assessment	Due diligence Assessment	Ad-hoc assessment

The types of assessments are as follows:

- **Entry Assessments**: Full assessment from a data security and data protection perspective, conducted on all Code entities and service providers upon entry to the Code, on signing an access agreement (in the case of Other Users), or on procurement of service providers.
- **Annual Assessments**: Self-assessment questionnaires will be issued by all Code entities and service providers on an annual basis. These will be assessed by the Code Compliance Officer to determine if further investigation and / or an ad-hoc assessment is necessary.
- **Ad-hoc Assessments**: These assessments may be conducted where a risk is identified with respect to a Code entity such as the Code Manager, DSP, Code Parties (which include the DSO and Suppliers) and Other Users or a processing activity following a security incident or data breach by a Code entity, or where a new User Category or new

data item is requested. In these situations, the Code Compliance Officer may carry out an ad-hoc assessment of these Code entities.

The procedures for all the above assessments shall be further defined in Schedules 2, 4 and 5 of the Code. The requirements for each assessment will be defined by the Code Compliance Officer, which shall include good industry practice, and then approved by the Security Sub-Committee within the Code Panel setup.

The CRU would like to reassure industry that it will be responsible for appointing the Code Compliance Officer to ensure independence and impartiality within the proposed governance model. The CRU considers that the auditing role of the Code Compliance Officer needs to be robust and that any recommendations it makes from an assessment must to be implemented to ensure an efficient management and enforcement of the Code. The CRU believes that access to smart meter data must be seen to be as permissive as possible, which supports eligible parties in achieving climate action targets, with respect to these proposed assessments that seek to ensure compliance with data protection legislation.

Question 2: The CRU would welcome any views on the proposed entry, annual and ad-hoc assessments placed on all Code entities.

2.4 Governance and Enforcement of the Code

2.4.1 Summary of consultation position

In relation to how the Code will be managed and enforced, the CRU considered a number of options for governance in the consultation paper, and an overview of the pros and cons of each of these options were provided, including the CRU's preferred option. The governance options discussed were:

- Special Purpose Vehicle (SPV)
- Code Administrative Service (CAS)
- In-House
- Outsource to the DSO
- RMDS as the Code Manager
- Hybrid – In-House and CAS combined (preferred option)

The governance options each provided a high-level view of the responsibilities of the Code Manager, the Code Panel, and the CRU. In each option, the Code Manager was considered responsible for assessing applications to access smart meter data, investigating data breaches while developing Code processes, access agreements and the Data Register. The Code Panel responsibility to assess the Code Manager's recommendations on applications, breaches and Code modifications was also discussed. The CRU would then be required to issue a final decision on recommendations submitted by the Code Panel.

The CRU believed at the time that the Hybrid option would be the most realistic choice for governance. The CRU's position was based on how quickly the Hybrid model could be set up more quickly than the other options presented, which was considered advantageous in terms of the timelines involved to deliver the Code. The option was also seen as fair and transparent.

In this Hybrid option, the in-house Code Manager, would be responsible for developing Code processes, data access arrangements and the Data Register, assessing applications to access the data and potential breaches, would carry out the full administration of the Code. This would allow the Code Panel (Code Administrative Service) to focus solely on decision making and recommendation responsibilities.

Given that market representation would be included on the Code Panel, the CRU was of the view that this option would help alleviate concerns on who can access the data and what data can be accessed.

The CRU highlighted that outsourcing of data security expertise would be necessary to fulfil the role of Code Manager. In terms of compliance assessments, the CRU would have the option of a dedicated Compliance and Enforcement team, removing the need to outsource these functions of the Code.

The CRU asked respondents to give their views on the governance options presented.

2.4.2 Summary of responses

In general, respondents supported the implementation of a governance model that provides confidence and assurance to customers that their respective smart meter data will be used for legitimate purposes. Several responses required more clarity around the roles and responsibilities of the Code Manager and Code Panel to ascertain whether the Code can meet with the requirements of the S.I. and comply with GDPR.

In terms of the governance options included in the consultation, the responses provided various preferences for a governance model. Some respondents favoured the Special Purpose Vehicle model as it assures independence of operation, impartiality and transparency, and that the smart meter data is adequately protected. Several responses highlighted the necessity for a governance model to have expertise in data security and assurance. An alternative governance option in place of the RMDS as Code Manger model was submitted with a stakeholder response.

A number of respondents suggested the Code to be either drafted under Article 40 of GDPR as a Code of Conduct or accredited by the Data Protection Commission (DPC) under Article 41[17] of GDPR. There were several queries raised in the responses about how the relationship between some stakeholders and DPC would work under CRU's preferred model and stressed that these stakeholders' priority is to comply with GDPR first with the Code Manager being kept informed.

Relating to the remediation steps when a breach of smart meter data has occurred, there was general understanding in the responses that existing requirements under GDPR already provide a route for entities, who are data controllers/ processors, to report a breach of such data to the DPC and this needs to be reflected in the Code.

[17] Article 41 GDPR – Monitoring of approved codes of conduct

Several responses requested further clarification on the process in the event of a breach of the code and suggested that the process should cover only the breaches of the Code rather than breaches of personal data which has an established clearly defined process with data protection legislation. Some of the responses asked for the Code to provide further details on the possible sanctions that may be actioned depending on the type of incident.

Some respondents highlighted the role of the Code Panel, specifically, what happens when the breaching party is sitting on the Panel. Other responses suggested that Code Compliance Officer should be accredited by the DPC as provided for in Article 41 of GDPR. Several responses recommended robust auditing before access to smart meter data is granted is necessary to prevent breaches. There were concerns raised by some respondents on the potential double remediation where personal smart meter data breaches are concerned.

2.4.2 The CRU's Proposed Decision

The CRU is proposing the ESB Networks ring-fenced model by delegating the role of Code Manager to the existing ESB Networks ring-fenced entity, MRSO, with both an independent Code Compliance Officer and Chair of the Code Panel. The CRU believe that, through the MRSO, ESBN has significant knowledge and experience in the processing and sharing of the meter data, which includes handling data access requests and is well placed to manage and administer the Code as Code Manager. It is also understood that the MRSO is an already established entity which the CRU considers to be advantageous regarding the timelines to deliver the Code. In terms of setting a new entity up, in the case of a Special Purpose Vehicle, through legislative change, and the Code Administrative Service, through a procurement process, the CRU believe either scenario would lead to impact the timeline to deliver the Code.

The CRU carried out a review internally of the preferred Hybrid model after assessing the consultation responses received. The review highlighted that the Code Manager, in all of the governance options presented, is a Data Controller and subject to obligations under data protection legislation. This signified that CRU would be a Data Controller in the Hybrid Model and combined with the CRUs belief that its focus should solely be on its regulatory function, led to the CRU reconsidering the governance options where the CRU would not be seen as a Data Controller. Furthermore, there is a requirement for the Code Manager to have specialist expertise in data security and privacy when dealing with data access and potential breaches, which would require the CRU to outsource or contract to be able to fulfil the Code Manager role in the Hybrid option.

The most realistic governance options remaining, reconsidered by the CRU, were the Special Purpose Vehicle, the Administrative Service and the ESB Networks Ring-fenced MRSO Option,

which ESB Networks included in their consultation response. With each of these options, CRU is not seen as a Data Controller as it will not make decisions on data access requests and data breaches but as a signatory to the Code, it will maintain oversight of the Code.

The CRU is of the view that the MRSO would be able to acquire, in a timely manner, additional expertise in data security and privacy to develop the processes and assess data requests to be able to run the Code effectively. Considering the CRU's earlier proposal to allow access to be granted ahead of the Code, the CRU considers that the MRSO has the capability, with its significant experience already gained in meter data access requests, to be ready, upon final decision of the Code, to fulfil the role as Code Manager to assess requests / applications and facilitate access to smart meter data prior to the Code go-live date. Furthermore, the MRSO, as a licensed ring-fenced entity, is subject to the condition of the DSO Licence and the CRU's compliance and enforcement framework which the CRU believes that this can address any concerns industry may have with the MRSO proposed as Code Manager. While there were concerns from industry raised about independence, impartiality, and conflict of interest, in terms of the Outsource to the DSO governance model presented in the consultation paper, the CRU believe these concerns can be addressed by procuring an independent body carrying out the Code Compliance Office audit and assurance functions. These functions could also be extended to include data breach investigations, all User assessments, the onboarding process for Parties and Users acceding to the Code and auditing the Code Manager to ensure compliance.

To further mitigate any concerns around independence and impartiality, the CRU believes an independent Chair for the Code Panel, appointed by the CRU, would ensure the Code would be run efficiently and allow for additional oversight on the MRSO as Code Manager. Within the Code Panel setup, complex access requests, data breaches, Code processes and modifications and recommendations from the Code Manager would be assessed and then either approved or rejected by Code Panel via a simple majority method of voting. In terms of the Code being drafted as a code of conduct under Article 40 GDPR, or accredited by the DPC under Article 41 GDPR, this is covered in Section 2.5.3 "The Code as a Code of Conduct". The CRU would like to note that any potential data breaches caused by the Code Manager, or any associated entity, would be managed in closed sessions without the Code Manager and those associated entities present.

The CRU believe that there is a need to keep the proposed governance option under review and that it should not be considered an enduring framework at this time. The CRU will monitor the proposed governance framework in operation and be in a position to adopt a different governance structure if the management of the Code is seen to not be functioning efficiently.

The next section will look at the operational and data protection responsibilities of each of the entities included in the proposed governance model.

Code Operational Responsibilities

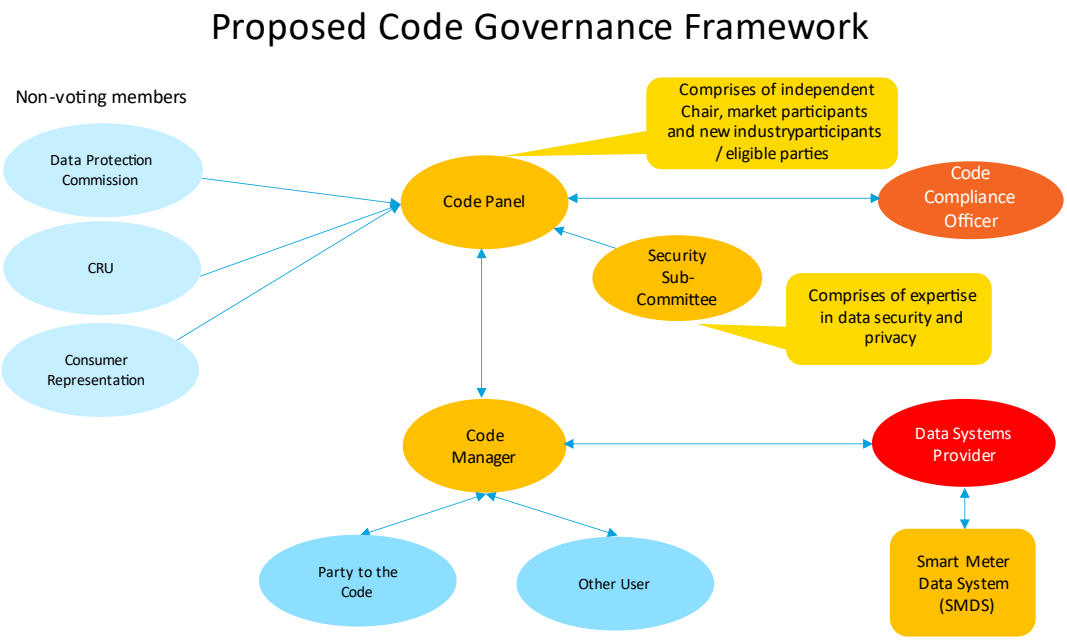

Figure 3 – Overview of the Proposed Code Governance Framework.

The following section considers the operational responsibilities and tasks of the different code entities of the proposed governance model.

Code Manager

The MRSO as Code Manager will provide an administrative and secretarial function, in relation to the management of the Code. The Code Manager will potentially hold any service provider contracts for any system e.g., used for communication to Code entities. Under the proposed governance option, the Code Manager's functions will consist of the following:

- **Receiving and assessing Code Party / Other User access requests / applications**. The Code Manager will be involved in receiving and reviewing requests / application to access smart meter data, provide Code Parties / Other Users access once approved, notifying the DSP to grant access and escalating any requests / applications that include a new user category or new data item to the Code Panel for a decision.

- **Managing access arrangement for Code Parties and access agreements for Other Users**. These arrangements / agreements would set out the responsibilities for Code

Parties / Other Users, with respect to data protection and information security. The Code Manager will submit these arrangements / agreements to the Code Panel for approval and sign-off.

- **Managing any Code modifications.** This would involve managing the secretariat process in relation to Code modifications, including drafting change proposals, coordinating both input into these modifications and the meetings set up to review them and presenting such modifications to the Code Panel. The Code Manager will be responsible for updating and communicating approved changes to the Code e.g. When a new user category is approved by the Code Panel, the Code Manager will raise a change proposal for Code Panel approval, which identifies the criteria to be used in assessing an access application form from a new user category, the purpose for such access, the data items this new category can access and any measures to mitigate risks.

- **Managing Code Panel meetings**. This includes providing a secretariat function that involves meeting timings and invites, meeting minutes and actions, and meeting communications. There could be scenarios where Code entities represented on the Code Panel are subject to a security incident or breach event and such representatives will be excluded from Code Panel meetings where this incident is being reviewed. Consideration will be required as to whether this signifies the Code Manager, by affiliation with the DSO, would need to be excluded from relevant Code Panel meetings, if any part of the DSO group is subject to a breach.

- **Issuing Code Party / Other Users communications**. This involves maintaining the communication list of Code entities, and potentially using software to communicate any Code modifications, meeting invites, guidance issued by the Code Compliance Officer, timings of assessments on Code Parties and Other Users.

- **Maintaining the Data Access Register in relation to Code Parties and Other Users**. This register will detail a) which types of data and whether such data are Personal Data (as per the Data Glossary) that Code Parties, Other Users and other entities can access, b) the User Categories allowed such access; and c) the method of access; d) the legal basis for that access for requests that include personal smart meter data.

- **Market Exit**. In the event of a Code Party's exit from the market and subsequent withdrawal from the Code, the Code Manager will undertake actions involved in offboarding the Code Party, in liaison with the DSP, from the Smart Meter Data System. The Code manager will be responsible for updating records, including the Data Register, and offboarding the Code Party's staff and any associated third parties from the relevant

systems. The Code Manager will notify the Code Panel of this withdrawal and the Code Compliance Officer will update its assessment records.

Code Panel & Security Sub-Committee

Code Panel

The Code Panel is proposed to consist primarily of market participant representation, however, the CRU considers that a balanced make-up for the Code Panel is necessary and the inclusion of representation for price comparison websites (PCWs) and new industry players, considered eligible parties, like demand side units (DSU), aggregator generator units (AGU), renewable energy communities (REC) and citizen energy communities (CEC) would achieve the required balance. The CRU believes this will prevent any Code Panel representatives from potentially acting in their own entities' interest. Further measures like each representative on the Code Panel signing a confidentiality and impartiality agreement before becoming a Code Panel member would ensure transparency in decision making. The CRU will be represented on the Code Panel as a non-voting member. The CRU will be seeking to invite the DPC to be represented on the Code Panel in a non-voting capacity as the CRU considers it would be beneficial for the DPC, as supervisory authority on data protection, to be kept up to date on data privacy and security matters under the Code during Code Panel meetings. Under consideration is how customers could be represented on the Code Panel and the CRU will determine whether a suitable entity exists to fulfil this non-voting member role or whether its own representation can be considered as representing the customer. In terms of decision making, the voting method is proposed to be based on a simple majority, as the CRU considers decisions based on market share, meaning only those representing suppliers, is not seen as a balanced and fair method, when taking into account the other eligible parties that will be on the Code Panel.

The Code Panel is proposed to be informal body of individuals rather than an incorporated entity. In relation to the independent Code Panel Chair to be appointed, the CRU are considering this role to be performed by an individual. Where the Panel Chair signs agreements (Accession Agreements, Access Agreements and potentially a MoU with the DPC), it is likely to do so with its natural personality as an individual acting in a role. Regarding indemnification, the Code Manager is the designed entity under the Code that is proposed to indemnify each Panel member (including the Chair) from and against all costs, charges, expenses, damages or other liabilities incurred by that individual in relation to the exercise of the individual's responsibilities under this Code as Code Panel Chair.

The operational responsibilities of the Code Panel are as follows:

- **Signing Access Agreements / Arrangements.** The Panel Chair has been designated to sign agreements because the Panel is responsible for decision-making on access for Other Users and Code Parties. Whether the Code Manager has legal personality to sign agreements depends on the Code Manager role being included as a function of the MRSO.

  Under Irish law (Section 40(1) of the Companies Act 2014[18]), directors and other registered persons of incorporated companies can bind the company through agreements. This will not extend to the Panel in its proposed format. The CRU will also consider the following options for the Code Panel:

  1.Maintain the Panel Chair as signatory, with limited liability for agreements as included in the minded to governance framework option.

  2.To incorporate the Panel as a registered company, that could allow a more basic assignment of responsibilities and liabilities.

  3.To assign the responsibility for signing such agreements to the Code Manager, subject to the Code Manager role being included to the function of the MRSO.

  4. Provide for the Panel Chair to be a legal entity, rather than a natural person, subject to legal opinion on the viability of this that prevents a legal entity from doing this role.

- **Approving Code modifications**. This will include sign-off on any Code modification that has been considered by the Code Manager. These modifications would then be implemented by the Code Manager.

- **Approving complex requests that include new user categories or new data items**. This involves a review of whether to grant access to smart meter data to a new user category and considers their energy industry related role. These access requests are first assessed by the Code Manager and then escalated to the Code Panel for a decision. The Code Panel will also consider, on appeal, a decision taken by the Code Manager to not admit a Code Party or Other User within an existing user category.

- **Deciding on enforcement actions of Code Party / Other User for non-personal data and Code breaches**. The Code Panel will be responsible for the investigation of an event of breach of the Code, as well as taking steps with respect to the Code Party /

[18] Section 40(1) of the Companies Act 2014

Other User in breach. For personal data breaches, the Code Panel will assist the DPC in its investigation and upon DPC notification, implement an enforcement action.

For other breaches, the Code Panel will decide on what action to take on a Code entity found to be in breach of the Code. Such actions may include a remediation plan, suspension of access to smart meter data, provided the suspension does not impact on licence obligations, or potentially expulsion from the Code. These actions will depend on findings and recommendations from assessments carried out on the Code entity found to be in breach.

- **Derogations.** Separately, the Code Panel will be responsible for deciding on granting a derogation to compliance with provisions in the Code, where it is requested by Code entity and escalated by the Code Manager.

- **Oversight on the Code Manager, Security Sub-Committee and Code Compliance Officer**. This will include delegating actions for the Security Sub-Committee to consider or issue a recommendation, approving parameters and schedules of assessment work for the Code Compliance Officer.

  The Code Manager will be appointed by the CRU and subject to a clarification of the DSO licence being issued to confirm this, the CRU will monitor and consider the Code Manager's performance. Similarly, the Code Compliance Officer will be appointed by the CRU and its performance will be monitored by the CRU. However, the Code Panel will be able to direct the Code Manager and Code Compliance Officer as set out in the Code to ensure the work of both entities under the Code is overseen.

- **Overseeing the procurement of service providers**. This will involve approving the Code Manager's use of a third party or service provider. The contracts for these parties would reside with the Code Manager.

Security Sub-Committee:

This is a new entity proposed that sits with the Code Panel and may contain a number of the same members represented on the Code Panel. The main purpose of this committee is to provide an extra layer of governance and data protection and security expertise. These technical matters relate to certain Code modifications affecting access to smart metering data, decisions with respect to breaches of the Code and assessments of the compliance of Code entities. The CRU is clarifying that final decision-making and any appeals of such decisions rest solely with the Code Panel.

The Security Sub-Committee (SSC) would be responsible for:

- **Reviewing complex access request**s. This will include reviewing complex access requests that involve a new user category or new data item. The committee would also review the report from the Code Compliance Officer on whether the new Code Party or new Other User applicant fulfils relevant criteria and the risks associated with such access.

- **Reviewing Code modifications that affect means and purposes of smart meter data**. The SSC potentially could collaborate with the Code Manager in drafting such modifications. Once the modification is approved by the Code Panel, it is implemented by the Code Manager

- **Reviewing Code modifications that affect obligations in relation to data privacy and information security**. The committee could again be involved in the drafting of these type of modifications and once approved by the Code Panel, it can be implemented by the Code Manager.

- **Managing privacy and security risks and incidents**. This would involve the committee assessing such risks that have arisen from a DPIA or assessment conducted by the Code Compliance Officer and developing a risk management plan with the Code Compliance Officer. For personal data breaches, the committee would work with the Code Panel in assisting the DPC in its investigation.

- **Approving guidance and assurance strategy developed by the Code Compliance Officer**. This strategy would cover good industry practice for data privacy and information security compliance on relevant systems. The committee would review the strategy or guidance aimed at Code Parties / Other Users (and other Code entities). This can include best practice on elements such as developing consent forms for customers, sharing smart meter data with customers and other compliance measures.

Code Compliance Officer

The function of the Code Compliance Officer (CCO) is to provide an independent assessor of compliance within the Code and sharing recommendations on the access to smart meter data for Code Parties / Other Users. This independent assurance role is used in a variety of codes in EU Member states and the CRU believes the inclusion of this entity is necessary to achieve an overall balance within the proposed governance framework.

The role of the CCO includes:

- **Entry and Access Assurance**. In this assessment, the CCO will determine:

- If a Code Party / Other User applicant is to be admitted as a Code Party / Other User and notify the applicant if they are able to accede, as a Code Party, or gain access via an access agreement, as an Other User.
- If any further mitigating measures are necessary
- If access is approved, what information needs to be collected from the Code Party / Other User
- If access is not possible and therefore, not granted.

For parties who are licensed and who wish to accede to the Code, the CCO shall support these applicants through the accession and access processes (Schedule 2 Access Arrangements, Schedule 3 Accession). For Other User applicants requesting access to smart metering data, the CCO shall support such applicants through the access agreement process (Schedule 2 Access Arrangements). The onboarding for both entities will involve an entry assessment with respect to data protection and data security, reviewing the legal basis applicable to access personal smart meter data, determining if further mitigations are required for the licensed party and the drafting and issuing of reports for the Code Panel on the licensed party, which may include recommendations on further actions.

- **Ongoing Assurance**. This involves the CCO Officer carrying out a review of annual self-assessments from Code entities. The assessments would be conducted to confirm data protection and information security controls are in place, that entities are performing their roles under the Code and are complying with all provisions within the Code. The CCO would also support the Code Manager with due diligence on procured service providers / third parties, as required.
- **Assessing and providing support on security incidents / breaches**. The CCO will be notified by Code entities of any security incidents and be tasked with investigating such incidents. For personal data breaches, the CCO will provide assessment and mitigation support to the Code Panel while assisting the DPC in their investigation.

  For breaches of the Code and non-personal data, the CCO will provide recommendations for remediation and enforcement to the Code Panel for a decision. A breach of the Code could occur during an assessment by the CCO or as reported to the CCO by a Code entity.
- **Conducting risk assessment and DPIAs**. This includes the CCO conducting risk assessments and DPIA's concerning processing activities for the Code Panel, for the

purposes of new user categories, new data items, and potential new systems being in place. These assessments could result in Code modifications relating to access to smart metering data. The CCO will be tasked with issuing an initial opinion on whether a DPIA is required (Schedule 2: Access Arrangements)

- **Market Exit**. The CCO would support the Code Manager with the process involving a Code Party exiting the market. With this support, the CCO would need to provide the Code Manager with information and expert advice to determine the withdrawal conditions have been met.

  The process would commence with the Code Manager ensuring that there are no associated license conditions that require the exiting party to be a Code Party and that there are no metering points registered with the party due to a Supplier of Last Resort process. The Code Manager would escalate the withdrawal with the Code Panel, who will instruct the CCO to update its assessment records and seek confirmation from the exiting party and any third-party entities that the smart meter data it has accessed is now deleted, via a self-declaration form developed by the Code Manager. The CCO would also seek confirmation from the DSP that access to the Smart Meter Data System for the exiting party has been removed and that the data access log is updated.

Data System Provider

The Data Systems Provider (DSP) will be responsible for managing the Smart Meter Data System, including information security, access controls, and all data stored in the system.

The DSP has the following operational responsibilities:

- **Maintaining security measures on the Smart Meter Data System**. This will involve the development of an information security management system, a set of policies and procedures, governing information security controls, which includes security around human resources, physical and environmental aspects, and service providers. The CRU is aware that this management system made already be in place and the DSP will maintain this system, including any necessary updates. Furthermore, the DSP will manage access controls, network security controls, incident detection and monitoring on their systems. These controls will be audited on an annual basis (Schedule 4: Data Security).

- **Facilitating access to data for Code Parties / Other Users / Customers.** The DSP has developed an online account interface to allow customers to access their own smart meter data. Additionally, it has been established that the main method of access will be

connected systems and there will also be flexibility to allow for secure file transfer access for bulk smart meter data requests. The DSP will maintain these access interfaces that will allow data to be accessed by Code entities. (Schedule 5: Data Privacy)

The DSP will facilitate the granting of access to Code entities, upon notification from the Code Manager. It will need to ensure the Smart Meter Data System is accessible to Code entities. This will include identification of specified Code entities' users and management of passwords and authentication. (Schedule 5: Data Privacy)

For CRU's proposal to access to smart meter data before the Code is live, the DSP will be in a position to facilitate the access to the Smart Meter Data System once the Code Manager has assessed and approved the request to access smart meter data.

- **Maintaining a data access register in relation to Code Parties / Other Users' access to smart meter data.** This involves monitoring user activity and maintaining audit trails on the Smart Meter Data System to be able to identify access and other system activity by Code Parties / Other Users. The log will detail who has / had accessed customer smart meter data, what data is being / was accessed, and the time period the smart meter data is being / was accessed. (Schedule 4: Data Security; Schedule 5: Data Privacy)

- **Market Exit.** The DSP will support the Code Manager in offboarding a Code Party exiting the retail market. Once the withdrawal has been raised by the Code Manager, the DSP will update their records with respect to the exiting Code Party's staff and associated third parties, if applicable. The DSP will then terminate access and offboard the exiting Code Party's staff from access to the Smart Meter Data System.

  For onboarding, the DSP will support both the Code Manager and CCO in onboarding a Code Party / Other User to the Smart Meter Data System once the entry assessment has been completed. The Code Party / Other User's staff records will be added to the DSP's records for access control management purposes.

<u>Code Party / Other User</u>

Under the proposed governance model, the responsibilities of Code Parties include:

- **Processing personal smart meter data as per its specified legal basis.** Each Code Party / Other User is expected to have its own permitted legal basis (or bases) for accessing personal smart meter data for purposes other than billing requirements, as set out in existing license conditions. Once it has been established that the basis is

complying with data protection legislation, then this basis will be included in the Code Manager's Data Register and access to smart meter data will be granted.

- **Provision of access to their respective customer to their smart meter data.** Code Parties will be responsible for providing their customers access to their smart meter data. This provision includes confirming the identity of the customer before providing such data to them.

- **Maintaining information security systems**. Code Parties / Other Users will maintain an information security management system to provide security controls for staff and respective IT systems used to access and process smart meter data. Code Parties / Other Users will maintain policies covering retention and deletion of smart meter data. CRU is aware that these systems are already established, and Code Parties / Other Users will maintain the systems, including necessary updates.

Data Protection Responsibilities

This section provides more detail on the assignment of data protection responsibilities for the roles involved in the proposed governance option.

Code Governance Entity	**Controller / Processor**	**Role**
Code Manager	Controller	• Processing personal data of persons who are Parties to the Code, for administrative purposes. • Managing categories of Users able to access smart meter data. • Maintaining a list of the type of smart meter data that Users are able to access. • Potential role in maintaining permission list and log, validating permissions.
Code Panel	Controller	• Accession or suspension of Parties to the Code. • Access of Parties to smart meter data when recommended by the Code Manager and / or Code Compliance Officer. • Approval of User Categories and data items under the Code.
Code Compliance Officer	Controller and Processor	• Conducting entry assessment activities and processing personal data of persons who are Code Applicants. • Processing personal data of persons who are Parties to the Code, for administrative and audit purposes.

		• Conducting data protection impact assessments on access of new user categories to smart meter data and potential new data items being made available. • Processing personal data of persons who are Code Manager and DSP for auditing purposes.
DSP	Controller	• Providing access to eligible Parties / Users to smart meter data. • Managing access and other controls on the Smart Meter Data System. • Managing the retention of smart meter data in the Smart Meter Data System. • Managing access logs to the Smart Meter Data System.
Code Parties & Other Users to the Code	Controller	• Legal / contractual / consent requirements allowing the processing of smart meter data from the Smart Meter Data System. • Managing customer rights over smart meter data and other personal data. • Managing the collection of consent from customers, where applicable. • Collecting and validating the identity of customers.

Code Manager

The Code Manager will be a Data Controller, owning to its responsibilities in defining the means and purposes of processing activities with respect to Code Parties / Other Users. The Code Manager's role includes:

- **Maintaining the Data register**: This includes a list of approved user categories and the type of smart meter data each category can access.
- **Managing Permissions Log**: This is a potential role under the new EU implementing regulations for the Code Manager to maintain a permission list and log and validate permissions.
- **Communications**: Collecting and managing Code Party / Other User's staff contact details for onboarding purposes, managing direct communications to these contacts.
- **Meetings**: Managing Code Panel entity staff contact details for organising Code Panel meetings. The Code Manager will decide which data to collect from such staff, how long to store it for and how and when to communicate to these individuals.

In terms of a potential MoU, the Code Panel (or Chair) is seen as the likely Code entity to engage with the DPC to ascertain if a MoU is possible, due to the fact the Code Panel is involved in decision-making in relation to enforcement. However, if the governance model preferred by the CRU or industry is one where the Code Panel Chair does not engage with DPC about a MoU, considering that the Code Panel Chair may leave part way through their term, or may be

replaced, another governance model could involve the Code Manager engaging with the DPC in terms of a MoU. This may also be appropriate in a pre-Code scenario where the Code Manager makes decisions over applications prior to the Code Panel being established.

However, whether a MoU is possible between the Code Manager DPC will depend on:

a) the MRSO is assigned the Code Manager role as a function, subject to a CRU clarification on the DSO licence to permit the MRSO to undertake this legal responsibility. In this case, the MRSO as a legal entity, and thus the Code Manager, could be able to engage with the DPC to explore the possibility of a MoU, as opposed to the Code Panel Chair, or

b) the MRSO is just delegated the Code Manager role. In this scenario, the Code Panel would be the entity to engage with the DPC about a possible MoU.

Code Panel

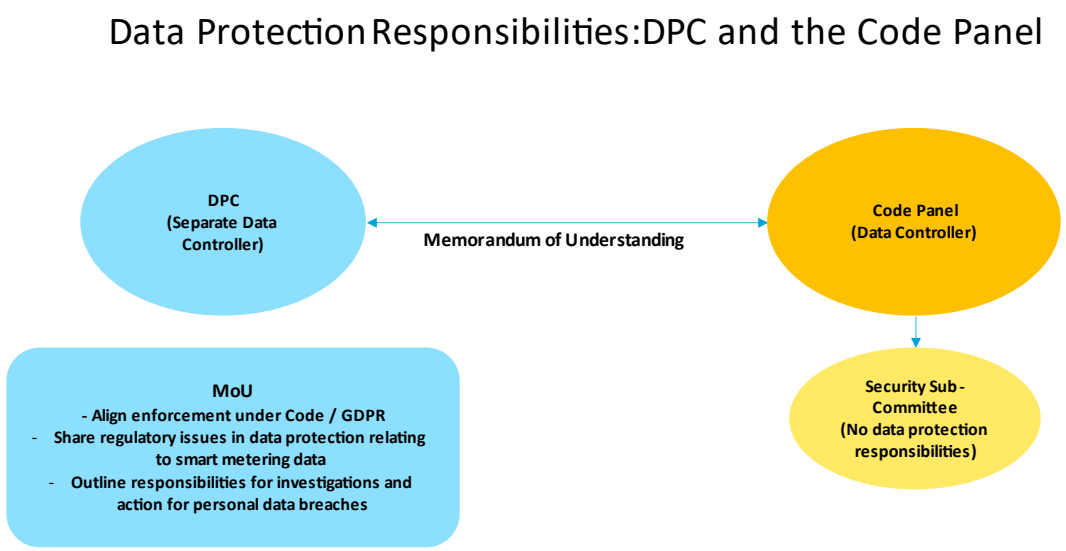

Figure 4 – Overview of the data protection responsibilities between the DPC and the Code Panel.

The Code Panel will be a Data Controller and its data protection responsibilities include:

- **Modifications**: The Code Panel will be responsible for approving modifications that will impact user categories, and ultimately the parties that can access smart metering data, which will affect the means and purposes of data processing activities.

- **Enforcement**: The Code Panel will also be tasked with enforcement, with respect to Code Party / Other Users' access to smart meter data. Concerning personal smart meter data, this enforcement will be determined by the DPC as part of its own investigation. For non-personal smart meter data and breaches of the Code itself, mitigation steps taken by the Code Panel could impact access to smart meter data for Code Parties / Other Users.
- **Third Party / Service Provider**: The Code Panel will be involved in approving decisions to use certain service providers i.e., for the Code Manager's secretariat functions.

The CRU will consider the following arrangements for the Code Panel:

- **Memorandum of Understanding (MoU) with the DPC**: The Code Panel will engage with the DPC to explore the option of a MoU. This MoU could set out the functions of each entity, in terms of personal smart meter data and could separate out responsibilities, the Code Panel for the enforcement of the Code, the DPC for the enforcement of data protection. The MoU would set out a framework governing the sharing of relevant information between each entity for the purposes of each entity's own enforcement. The CRU believes a MoU would avoid overlapping responsibilities and prevent double remediation from taking place.

  The MoU could be signed by Code Panel Chair, and be valid for a set agreed period, subject to reviews should legislative changes occur and / or whether the scope of either the Code Panel or DPC has changed. There needs to be consideration on who is appointed to take on the role of Code Panel Chair and the implications on this legal person / entity in the event of a dispute over a decision. The MoU could also cover the role of the CCO, as the expert body and first Code entity to be notified of potential personal smart meter data breaches. It is not envisaged that the CCO would need to be a party to the MoU, as its investigation and knowledge sharing would be reported to the Code Panel in any case.

  The MoU could be seen as necessary, in the absence of the Code constituting a Code of Conduct that can be enforced, and could be developed to support:

  - **Regulatory Alignment**: The MoU could align the scope of regulatory enforcement between the DPC and the Code Panel where these enforcement responsibilities are seen to overlap i.e., A breach of the Code is also a breach of data protection legislation.
  - **Knowledge Sharing**: The MoU could facilitate knowledge sharing around key issues and challenges in data protection with respect to smart meter data.

- **Enforcement**: The MoU could identify areas of responsibility for both entities to mitigate against double regulation. For example, the DPC could be set as the primary body responsible for investigating personal smart meter data breaches and the DPC will liaise with the Code Panel during the investigation, and that the DPC could outline any remediation action required. This could help avoid a secondary investigation and enforcement being carried out by the Code Panel.

Within the context of the Code, the MoU could set out expectations for each entity to follow and could cover the roles of both entities for enforcement, information sharing, frequency of meetings, any data sharing arrangements where personal smart meter data or personal data of Code Parties / Others' staff, and confidentiality controls.

Under the MoU, both entities could share information relevant to enforcement, which potentially may include limited commercially sensitive information, rather than personal data of Code Parties / Other Users' staff. As such, a data sharing agreement would not be seen as necessary between the Code Panel and the DPC, which would then signify both acting as separate Data Controller, each having their separate enforcement responsibilities. Should personal data be shared in the future, then a data sharing agreement could be considered.

- In the event that a MoU is not possible with the DPC, the Code Panel could invite the DPC to examine and investigate processes under the Code, relating to personal smart meter data, that are seen not be working correctly, with respect to data protection legislation.

Security Sub-Committee

The Security Sub-Committee (SSC) will not be a Data Controller as it will solely make recommendations to the Code Panel on data security, data privacy and processing activities, which are subject to Code Panel approval. Furthermore, the Code Panel will delegate actions to the SSC and as such, it is unlikely that any data sharing arrangements will be required.

The SSC will draft recommendations on modifications and risk management, which can include assessment of data security and data privacy under the Code. It will also review any guidance or assurance strategy developed by the CCO.

Code Compliance Officer

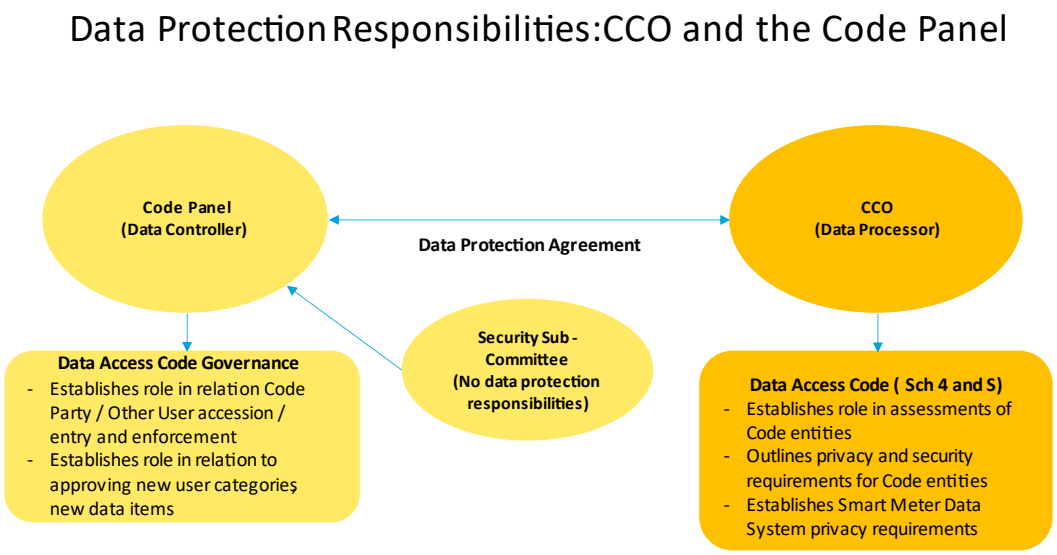

Figure 5 – Overview of the data protection responsibilities between the CCO and the Code Panel

The CCO will primarily be a Data Processor responsible for processing activities involving Code Parties / Other Users' staff personal data and customer smart meter data. The CCO is unlikely to exercise discretion over personal data collecting during assessments as its methodology, evidence collection and activities for assessments will either be defined by the Code Panel, with SSC recommendation, or set out in the Code. All of the CCO's actions will be reportable to the Code Panel, including assessment reports that are subject to the Code Panel decision.

The CCO's Data Processor role will include:

- **Applications**: Assessing entry applications to gain entry to the Code and supporting Code Parties / Other Users during the onboarding process. This will involve collecting and managing contact information of Code Parties / Other Users' staff and deciding on which data to collect and how long to store the data for.
- **Assessments**: Receiving and processing the personal smart meter data of customers and personal data of Code Parties / Other Users' staff, as necessary for conducting assessments of these entities, from a data protection and data security aspect.
- **Incidents**: Receiving and processing the personal smart meter data of customers and personal data of Code Parties / Other Users' staff, as necessary for incident investigation and management purposes.

The Code will set out the Processor arrangements for the CCO for its role in assessments. In addition to this, the CCO will enter into a data protection agreement with the Code Panel, which will include terms in relation to the CCO's responsibilities as a Data Processor, and this agreement aligns with Article 28 of GDPR legislation[19].

Data Systems Provider

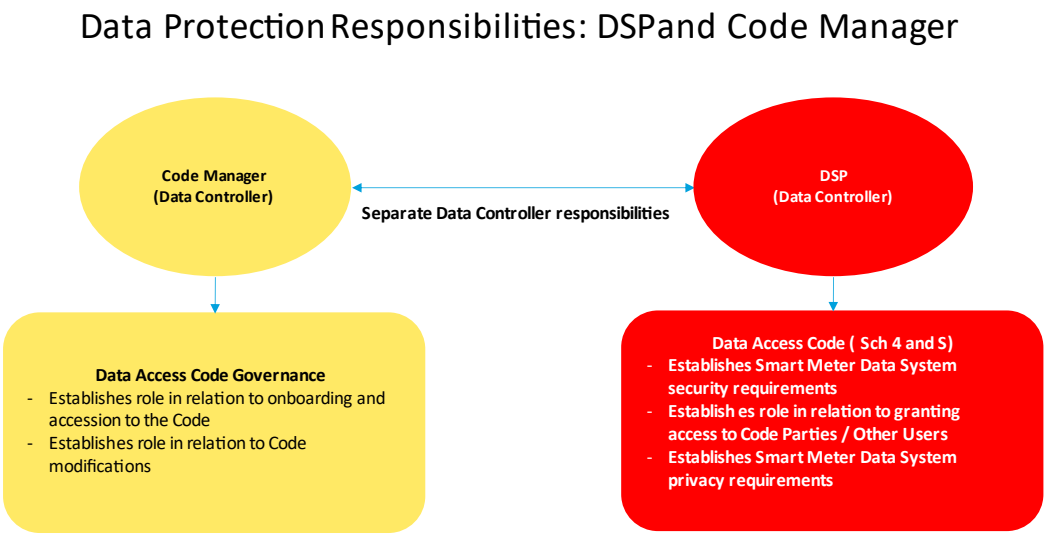

Figure 6 – Overview of the data protection responsibilities between the DSP and the Code Manager

The Data Systems Provider (DSP) will be a Data Controller, and its responsibilities include making decisions on the non-essential means of processing, which involves which hosting platform to use and network security controls, providing and managing access to the Smart Meter Data System to Code entities, and deciding on how long to retain audit and access logs for access to the Smart Meter Data System.

The DSP will be a separate Data Controller as it will define the means and purposes of processing for its own purposes i.e., granting access, managing security incidents, facilitating access to smart meter data to customers. The DSP data protection activities will involve:

[19] Article 28 of GDPR

- **Access Controls**: Providing access to the Smart Meter Data System to staff of Code entities, including maintaining administrative roles to manage this access for the relevant individuals.
- **Audit Logs**: Conducting monitoring of the activities of Code entities' staff accessing the Smart Meter Data System, which includes defining the time period for which audit logs can be stored.

Therefore, the CRU does not envisage the DSP requiring any other data sharing arrangements under the Code.

Code Parties / Other Users

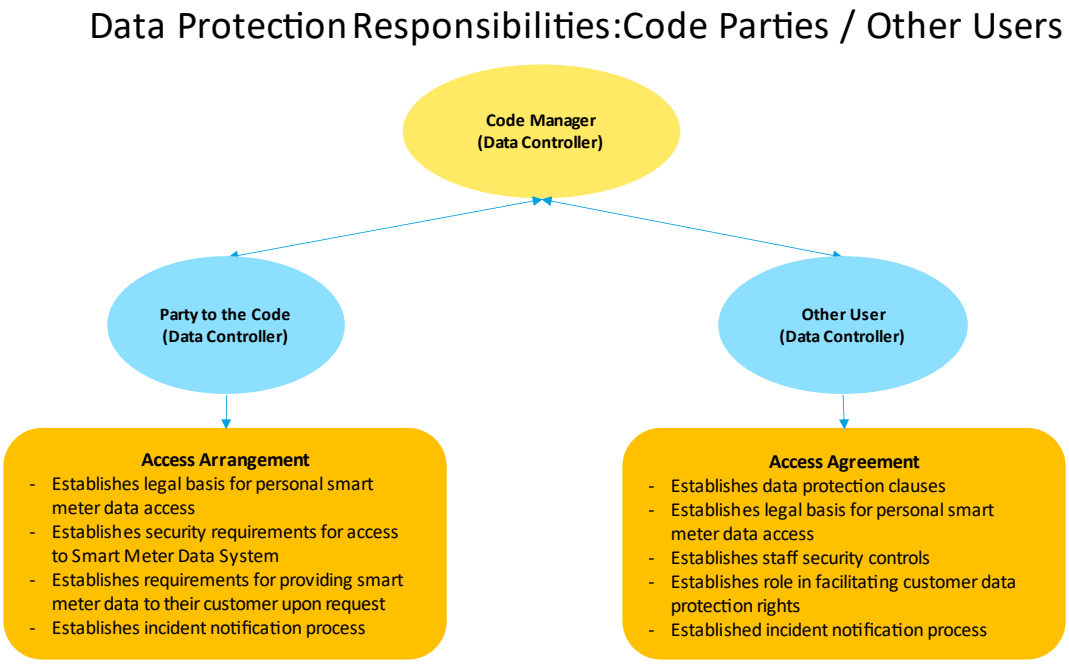

Figure 7 – Overview of the data protection responsibilities between the Codes Parties / Other Users and the Code Manager

Code Parties will be Data Controllers, considering they will be expected to have their own legal bases for accessing and processing personal smart meter data and their own obligations relating to the collection of consent from the customer, as appropriate. Code Parties will be responsible for ensuring that their customers are provided with their respective smart meter data at their request. This particular role will be further defined the final version of the Code.

As Code Party responsibilities, with respect to personal smart metering data, will be outlined in the Code, the CRU does not see any other data sharing arrangements being required for Code Parties.

Other Users will also be Data Controllers, noting they will be expected to either have their own specific contractual obligation to customer or consent from the customer for the purpose of accessing and processing personal smart meter data. Other Users will be required to sign access agreements under the Code, which will cover data protection and information security clauses.

Similarly for Other Users responsibilities, these will set out in the Code and the CRU does not see any further data sharing arrangement being required for Other Users,

The CRU

Under the Code, the CRU will have the following responsibilities:

- **Governance:** Conducting a role in approving governance modifications to the Code that do not impact on the processing of personal smart meter data.
- **Enforcement:** Undertaking its own enforcement decisions and activities outside of the scope of smart metering data processed under the Code

The following section looks at the potential scenarios that were considered where CRU could be viewed as a Data Controller and the mitigations that are expected to be place under the Code.

Code Panel Decision Making

The CRU will not have a role in decision-making in managing user categories, data items and accessions to the Code under the Code Panel. The CRU will only have non-voting representation on the Code Panel and as such, it would not be a Data Controller, as it would not be able to influence decisions over processing of smart meter data. The Code Panel itself will conduct a high-level role in defining the means of processing, where the management of decisions made by the Code Panel will be carried out by the Code Manager and Code Compliance Officer.

Appeals

In terms of appeals from decisions made by the Code Panel, the CRU, as the competent authority, may act as an escalation point, allowing Parties to the Code / Other Users to appeal Code Panel decisions to the CRU. In this situation, the CRU is likely to be seen as a separate Data Controller, depending on how its activities are defined under the Code.

In addition to this scenario, the CRU would be involved in processing personal data of persons who are Parties to the Code / Users for appeal purposes, which is not subject to the Code. Much of the consideration of whether the CRU is a Data Controller for such appeals depends on whether it recommends processing activities to a Party to the Code / User, making it a Data

Controller, or whether its role involves affirming or not approving the Code Panels decision, which would place the CRU as a separate Data Controller, as it would be acting as an independent supervisory authority.

To prevent the CRU from being considered a Data Controller in this instance, the proposed governance framework could be drafted to allow appeals, relating to the means and purpose of processing smart meter data, against Code Panel decisions to be considered by the Security Sub-Committee. The CRU proposes to ensure that appeals escalated to the CRU, other than those relating to the means and purpose of processing personal smart meter data, will be included as an appeals process in the final version of the Code. Any such appeals would be carried out by the CRU in its independent capacity as the recognised regulatory authority, via a mechanism separate from decision-making by the Code Panel.

Drafting of the Code

The CRU believes that the ability to develop rules on the purpose of processing personal smart meter data is constrained by legislation rather than allowing discretion to the CRU. The CRU's role in drafting the Code will be limited to high-level objectives rather than the means and purposes of data processing activities.

For any potential system design that may involve the purposes of data processing, and where the CRU is involved, this will indicate that the CRU is a Data Controller. It is understood that the Code Manager, Code Compliance Officer, DSP, and Parties to the Code / Users will be Data Controllers in their own rights and will therefore take most of the obligations under the Code as Data Controllers. This is due to their involvement in choosing the means and purposes of data processing by means of their respective policies and governance frameworks, rather than this decision being made for them by the CRU during the drafting of the system design under the Code. Overall, whether the CRU is a Data Controller for the drafting of the governance framework is dependent on how much the CRU will follow legislative models or use its own discretion in governance design.

To avoid the CRU exercising discretion over any potential changes to relevant legislation that the Code sits under, is it important that DECC is seen to be the responsible entity for any legislative drafting and the CRU delegates the drafting of implementation of such legislation to its technical advisors. Once the Code is live, it will be maintained by the Code Manager and Code Panel. The CRU notes that any requirements on reporting on national practices related to smart meter data access will be kept separate from the drafting of the Code.

Code Amendments / Modifications

The CRU could be involved in sharing an opinion and potentially approving certain amendments to the Code once it is live which could be viewed as involvement in defining the means of data processing, when choosing when or which parties can access smart meter data. As such, approving such amendment as above could render the CRU as a Data Controller.

To mitigate against this likelihood, any amendments that require approval from the CRU could be limited to governance. This prevents the CRU being a Data Controller involved in amendments on assessing user categories or data items. Additionally, the CRU believe that the Code Manager and the Code Compliance Officer should be given discretion on assessing user categories / data items before access is granted. This limitation on CRU approving amendments is proposed to be drafted in the finalised version of the Code.

The DPC

The DPC will be invited to become a non-voting member and in the event of such, will not be expected to have any responsibilities under the proposed governance framework. Outside of the Code, it has separate responsibilities such as:

- Assessments: Conducting investigations and assessments of compliance with data protection legislation.
- Enforcement: Conducting its own enforcement decisions and activities, which can include enforcement notices, warnings, injunctions, remedial action, or administering fines for breaches of data protection legislation.

As discussed previously, The Code Panel will engage with the DPC to explore the option of a MoU. This arrangement could set out a framework governing the sharing of relevant information between both parties for the purposes of regulatory enforcement and could prevent overlap of responsibilities and double regulation and enforcement from taking place.

Question 3: CRU welcomes views on the minded to model for the governance and enforcement of the Smart Meter Data Access Code.

2.4.4 EU Implementing Regulation

The CRU acknowledges the recent adoption of the new EU Implementing Regulation 2023/1162 and Annex[20], which covers interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data, regarding Article 24 of EU Directive 2019/944. The implementing regulation includes clearly defined roles and responsibilities and sets out rules and procedures that Member States must apply to ensure interoperability.

The CRU has considered these new requirements and established an indicative outline of the assigning of the implementing regulation roles within the proposed governance model, which includes data protection responsibilities, as follows:

Implementing Regulation Role	**Definition**	**Proposed Governance Framework Assigned Entity**
Metered Data Administrator	Entity responsible for storing validated historical metering and consumption data and distributing these data to final customers and/or eligible parties	Primary: DSP Secondary: Code Manager
Metering Point Administrator	Entity responsible for administering and making available the characteristics of a metering point, including the registrations of eligible parties and final customers linked to the metering point	Primary: Code Manager / DSP
Data Access Provider	Entity responsible for facilitating access, including in cooperation with other parties, to validated historical metering and consumption data by the final customer or by eligible parties	Primary: DSP Secondary: Code Manager
Permission Administrator	Entity responsible for administering a register of data access permissions for a set of metering points, making this information available to final customers and eligible parties in the sector, on request	Primary: Code Manager Secondary: DSP
Identity Service Provider	Entity that manages identity information; issues, stores, protects, keeps up to date, and manages identity information for a natural or legal person and provides authentication services to eligible parties and final customers	Primary: Code Manager / DSP

[20] Implementing Regulation for access to metering and consumption data and Annex to the implementing Regulation for access to metering and consumption data (EU) 2023/1162

The responsibilities for each of the implementing regulation roles are as follows:

- **Metered Data Administrator (MDA):** This involves making validated historical metering and consumption data available to customers and maintaining a data access log and make it available to customers on request. For eligible parties' access to such data, with respect to data protection legislation, the MDA is responsible for ensuring that there is an active permission or legal basis for the data to be accessed and processed.

  The DSP is the most suitable entity to take on the role of MDA as it manages and maintains the Smart Meter Data System where the smart meter data is stored. The DSP currently makes validated historical metering and consumption available to customers through their online account. In terms of validating an active permission or legal basis to make such data available to eligible parties, the Code Manager's contribution to the MDA role will involve assessing requests to access smart meter data, which includes confirming a legal basis for accessing and processing that data, and on approval, notifying the DSP to make the data available.

- **Metering Point Administrator (MPA):** The MPA must notify the permission administrator and the metered data administrator of any changes in the assigning of customers to metering points.

  The CRU considers the Code Manager to be best suited for this role. The MRSO, as Code Manager, is presently responsible for linking a metering point to a customer and maintaining the meter point characteristics. The MRSO also has due discretion in updates to metering points i.e., changes as part of a Change of Supplier or Supplier of Last Resort process and must informs the relevant market participants of any such changes or updates to metering points. The CRU is aware that the DSP will likely be involved, as part of the processes mentioned above, in the fulfilment of the MPA role.

- **Data Access Provider (DAP):** This role involves making publicly available, through an online interface, all procedures relevant to providing access to validated historical metering and consumption data to customers. The DAP must also maintain customer log information, which includes a timestamp of when an eligible party or customer has been given access to their data and the type of data accessed and make it available to customers on request.

  The CRU considers the DSP as the primary entity to carry out this role. This is due to the assigning of the DSP to the role of MDA whose responsibilities are similarly defined, providing validated historical metering and consumption data to customers, and maintaining an access log and making it available to customers on request. Again, the

Code Manager is likely to be involved in the DAP role, tasked with providing rules for access to data as well as assessing data requests / applications and upon approval, notifying the DSP to grant access.

- **Permission Administrator (PA):** This role involves granting permission to eligible parties to access to validated historical metering and consumption data and revoking such permissions on a customer's request. An overview of active and historical permissions must be shared with the customer on request. The PA must also process notifications and inform the MDA, eligible party, and customer about invalidated permissions. A permission log must be kept for customers and made available to the customer on request.

  The CRU's initial view is that this role is primarily assigned to the Code Manager. In terms of assessing requests / applications to smart meter data, the Code Manager will review the permission / legal basis before approving the request and will be responsible for maintaining a permission log as well as the Data Access Register or a combination of both. Similarly, the DSP, who grants access to smart meter data upon Code Manager notification, could maintain a permission log in addition to the data access log under the MDA role.

- **Identity Service Provider (ISP):** This role is focused on identity management and authentication identity services to customers and eligible parties.

  The CRU considers this role to be carried out by either the Code Manager or the DSP as both are best placed to store and manage the identity of the customer. The Code Manager, similar to the PA role, is likely to naturally maintain a permission log given its role in assessing data requests / applications. One of the functions of the Code Manager is to develop Data Access Register, which is expected to include the permission / legal basis used to access the smart meter data. The DSP is likely to be involved in the ISP role in some capacity, primarily to verify the identity of a customer against its own records.

  There is also consideration that this role could be outsourced to a service provider with expertise in identity and authentication management.

The CRU is engaging with its own legal team and DECC to see if legislative amendments and / or license condition clarifications can be made to determine how and to whom each of these roles can be assigned, in the context of the Irish electricity retail market.

Access to validated historical metering and consumption data by the final customer.

One of the set procedures in the implementing regulation that Member States must implement is access to validated historical metering and consumption data by the customer. This procedure will be discussed in the context of how the proposed governance framework entities perform the defined roles, given that access to such data is presently being provided to customers by the DSP through their online account.

1. Customers identify the DAP, in this case the DSP as the primary entity, and identify themselves through communication with the DSP or registering to the DSP's online account. (Steps 1.1., 1.2)

2. With multi-factor authentication, the DSP confirms the identity of the customer, and the customer can now complete the registration process online (Steps 1.3, 1.4)

3. The customer must then link their metering point ID, their MPRN, to their online account to be able to access and view their own validated historical metering and consumption data. With this linking of MPRN, the metering point is validated, and the data for that metering point is then automatically presented in both graphical form and downloadable format on the customer online account. (Steps 1.5 – 1.12)

   In this process the DSP is performing the MDA, DAP, and ISP roles, removing the need to notify a different entity for authenticating identity, validating the data request, and providing the requested data. Customers do not need to specify the requested data as the online account automatically provides the validated historical metering and consumption data, once customer has linked their MPRN, metering point, to their account. Given that the reference model contained in the ANNEX to the implementing regulation allows for procedural steps to be combined or carried out in a different order, the CRU believe that the first set procedure is likely to be seen as implemented. However, the CRU is aware of the lack of an identity service authenticating the customer's identity covered in step 1.3. While the customer can identify themselves to the DAP, the implementing regulation stipulate that an identity service provider validates the identity of the customer to the DAP and the DAP then notifies the customer of the authentication result.

The CRU is currently reviewing the remaining five set procedures and will confirm how each of the defined roles will be assigned to entities in the proposed governance model in the decision paper. These five procedures are as follows:

- Access to validated historical metering and consumption data by an eligible party. The customer identifies the eligible party that they intend to make their own data available to.
- Termination of service by an eligible party. Here, the eligible party notifies the PA of the expiration of a permission and the MDA stops the access to data.
- Revocation of an active permission by the customer. Upon receiving a list of active and historical permissions, the customer informs the PA which active permission will be revoked.
- Activate near real-time data flow from smart meter or smart metering system. In this instance, the customer requests near real-time data from the meter operator.
- Read near real-time data from smart meter or smart metering system. Dependent on the previous procedure, this allows the customer to then read the real-time data, now activated, via an interface.

The CRU is reviewing the impact the new implementing regulation potentially has on Regulation 6 of S.I. 37 of 2022, which the Code falls under, and determining if there is scope to amend this regulation of the statutory instrument to align or at least refer to the implementing regulation. The CRU considers that the Regulation 6 provisions, as currently drafted, merit amendments being made to them by DECC considering the implementing regulation. Considering that the primary legislation, EU Directive 2019/944, sets out that rules around smart meter data access must be developed by each Member State and that the new implementing regulations now provides a clear set of rules and procedure around access to metering and consumption data, which falls under the definition of smart meter data, the CRU believe that a review of Regulation 6 of the statutory instrument is necessary. An example of this is shown below for the definition of eligible parties in both pieces of legislation:

S.I. 37 of 2022 – *eligible parties" means persons authorised under the Smart Meter Data Access Code to access smart meter data, in accordance with the provisions of that Code;*

EU Implementing Regulation 2023/1162 - *eligible party' means an entity offering energy-related services to final customers, such as suppliers, transmission and distribution system operators, delegated operators and other third parties, aggregators, energy service companies, renewable energy communities, citizen energy communities and balancing service providers, as far as they offer energy related services to final customers;*

The differences between both regulations are shown clearly here, whereby the Code seems to determine who is an eligible party under the S.I., but the eligible parties are concisely defined in

the implementing regulation. The CRU will engage with DECC on these notable differences to determine whether amendments can be made to the S.I.

Furthermore, the defined roles prescribed in the new implementing regulation likely apply to the following Code entities; DSP and Code Manager as has been highlighted above. From this, there seems to be merit in the CRU re-evaluating the roles of the remaining proposed Code entities of the Code Panel, Security Sub-Committee and Code Compliance Officer to determine what level of oversight will be needed, if any, when considering the implementation of the rules and procedures provided in the implementing regulation.

Given that the statutory instrument, as currently drafted, includes provisions that the Code must perform, the CRU see the proposed governance model as the appropriate framework to execute these provisions. However, the CRU is also aware there needs to be consideration on whether the proposed model fits efficiently into the implementing regulation reference model, with an understanding that further implementing regulation will be developed by the European Commission concerning interoperability requirements for data required for customer switching, demand response and other services.

In relation to the CRU's proposal on access to smart meter data ahead of the Code going live, the CRU believe that the proposed Code entities that would be expected to be in place, upon the decision paper and final version of the Code publication, are the DSP, MRSO (proposed as Code Manager) and Code Parties / Other Users. The CRU considers that these already established entities (DSP, MRSO Code Manager function subject to licence clarifications) would have the competence to implement the reference model and its procedures effectively, as was proven previously, when assigning the implementing regulation roles to these entities.

The CRU considers that both the DSP and MRSO are the appropriate Code entities to implement the reference model, as set out in the implementing regulation. The CRU believe that the MRSO, as proposed Code Manager, in having the necessary experience in dealing with meter data requests and ensuring adequate expertise in data security and data protection. can assess requests / applications to access smart meter data and approve access pre-Code. The CRU considers that the MRSO can carry out the MPA and PA role prescribed in the reference model in the implementing regulation. Similarly, the DSP, with its significant experience and expertise in data security and data protection, is well placed to facilitate access to smart meter data once the request / application has been approved and CRU is of the view that the DSP can fulfil the combined roles of MDA and DAP in the implementing regulation. Finally, the CRU believe that the Code Manager and the DSP are best placed to efficiently take on the roles of PA and ISP defined in the implementing regulation, through a service provider, if it is considered necessary.

The CRU is welcoming views from industry and interested parties on the most suitable governance model for the Code, including the proposed governance option provided in this paper, to perform the rules and procedures set out in the implementing regulation.

Question 4: The CRU would welcome any views from industry and interested parties on the most suitable governance framework to implement the rules and procedures of the implementing regulation.

2.5 Data Security and Data Privacy Obligations

2.5.1 Summary of consultation position

The obligations for data security were set out in this section and applied to all Parties and Users who can access or request access to smart meter data from the Smart Meter Data System.

The DSP obligations, as the entity responsible for oversight of the Smart Meter Data System, are to establish policies and procedures known as “DSP Information Security Management System”, which include the DSP approach to security of information, policy development around access control, risk identification and mitigation regarding data security and processes that cover management of information security incidents.

For Users who apply to access to smart meter data, the data security obligations are set in each Access Agreement, which is dependent on the data requested. They must submit details on internal information security, data protection risk assessment, and a completed GDPR checklist to the Code Manager. If the Code Manager has concerns over the submitted information, the User is notified to carry out corrective action before any access to smart meter data is granted. Once the request has been granted, an Access Agreement is developed for the User and this includes data security obligations, which are set and are dependent on the data requested.

Where unaggregated bulk smart meter data is being requested via an application, the User needs to show compliance to an information security standard, including processing of personal data, which they believe meets the data security requirements contained within this schedule.

For Parties to the Code who become Users when accessing smart meter data, there is a requirement to establish their respective policies and procedures known as a User Information Security Management System that include information security, access control and management of information security incidents. Each Party must also develop and maintain a User Data Retention Policy.

In terms of the accessing and processing of personal data from the Smart Meter Data System, the data privacy obligations set out in this schedule for Parties and Users were discussed.

The DSP, Parties to the Code, and Users with Access Agreements will be deemed Data Controllers as they will each be determining the purposes for which and the means by which personal smart meter data is processed. There will be Users that are Data Processors, processing personal smart meter data on behalf of a Data Controller.

Before requesting personal smart meter data from the Smart Meter Data System, Data Controllers, including the DSP, must ensure that consent / legal basis is present, customers are informed of the use of their personal smart meter data, and their rights around consent and data access and removal requests. Additionally, Data Controllers, shall guarantee that only authorised individuals, who are committed to confidentiality, are allowed to process personal smart meter data, and must notify the DPC and Code Manager within 4 hours of a personal smart meter data breach.

Where a service provider is used by the DSP to process smart meter data, the service provider must follow the documented instructions of the DSP, including agreeing to process data for a specific time period, and notifying the DSP of any other service provider involved in the data processing, personal data breaches, data subject requests, and complaints relating to the processing of data under the Code.

For Users who will be Data Processors, they are obliged to only access and process data for a specific period as authorised in an Access Agreement (Schedule 2) or providing a service for a Data Controller. Data Processors must adhere to data protection legislation in terms of informing customers of how they can access their personal data and exercise their rights to this data. The same data privacy obligations placed on Data Controllers apply to Data Processors.

The CRU asked respondents for their views on the data security and data privacy obligations discussed in this section.

2.5.2 Summary of responses

With regard to data security, generally, respondents were in agreement that data security obligations are necessary before accessing smart meter data but stressed the obligations need to be line with their existing requirements under data protection legislation.

Some responses highlighted that any data security assessments must be clearly specify the exact requirements a party must have in place to be provided with access to smart meter data. Other respondents suggested the level of security assessment should depend on the type of

data being shared i.e., firmer restrictions for personal data and lighter procedures for non-personal data.

There was an expectation from some responses that required procedures under the data security obligations should be the same for all entities, irrespective of whether an entity is licensed or not. It was noted in several responses that for the DSP, there needs to be obligations in place that are similar to Parties to the Code / Users, in terms of notification of security incidents and compliance to a recognised information security standard. One response suggested regular formal reviews and / or audits would be an appropriate control to ensure alignment with data security standards.

In terms of consent, several respondents asked that the GDPR definition of consent should be used in place of appropriate consent that is used in the Code, to enable all entities, who rely on the legal basis of consent to get access to smart meter data, to clearly understand whether the conditions of consent apply to their request to access data.

For the data privacy obligations, there was general agreement among the respondents that these requirements mostly aligned with data protection legislation. Some responses cautioned on the Code potentially duplicating data protection legislation and suggested that the Code should supplement the regulation.

Most of the responses highlighted the data privacy obligations that already exist under GDPR and proposed that any requirements under the Code should be clearly outlined, with consideration of existing data protection obligations, for all entities to understand and manage appropriately.

2.5.3 The CRU's proposed decision

The CRU is cognisant of the existing requirements under data protection legislation that Code Parties / Other Users are subject to, and the CRU would like to reassure industry that the proposed Code obligations on data security and data privacy considers these requirements. The CRU believe it is up to Code Parties / Other Users to ensure their respective systems and procedures on data security and data protection are compliant before requesting / applying for access to smart meter data. Given that systems and access controls need to be upgraded / validated to be able to access data from the Smart Meter Data System, these requirements are considered necessary under the Code.

In the consultation paper, it was highlighted that for the purposes of accessing personal smart meter data, Code Parties / Other User are deemed Data Controllers as they determine the means and purposes to process personal data. The CRU understands that Code Parties / Other

Users have established data privacy obligations under GDPR legislation, and the CRU re-iterates that the Code's proposed data privacy obligations will not impede on these existing requirements that Code Parties / Other Users are subject to.

The CRU acknowledges the need for the GDPR definition of consent being applied within the Code provisions to give Code Parties / Other Users, who depend on this legal basis, a clear understanding of the necessary conditions required to access personal smart meter data. The CRU recognises that the proposed data security and data privacy obligation set out in the Code should be applicable to the DSP also to ensure that all Code entities are subject to the same provisions and the Code will be updated to reflect this.

In terms of Code Parties / Other Users looking to gain entry to the Code and access to smart meter data, the proposed entry assessment carried out by the CCO, as part of the onboarding process which includes the Code Manager and DSP, will now be considered.

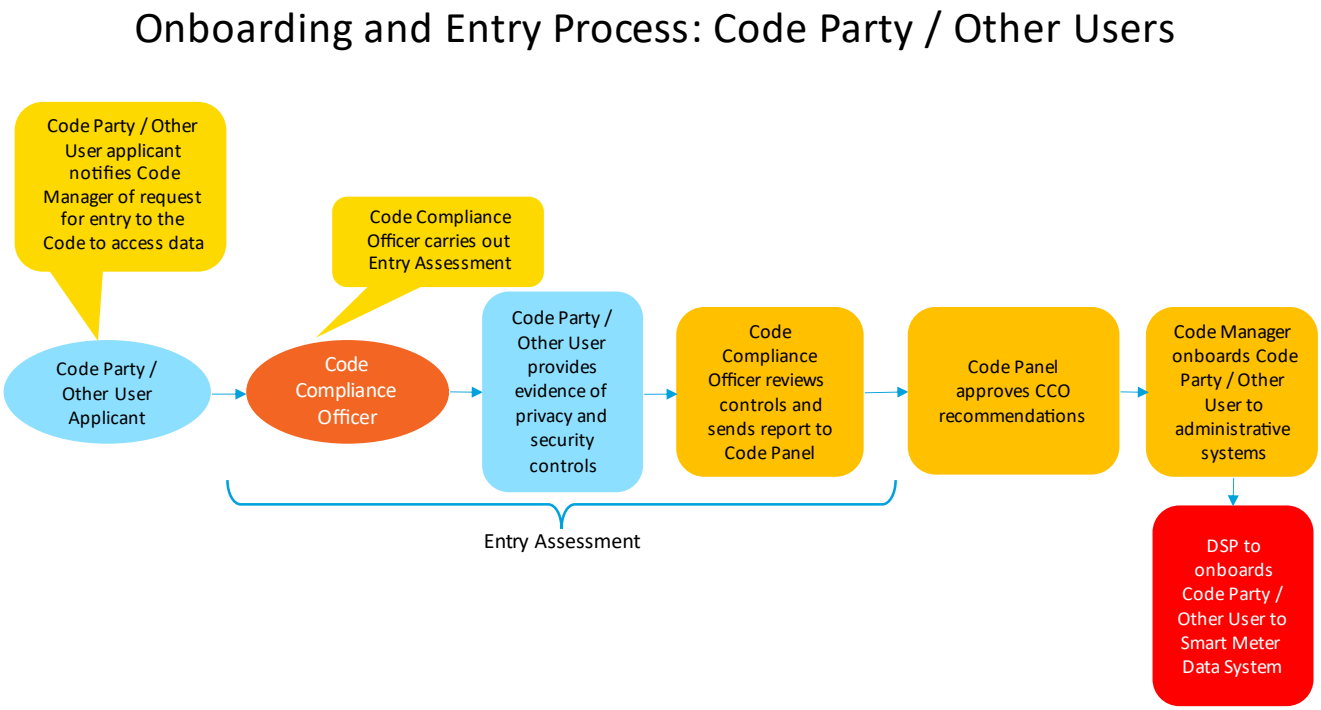

Figure 8 – Overview of the onboarding process for Codes Parties / Other Users

Code Parties / Other Users seeking to gain entry to the Code to access smart meter data will notify the Code Manager, who in turn, informs the CCO, to carry out the entry assessment. The Code Party / Other User must provide evidence of data privacy controls, which includes a legal basis for personal smart meter data requests, and data security controls. The CCO reviews the controls provided by the Code Party / Other User and provides a report with recommendations to the Code Panel. Another potential outcome is the CCO, during assessment, decides that further

information or remedial action, in the case where risks are identified, and the Code Party / Other User implements the mitigating measures and resubmits the required evidence. The Code Panel ratifies the recommendations from the COO and the following onboarding processes apply:

- Code Manager onboards the Code Party / Other User to the administrative systems developed for the Code.
- The DSP onboards the Code Party / Other User to the Smart Meter Data System.

Once the onboarding is completed, the Code Manager updates the Data Access Register to include the Code Party / Other User and its approved access, the legal basis for personal data, the type of data that was accessed, and the method of access used. This allows the Code Manager to identify the permitted access to data and informs the DSP of the data to be made available on an ongoing basis. It is important to add that any request from a Code Party / Other User for smart meter data that does not fall into an existing approved access arrangement / agreement will require further assessment by the Code Manager to ensure data privacy and data security requirements are in place prior to the request being approved. If such requests include a data item that is not currently available in the Smart Meter Data System, and not defined in the Data Glossary, the following process applies:

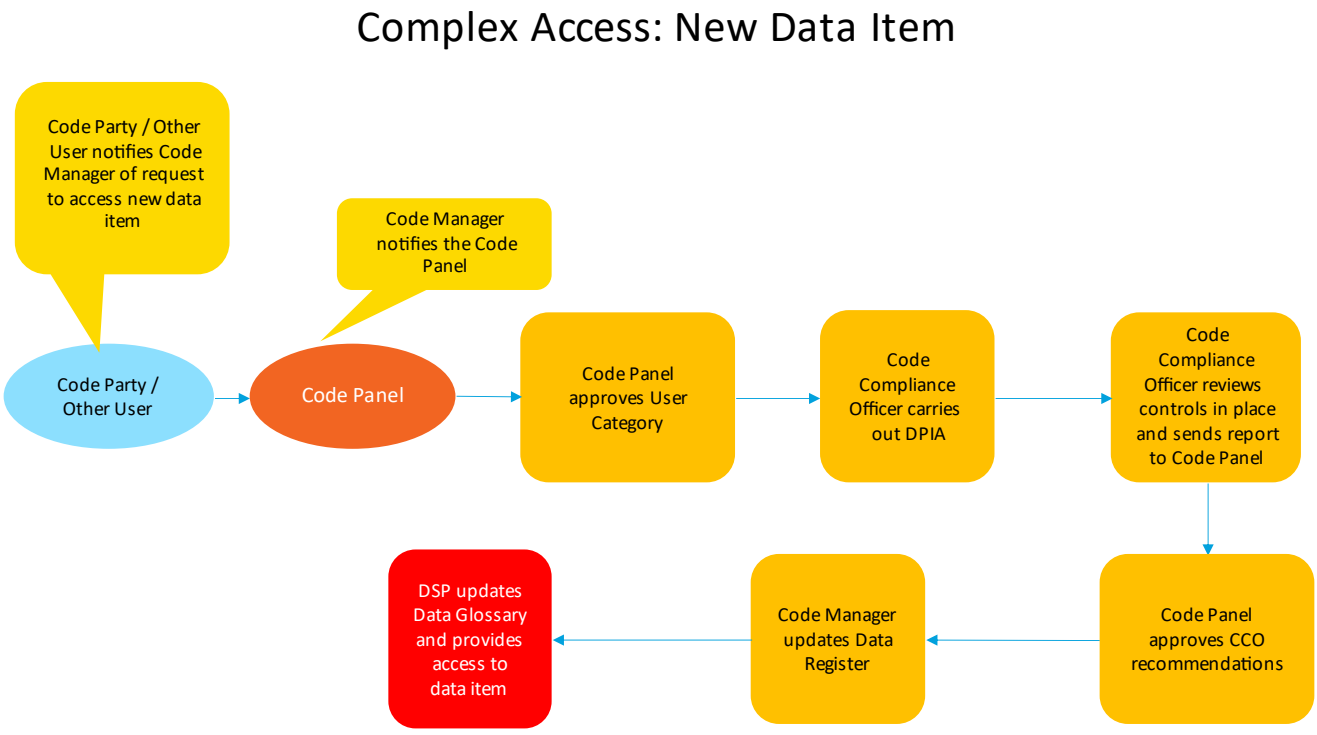

Figure 9 – Overview of an access request for a new data item.

The Code Manager, once informed on the request to access a new data item, notifies the Code Panel, who assess the suitability of providing access to the new data item. On approval of the new data item, the CCO is responsible for carrying out an ad-hoc assessment of the existing data privacy and security controls. The CCO may identify risks in its assessment and outlines remedial measure to the Code Party / Other User requesting the new data item. The Code Panel reviews the assessment report and on ratifying the CCO's report with recommendations, the CCO conducts a Data Protection Impact Assessment (DPIA) on the accessing and processing activities, considering the new data item. The process is completed when:

- Code Manager updates the Data Access Register to include the new data item.
- DSP updates the Data Glossary and provides access to the new data item.

For Other User applicants from new User Categories not already captured in the Data Access Register, the process is as follows:

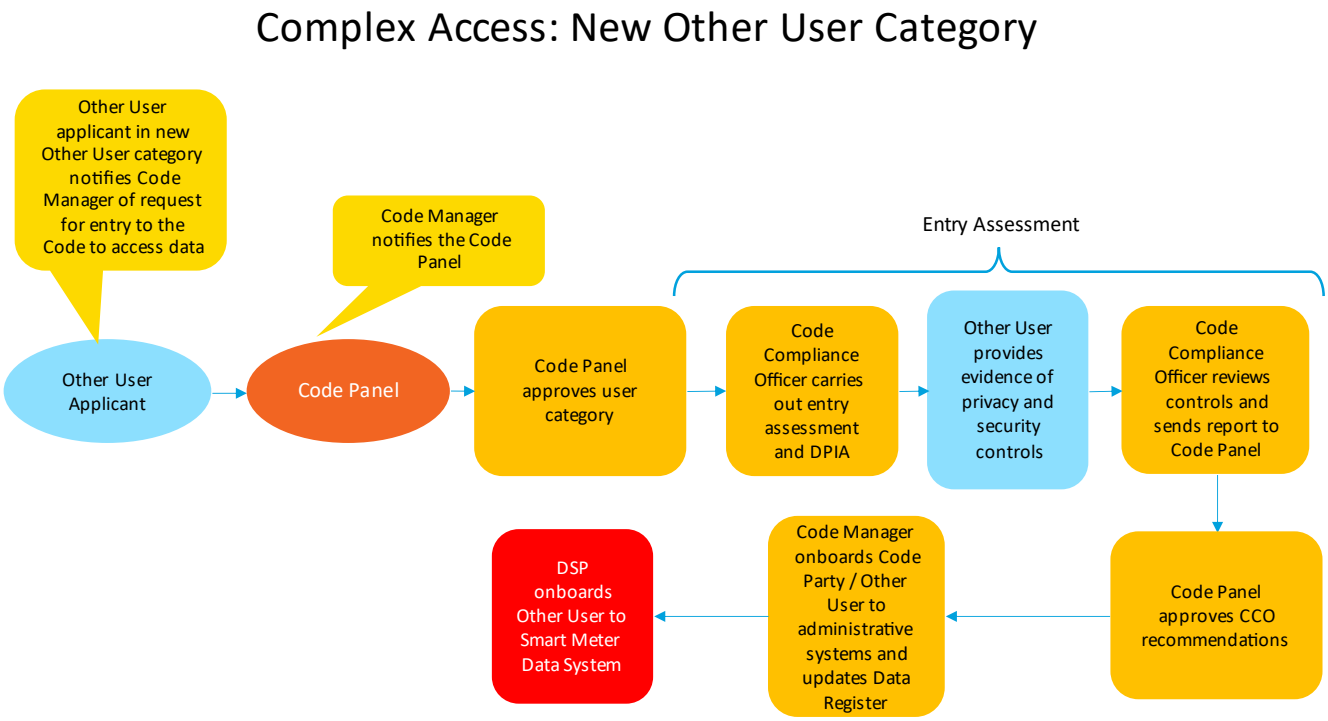

Figure 10 – Overview of an access request from an Other User in a new User Category

Once the Code Manager is notified by the new Other User Category applicant, the Code Panel is informed, and a suitability assessment is performed. Upon Code Panel approval of the new Other User Category, the CCO will schedule an entry assessment for the Other User applicant. As per the onboarding process for Code Parties / Other Users, this Other User applicant must provide evidence of data privacy and data security controls. The CCO completes the assessment

and issues a report to the Code Panel who ratifies the recommendations to approve the User Category or whether remedial action is necessary prior to access being granted. The CCO conducts a DPIA on the accessing and processing activities, considering the new User Category. Similar to the onboarding process:

- Code Manager onboards the Code Party / Other User to the administrative systems developed for the Code and updates the Data Access Register to include the new Other User Category.
- The DSP onboards the Code Party / Other User to the Smart Meter Data System

The Code as a Code of Conduct

The CRU would like to outline that the Code is being developed to include provisions on data protection irrespective of Code Parties / Other Users' GDPR obligations. The EU Directive 2019/944 specifies that Member States must introduce rules and measures to facilitate access to smart meter data. In addition, S.I. 37 of 2022 requires a Code to be developed to regulate access to such data. Given the market arrangements for the Smart Meter Data System, the Code is required to provide transparency of the process for using this system and ensure a fair one-stop shop approach for Code Parties / Other Users to access smart metering data.

The effect of both legislative requirements places the obligations under the EU Directive 2019/944, implemented by the Code, on top of GDPR and the Data Protection Act 2018 for Code Parties / Other Users that want to access smart metering data. The CRU believes, through the Code, these obligations can be introduced, and that Code Parties / Other Users can comply with them.

In terms of the Code being considered a Code of Conduct, as per Article 40 of GDPR, the CRU would like to highlight that:

- The scope of data covered by the Smart Meter Data System and the Code, and as required by the EU Directive 2019/944, is broader than just personal data, or metering and consumption data. As such, registering the Code as a Code of Conduct would require separating out enforcement and governance permissions for metering and consumption data from those referring to personal data, and the CRU consider this not to be practical.

- If the Code were to be a Code of Conduct, the CRU is concerned that this would cause Code Parties / Other Users to use their compliance with the Code as evidence they were meeting their obligations under GDPR. Additionally, Code Parties / Other

Users would still need to comply with the Code and the development of a Code of Conduct would not simplify these obligations.

- If a MoU is possible between the Code Panel and the DPC, this could show the interest in aligning enforcement of the Code with data protection regulation and enforcement. The CRU believe this could avoid a potential overlap or conflict of enforcement obligations with respect to approval and enforcement of the Code between the Code Panel and DPC, as may occur if the Code were also a GDPR Code of Conduct.

The CRU considers that the Code, as currently drafted and applying to data other than personal data also, means that Code Parties / Other Users would not be able to rely on its obligations to demonstrate they were complying with GDPR, and the CRU believes that it is unlikely that the Code will be developed as a Code of Conduct.

Data Protection Impact Assessment

Under Article 35 of the GDPR, a Data Protection Impact Assessment (DPIA) is required to be conducted for certain types of processing. According to Article 35(1)[21], the need for a DPIA occurs where a type of processing involves new technologies, and "taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons".

Guidance on what types of processing activities is likely to result in "a high risk to the rights and freedoms of natural persons" varies by jurisdiction and is usually a decision to be made by the data controller on the facts of the case. DPIAs are typically used to assess processing activities or a set of processing activities which typically cover not only systems, but the specific personal data used on those systems, and the operations performed on this data, such as collection, profiling, anonymisation, etc. The Article 29 Working Party, a former European Commission entity now known as the European Data Protection Board (EDPB), has outlined in its opinion WP248[22] in 2017 that the following nine criteria should be considered as processing operations "likely to result in a high risk":

[21] Article 35 (1) GDPR - Data protection impact assessment

[22] Article 29 Data Protection Working Party - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248 rev.01)

- Evaluation or scoring, including profiling and predicting
- Automated decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- When the processing in itself prevents data subjects from exercising a right or using a service or a contract

The CRU is aware the DPC has also adopted its own list, which includes:

1. Use of personal data on a large-scale for a purpose(s) other than that for which it was initially collected pursuant to GDPR Article 6(4).
2. Profiling vulnerable persons including children to target marketing or online services at such persons.
3. Use of profiling or algorithmic means or special category data as an element to determine access to services or that results in legal or similarly significant effects.
4. Systematically monitoring, tracking, or observing individuals' location or behaviour.
5. Profiling individuals on a large-scale.
6. Processing biometric data to uniquely identify an individual or individuals or enable or allow the identification or authentication of an individual or individuals in combination with any of the other criteria set out in WP29 DPIA Guidelines.
7. Processing genetic data in combination with any of the other criteria set out in WP29 DPIA Guidelines.
8. Indirectly sourcing personal data where GDPR transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.

9. Combining, linking, or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources where processing was/is carried out for difference purposes or by different controllers.

10. Large-scale processing of personal data where the Data Protection Act 2018 requires suitable and specific measures to be taken in order to safeguard the fundamental rights and freedoms of individuals.

From the above, points 1, 4 and 9 seem to be the most relevant risks to consider, with respect to smart meter data and the Code, as the Smart Meter Data System will process MPRNs and other relevant information from domestic and non-domestic smart meters across Ireland, which will be considered 'large-scale'. Based on the EDPB guidance highlighted above smart meters are likely to be considered a means of systemic monitoring, particularly where the collection of half-hourly consumption data and consumer profiling is involved and are also likely to be considered innovative or new technological solutions. The CRU is also aware of recent comments made by the European Data Protection Supervisor (EDPS) on the risks associated with smart metering data when assessing the EU Implementing Regulation 2023/1162 in 2022[23].

The CRU considers the best practice would be to consider conducting a DPIA in the following scenarios:

1. Previously, in 2020, a DPIA was conducted on the CRU's National Smart Metering Programme (NSMP)[24]. This covered the roll-out of smart meters, access by businesses to metering and consumption data, and the subsequent use by these organisations of smart metering data. Since then, the Code has been drafted and the EU implementing regulation has been recently adopted, which significantly advances the rules for access to smart meter data. Furthermore, ESB Networks conducted a DPIA for the Smart Meter Data System[25] in 2022. As such, the CRU considers it would be best practice to propose a new DPIA on the finalised Code being conducted, covering the separate scope of the management of the rules for access to this system and smart meter data, and the facilitation of data subject rights over their data.

[23] EDPS Formal comments on the draft Commission Implementing Regulation on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data
[24] Data Protection Impact Assessment Report for the CRU's Smart Meter Upgrade Phase 1
[25] ESB Networks – Smart Metering Data DPIA

2. The CRU proposes that any modifications to the Code should be subject to a DPIA, where they impact access to personal smart metering data. Such modifications are likely to affect processing activities related to the use of personal data on a large-scale, which is listed in Article 29 Working Party's DPIA criteria.

3. Any creation of new User Categories should require a DPIA to be conducted, as these will affect processing activities related to the potential use of personal data on a large-scale for a purpose other than that for which it was initially collected. For example, new User Categories will involve new organisations with likely new processing activities with smart metering data, and may involve profiling customers' consumption behaviour, that must be assessed. This would affect the purposes of processing such personal data. The CRU considers conducting a DPIA on such new User Categories is best practice.

4. Any new data items available on the Smart Meter Data System, which could include if a data item becomes available on the market or Smart Meter Data System or is requested by a Code Party / Other User where previous access was not provided. The new data item(s) would need to be assessed and a decision made to allow access to these additional data items. Where these data items are attributable to an individual premise, this would involve new personal data and thus new processing activities, potentially on a large-scale, as well as additional means of systematically monitoring, which the CRU propose that a DPIA should be carried out in this scenario.

The Article 29 Working Party and DPC recommend that a DPIA be conducted where it is not clear whether a DPIA is required, to help conduct such an assessment, as well as for the usage of new technologies. As the DPC outlines, "the use of a new technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms". The CRU recognise that where such situations arise, there will need to be regular consideration as to whether a DPIA is required. Moreover, the CRU are of the view that DPIAs should be revisited on an annual basis or where processing activities change as this is likely to mean that the risk levels have changed. The CRU invites market participants and interested parties to provide feedback on this section and the proposals presented.

Question 5: The CRU would welcome any views on the proposed onboarding and access processes required for both Code Parties / Other Users to gain entry to the Code and to access smart meter data.

2.6 Events of Breach and Consequences of Breach

2.6.1 Summary of consultation position

For breaches of the conditions of the Code, the process of notification, investigation, resolution, and remediation was initially discussed in this section.

A Party to the Code that breaches any of the conditions of the Code is known as the Breaching Party. Where a breach is notified, the Code Panel can decide to investigate such an event and afterwards, can take action such as instructing the Breaching Party to remedy or mitigate the effects of the breach, suspend access to smart meter data, or recommend expulsion of the Breaching Party from the Code.

In the draft version of the Code, the CRUs potentially could suspend the rights of a Breaching Party and also deal with any appeals arising from such suspensions. Any decision on appeals made by the CRU is considered final and binding.

The CRU asked respondents for their views on the draft process concerning an event of a breach, with respect of the Code, by a Party of the Code.

2.6.2 Summary of responses

There was general agreement from respondents that a breach process is required under the Code but asked for further details on how this process will interact with existing breach processes required for GDPR compliance.

Some responses highlighted the potential adjudication role of the CRU on compliance and appeal actions and requested further details on the nature of breaches that the CRU aims to address in the Code. Several respondents noted this section only discussed licenced Parties and asked how non-licensed Users would be overseen.

The majority of respondents considered the impact of the consequences in the breach process in relation to the data types that licenced Parties require in executing their responsibilities under licence conditions. Some responses raised protection concerns on information being shared by a breaching Party investigated as a result of a breach and asked that the Code recognises that no sensitive information would be shared.

Several respondents noted that it is important that any risk of double remediation is mitigated in the Code and that it is made clear that the breach process discussed in this section only covers the Code provisions and any personal smart meter data breaches would fall under GDPR and DPCs remit.

2.6.3 The CRU's proposed decision

The CRU believes that security incidents, which impact the Smart Meter Data System, and personal data breaches, and the procedure for their identification, assessment, and management, are key issues to be regulated under the Code. This is due to the risks they pose for both the Smart Meter Data System and for the personal smart meter data of customers.

The CRU is conscious of the importance in ensuring that there is no double regulation under the Code and that for personal data breaches, the DPC remains the supervisory authority responsible for receiving reports of such breaches and the mitigation and enforcement actions that follow these breaches. The CRU considers that the DPC, who conducts investigations and issues subsequent actions in relation to personal data breaches, can help to ensure the safe operation of the Code and the Smart Meter Data System, through an MoU with the proposed Code Panel or collaborating with the DSP where the breach is relevant to the Smart Meter Data System. The CRU believes that the information sharing about security incidents and personal data breaches between the proposed Code Panel and the DPC is crucial in resolving these incidents / breaches.

The CRU would like to note that the arrangements for incident notification under the Code to the proposed Code Panel, via the CCO, are considered to be similar to the responsibilities for breach notification under the arrangements of Article 26 and 28 of GDPR. In particular, both articles impose obligations on Joint Data Controllers to inform each other, and Data Processors to inform Data Controllers respectively, where a personal data breach has occurred. The arrangements of these articles typically cover joint processing between Data Controllers, or processing by a Data Processor on behalf of a Data Controller. Under the Code, both joint Data Controllership and separate Data Controllership arrangements will apply, depending on the parties involved, making it necessary for incident notification arrangements to be included under the Code.

<u>Security Incidents</u>

The CRU proposes the following processes that cover the actions that would occur with respect to a security incident, which includes a personal data breach.

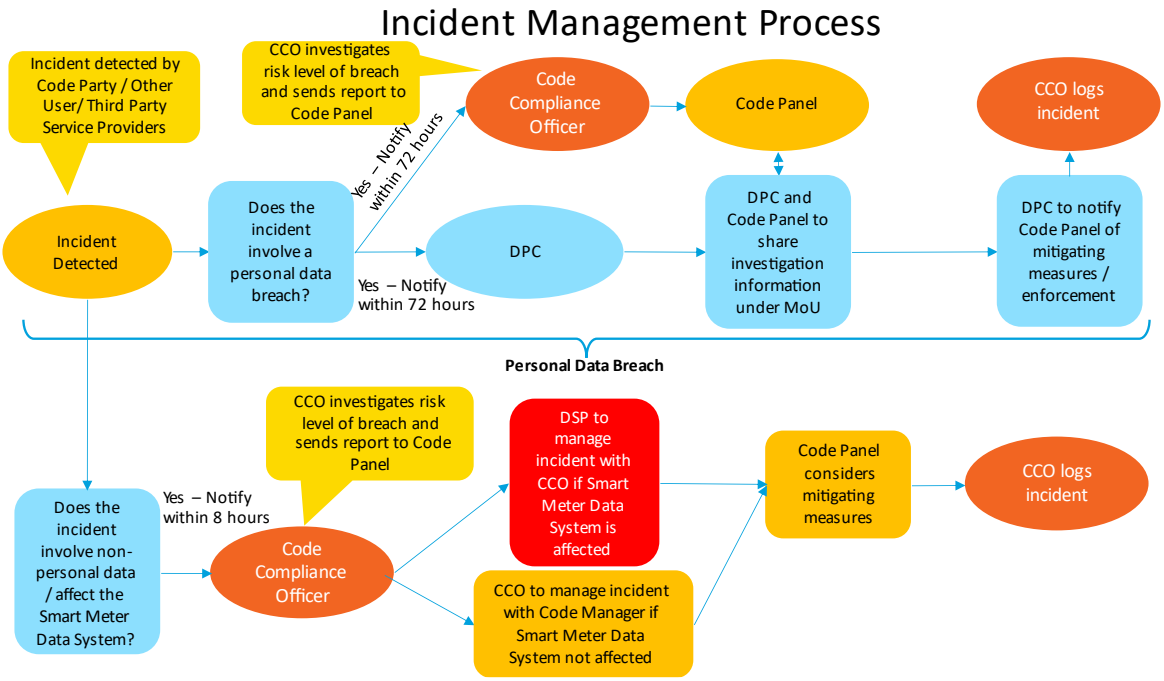

Figure 11 – Overview of an incident management process that includes a personal data breach.

The CRU considers the following processes managing a security incident under the Code:

- For a security incident that includes a personal data breach, Code Parties / Other User / third-party service providers will assess the breach and notify the DPC primarily within 72 hours, according to GDPR obligations. Under the Code, the CCO will be notified secondarily within 72 hours.
- For security incidents that do not involve a personal data breach, Code Parties / Other Users / third-party service providers will assess the breach and notify the CCO within 8 hours. The rationale for this notification period is that there would likely be a number of smaller incidents on the Smart Meter Data System, which the DSP would be able to manage in isolation.
- Upon security incident notification, the CCO shall evaluate the level of risk of the incident and determine whether a personal data breach as occurred.
- In the event of a personal data breach, the CCO shall advise the Code Panel on notification to data subject(s) and the DPC, as is necessary.
- If it is determined that the Smart Meter Data System has been compromised, the CCO will work with the DSP on any actions that need to be conducted on the Smart Meter Data System

- For other incidents on systems not related to the Smart Meter Data System, The CCO will advise the Code Manager on any mitigation steps on the systems maintained by the Code Manager.

- Following the mitigation process, the CCO ensures the incident and relevant actions taken are documented and maintained in a Code incident log. The DSP would be tasked with maintaining an incident log for the Smart Meter Data System.

The next incident management process is shown below, with respect to the DSP.

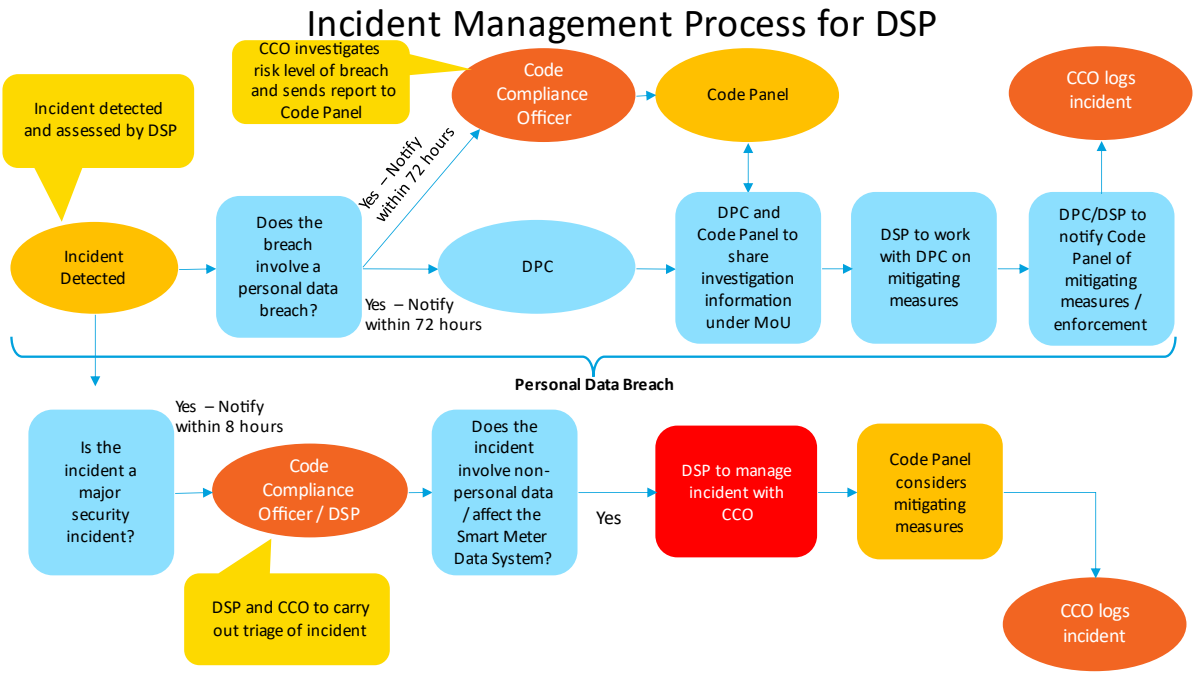

Figure 12 – Overview of an incident management process that includes a personal data breach and involves the DSP.

In this instance, the DSP shall:

- Assess the incidents and if a personal data breach has been detected, the DSP will notify the DPC within 72 hours, as per GDPR legislation. The DSP shall also notify the CCO within 72 hours.

- Notify the CCO within 8 hours if a major security incident, which has or may have affected the Smart Meter Data System and involves non-personal data. The higher threshold is due to the likelihood of several minor incidents occurring on the Smart Meter Data System, which the DSP can manage in isolation.

Upon being informed by the DSP, the CCO will determine the level of risk of the incident and whether a personal data breach has happened.

- The CCO will work with the DSP to resolve the incident if it has affected the Smart Meter Data System. For systems maintained by the Code Manager that have been affected by the incident, the CCO will advise the Code Manager on actions to take to rectify the incident.
- If the CCO determines the incident involves a personal data breach, it will notify the Code Panel and DSP on notification to data subject(s) and the DPC, as necessary.
- Following the mitigating actions, the CCO shall document the incident and steps take and maintain the incident log. Similarly, the DSP will log the incident and maintain the log for the Smart Meter Data System

Breach of the Code

The CRU would like to highlight that a breach of the Code could be caused by either a security incident or personal data breach that the Code Panel has determined as an Event of Breach, or a breach of the material terms and conditions of the Code. The following proposed breach processes, with respect to a breach of the Code, will now be considered.

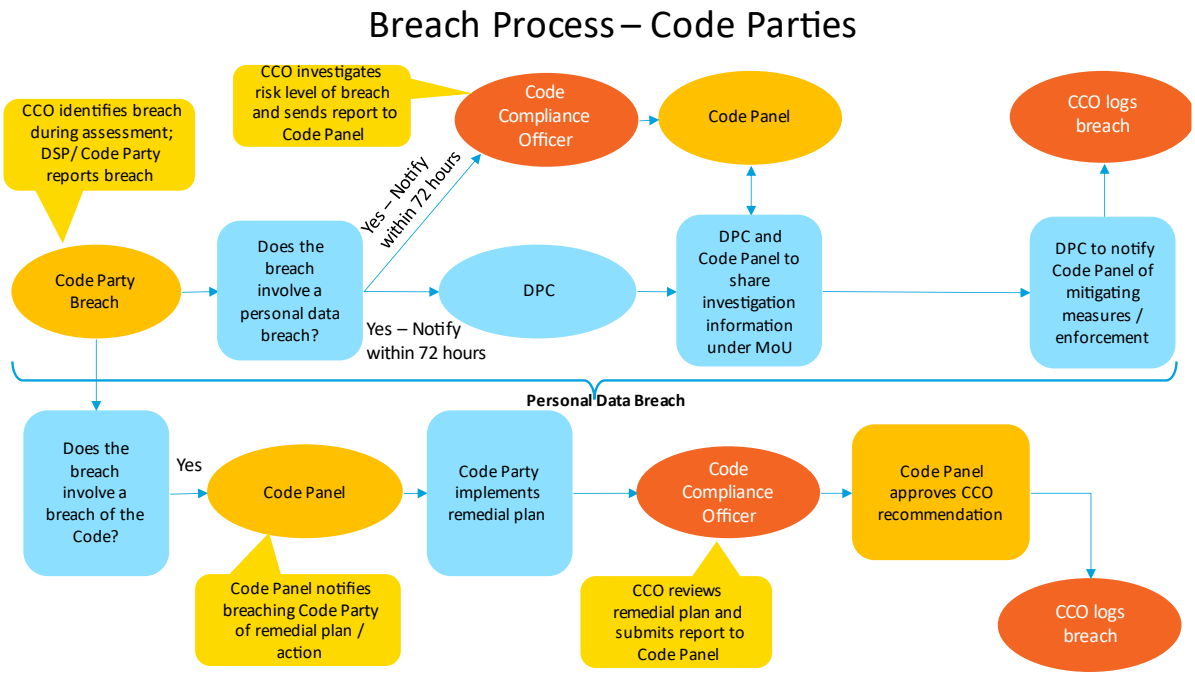

Figure 13 – Overview of a breach process that includes a personal data breach and involves Code Parties.

For this particular breach process, the CRU is proposing that the Code Panel prioritises a remediation plan as a primary action to take, ahead of any enforcement such as suspensions of rights or in extreme cases, expulsion from the Code. The CRU notes that in serious breach scenarios, the Code Panel may in the future have the potential to liaise with the CRU, in the case where a licence condition to comply with the Code may exist. However, the CRU believe this mechanism is unlikely to be utilised, given the fact that Code Parties' licences do not currently require compliance with the Code and that potential licence clarifications are only being considered at this stage.

The CRU would like to re-iterate that for personal data breaches, where the Code Panel determines and these breaches constitute an Event of Breach under the Code, the DPC remains the regulator responsible for receiving notification of such breaches and any enforcement action that may be taken. The DPC, through the proposed MoU, will collaborate with the Code Panel with respect to the outcomes of any investigations and any enforcement measures that the Code Panel may take, as instructed by the DPC. This is to ensure that there is no double regulation under the Code for personal data breaches.

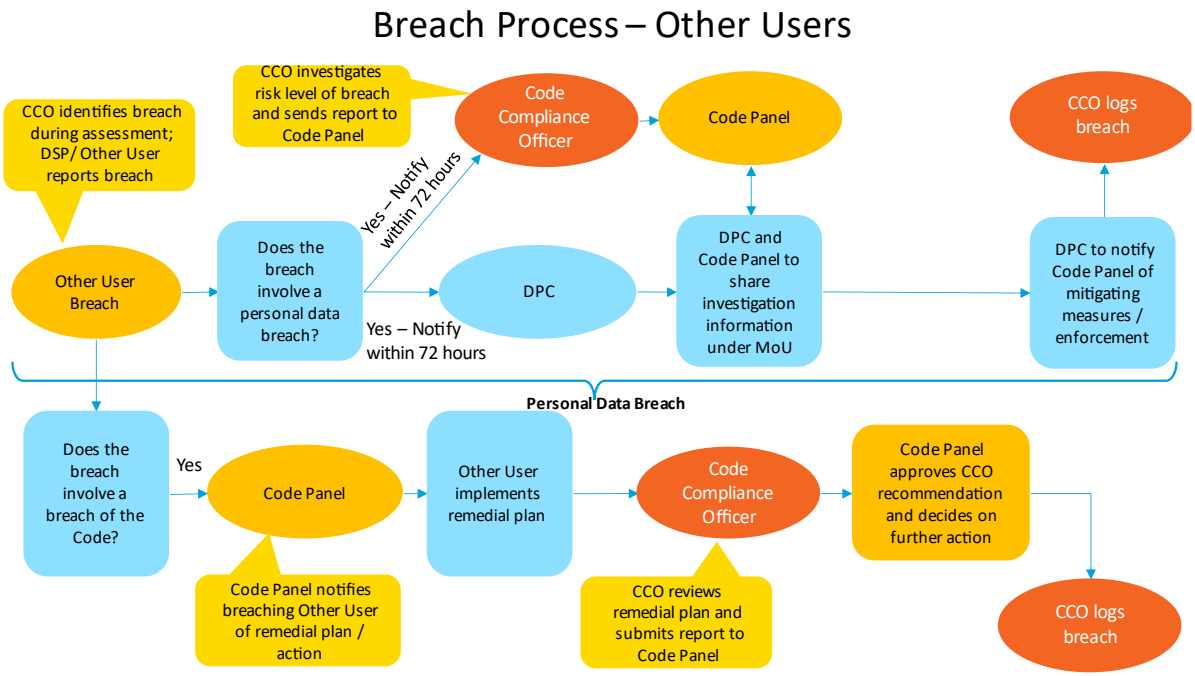

Figure 14 – Overview of a breach process that includes a personal data breach and involves Other Users.

The CRU is also proposing that the Code Panel will, in the first instance, inform an Other User found in breach of the remediation steps to take. Where more serious action is required with respect to Other Users, as they are not eligible to be Code Parties, they will not be able to have their rights under the Code removed or restricted in the same manner as Code Parties. However,

the CRU wants to note that for serious breaches of the Code, the main enforcement action taken against breaching Other Users will focus on the potential to suspend or terminate the Access Agreement and therefore, the associated access to smart meter that Other Users will have.

Similarly for Code Parties, should the Code Panel determine that a personal data breach, involving Other Users, signifies an Event of Breach under the Code, the DPC is the lead authority to deal with such breaches, and upon receiving notification of the breach, enforcing the data protection legislation. The Code Panel will engage with the DPC to explore the option of a MoU, which could include the sharing of information during the investigation and the resulting enforcement action that the Code Panel could implement. The CRU believes this potentially could give reassurance to industry that there is no doubling up of regulation and enforcement.

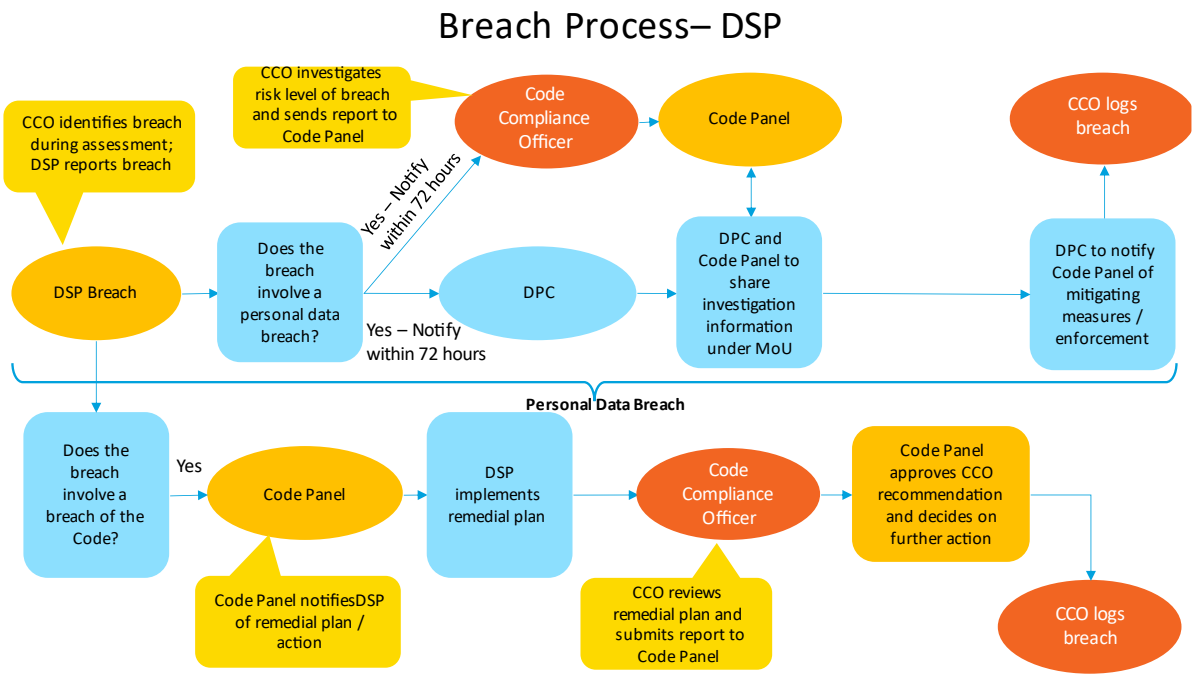

Figure 15 – Overview of a breach process that includes a personal data breach and involves the DSP.

The CRU proposes the following breach process with respect to the DSP. The Code Panel in this instance can take action to notify Code entities, instruct the CCO to conduct an ad-hoc assessment, or approve a remediation plan for any non-compliance in the DSP's obligations under the Code. As per Code Parties / Other Users, the first action to be taken by the Panel is remediation steps ahead of any further enforcement actions. There could be a scenario where more serious enforcement is required and the Code Panel may in the future liaise with the CRU to potentially take action, with respect to the DSO licence. The CRU stresses that this approach is unlikely to happen and as such, it is currently not possible due to the fact the DSO licence has not been modified to include the DSP function.

As highlighted in the breach process diagram, the DPC is the main regulator to investigate and take enforcement action on the DSP, in the case of a personal data breach being identified, either by the CCO during an assessment, or it is reported by the DSP. The Code Panel and DPC share information relative to the investigation as per the MoU and the DPC notifies the Code Panel of any enforcement steps that may be taken.

Code Manager Breach

The CRU would like to highlight an instance that may occur when the Code Manager has breached the Code. For example, an information security incident or personal data breach that is discovered during administrative or secretariat functions performed by the Code Manager. With this scenario, the CRU is proposing the breach process as follows:

- Personal data breach: Such breaches, with respect to the functions of the Code Manager can be identified by the Code Manager, the CCO during an assessment or by other Code entities. Once the Code Panel has been notified, it shall report it to the DPC, unless the Code Manager has already done so.

  The DPC will investigate the personal data breach and share information with the Code Panel, with the Code Manager absent from discussions, relating to the outcomes of the investigation and any mitigating or enforcement action the DPC may take, under the proposed MoU arrangement with the Code Panel.

- Breach of the Code: Once the breach of the Code by the Code Manager has been discovered, the Code Panel will be notified by either the Code Manager or CCO or any Code entity.

  The Code Panel will arrange meetings to fully investigate the breach, without Code Manager representation, and the Code Panel must ensure that the secretariat function is carried out for the duration of the investigation. The CCO will be tasked with investigating the breach and will notify other Code entities of the breach and if the breach is likely to affect their activities.

  Following the CCO's investigation, the Code Panel will prioritise remedial action that the Code Manager must carry out. Any potential further enforcement action depends on the contract with the Code Manager, likely to be held with the CRU, and the entity appointed to be the Code Manager, in this instance, the MRSO.

  Where the proposed Code Manager is the MRSO, the CRU could also take action with respect to the DSO license, however, this is dependent on the Code Manager model the CRU will decide to implement, either the MRSO is assigned the Code Manager role as a

function, subject to a potential CRU clarification on the relevant condition of the DSO licence, or the MRSO is just delegated the Code Manager role.

The CRU would like to add that this process for assessing and taking enforcement action with respect to the Code Manager is not likely to be used frequently, if at all, and the CRU will keep the breach process under continual review as a finalised governance of the Code is implemented and evolves.

Question 6: CRU welcome any views on the proposed security incident management and breach processes in the event of an incident or breach of smart meter data.

2.7 Ceasing to Be A Party

2.7.1 Summary of consultation position

In this section, the potential scenario of a party ceasing to be a Party of the Code was discussed.

A licensee party cannot be expelled from the Code by the Code Panel, nor can it voluntarily cease to be a Party to the Code. This is the case where potential licence modifications requiring it to be a Party of the Code were in place. The consultation position was that CRU could decide to approve the expulsion of a Party to the Code, which would mean that the expelled Party would have no access to the Smart Meter Data System. The CRU could potentially handle any appeals related to expulsion and that any decision would be considered final and binding.

Schedule 7 of the Code which covers Party Exit and Party Breach was pending the decision on governance of the Code. It is aimed to include the processes involved for expelling a Party or a voluntary withdrawal from the Code.

The CRU asked respondents for their views on licensed parties ceasing to be a Party of the Code.

2.7.2 Summary of responses

The majority of respondents agreed that for any Party expelled or withdrawn voluntarily from the Code, the Schedule 7 process must include obligations on retention and disposal of smart meter data. Some responses cited examples where exiting Parties retains smart meter data and asked that obligations requiring such Parties to comply with data protection legislation to be included in Schedule 7. Requirements on the disposal / destruction of smart meter data, security credentials

and confidential information before a Party exits, as a result of a breach, was also suggested by respondents.

Some responses recommended that Schedule 7 process aligns with other defined industry processes such as the example of a licensed party exiting the retail market. Several respondents noted the benefits of the circumstances for expulsion, appeals and re-instatement being clarified further in Schedule 7.

2.7.3 The CRU's proposed decision

The CRU acknowledges that the scenario where a party ceases to be Code Party that was discussed in the consultation assumed that there would be licence conditions requiring Code Parties to comply with the Code. As these licence changes are only under consideration by the CRU, the exit approach originally outlined, where a Code Party cannot volunteer to exit the Code due to such licence conditions, can be viewed as not appropriate at this time.

It is recognised by the CRU of the importance of an exit from the Code aligning with industry processes like the Supplier of Last Resort (SoLR) procedure that covers a licenced entity leaving the electricity retail market. The drafted schedule relating to Party Exit has considered the Supplier of Last Resort process as a potential scenario for a Code Party to exit the Code.

A Code Party can also initiate its own withdrawal from the Code which includes notifying the Code Manager. The Party exit schedule proposes that all smart meter data, including personal data, accessed from the Smart Meter Data System, will be deleted prior to the party exiting the Code voluntarily. The Code Manager and CCO are proposed to validate that the data has been deleted, and in the case of a Code Party being a supplier, that no MPRNs are registered to the exiting supplier prior to exiting the Code. The DSP will ensure that the exiting Code Party will have access removed from the Smart Meter Data System. The CRU proposes to have the final decision on any voluntary withdrawal of the Code which the CRU believes reflects its decision making in the established SoLR process. In the unlikely event of an exiting Code Party retaining their licence, thereby maintaining their eligible party status under legislation and the Code, the Code Party cannot withdraw from the Code until the CRU has approved the decision.

In the event of a breach of the Code, one of the enforcement measures can involve expelling a Code Party from the Code and the CRU is proposing to have the final decision on any expulsion from the Code due to a breach, based on the Code Panel's recommendation. The CRU believe that the withholding of data and suspension of a Code Party's rights under the Code are Code Panel remedial compliance actions that come before any decision around expulsion. As such, the CRU would not be required to approve these actions and this separation from the expulsion decision strengthens the case against the CRU being considered a Data Controller under

expulsions as the smart meter data access would already have been withdrawn by the Code Panel at that stage. The CRU considers this proposal is considered best practice and reduces the risk of an expelled Code Party using an appeals process where the CRU would be involved with in any case. The CRU would also like to stress that expulsion from the Code is seen as a last resort and is not likely to be enforced under the Code.

Question 7: CRU welcome any views on the proposed schedule relating to Code Parties exiting the Code.

Question 8: Do respondents have any other comments on other aspects of the updated version of the Code and the proposals discussed in this paper?

3.Licence Considerations

CRU is considering licensing obligations that may be required to be updated in order to ensure that licence holders accede to the Code and the rules established therein. This will involve modifying existing licences by either adding a new condition to the licence or modifying an existing condition within the licence. This section currently refers to entities who have licences that require them to be both a Party to the Code and are eligible to access the smart meter data i.e., the DSO, TSO, SMO, and Suppliers. The CRU is aware that new market players, considered eligible parties, such as aggregators, energy service companies, renewable energy communities, citizen energy communities, price comparison websites, demand response providers, and any entity that offers energy-related services to customers, are presently awaiting a framework / licensing regime to be established. Any such licensing updates that may arise for these entities will need to be considered whether a licence condition is required with respect to the Code.

3.1 DSO Licence

In order to strengthen the CRU's compliance and enforcements obligations set within the Code, CRU is considering licence modification with regard to Condition 9: Provision of Metering and Data Services of the DSO Licence. Furthermore, the role of DSP, as defined in the Code, will also require a modification to the DSO Licence.

Subject to a decision on the governance framework, one such license modification being considered for the DSO Licence is with respect to Condition 9 1. (e). This modification could include an explicit provision of smart meter data for the purposes of and in accordance with the Code. This would enable the DSP to carry out its responsibilities, as set in the Code.

Furthermore, the CRU notes the MRSO is proposed as the Code Manager in the governance framework, and should a decision be made to include this Code Manager role as a function of the MRSO, ensuring the Code Manager is a legal entity, this will likely lead to a modification required for the DSO licence with respect to Condition 8 Meter Point Registration Service to establish the function of Code Manager.

The CRU is also exploring how the DSO Licence could be changed to allow the DSO to access to and processing of smart meter data for network planning and operation, flexibility service provisions and revenue protection purposes. However, the CRU is engaging with DECC to determine whether any potential legislative amendments could be made that would enable the DSO to access and process the smart meter data for the purposes listed above, which would prevent the need for further licence changes being proposed.

The CRU is conscious that the DSO licence has not been modified or amended since 2009 and that this may be seen as an opportunity to modify the licence, with respect to how both the retail market has developed, and the metering technology has advanced. Any potential license modification process provides for a minimum 28 days for any objections or representations to be made to the CRU. The CRU is considering how the licence options discussed could impact the delivery of smart meter data to the Smart Meter Data System in particular, the benefits of the smart meter data being available to customers, suppliers and third parties.

3.2 Supplier and Other Licenses

As part of CEP implementation, the CRU plan to review the licence framework for suppliers to see what changes are required to comply with relevant legislation in CEP and in consideration of the necessity for a licence framework for new market participants such as aggregators, demand response, battery storage entities into the Irish retail market.

CRU is considering including a condition or modifying a condition within supplier and other entities' licences, with regard to the Code. In addition, the CRU notes that presently, the supplier licence only covers access to smart meter data for billing purposes. The planned review of the supply licence may lead to conditions pertaining to access to, and processing of personal smart meter data for a lawful purpose. This could potentially help establish a firm legal basis, including purposes for processing, for suppliers to access smart meter data and to fully comply with GDPR.

Any changes to the licences, as discussed above, would involve a public consultation, and the CRU will need to review any impacts these considered modifications may have on other conditions set within the licences and the potential delay of the benefits of smart meter data that suppliers and other entities can provide to customers.

The CRU is engaging with DECC to evaluate whether there is scope for legislative changes to allow suppliers to access smart meter data, as per MCR1208, ahead of the Code going live, which could give suppliers a firm legal basis and enable them to be proactive with their respective customers, by incentivising them to take up smart tariffs, and providing more attractive smart services / tariffs. This would help to avoid any requirement to modify the supplier licence.

For licensed entities such as the TSO and SMO, any potential licence modifications would need to be considered should the DSO and supplier licences be updated as a result of the modifications discussed in this section.

4.Next Steps

The CRU is seeking views from suppliers, consumer interest groups, industry groups, members of the public and all other interested parties regarding all aspects of the updated version of the Code, specifically the proposed option around governance and enforcement, the smart meter data that is available in the Smart Meter Data System, and the other proposals discussed in this paper.

A full listing of all questions asked throughout this proposed decision paper can be found in Appendix B “Summary of Question’s” of this paper.

The CRU will be running a workshop on the proposals discussed in this paper and the updated version of the Code with suppliers and interested parties during the consultation period to gauge views and expectations from industry. The CRU intends to schedule this workshop on publication of this proposed decision paper. This, together with consultation responses, will help inform the CRU in developing the final version of the Code and the CRU decision.

The proposed decision consultation closes on 15th September 2023, and the CRU intends to reach a decision in Q4 2023.

Appendix A - Frequently Asked Questions for Customers

What is the Smart Meter Data Access Code?

It is a set of rules and regulations, developed by the CRU, which determine who can access smart meter data, what type of data they can access, and what they can do with the data once it has been accessed.

Why is the Smart Meter Data Access Code required?

Smart meter data is considered important in enabling customers and market bodies to access and provide opportunities like improved energy performance in homes, renewable energy, and energy efficiency.

However, there is a need to ensure that smart meter data is secure and only processed where appropriate and the Smart Meter Data Access Code is required to achieve this.

What is smart meter data?

It is the data that comes from smart meters which includes customer energy consumption data, customer energy export data and technical data on the meter itself.

Who will be able to access my smart meter data?

The Smart Meter Data Code will be applicable to several eligible parties. These include ESBN, who will hold the smart meter data in a hub and require access for network and planning purposes; suppliers, who require access to smart meter data for their respective customers to enable them to create more attractive smart tariffs and services and incentivise more customers to sign up to these smart tariffs ;price comparison websites who requires access to customers' smart meter data, with customer consent, to be able to find the most appropriate smart tariff for customers; and new market participants such as aggregators, demand response providers, renewable energy communities, who require access as part of their contractual arrangements with customers.

Third parties, such as the Central Statistics Office (CSO), the Sustainable Energy Authority of Ireland (SEAI), Economic and Social Research Institute (ESRI), universities, journalists will need to apply to access smart meter data and obtain customer consent, if the smart meter data is personal, before their application will be assessed, to determine whether access will be granted or not.

Will I be able to still access my smart meter data?

Yes, you can create an account on ESB Networks website to access your smart meter data from ESBN here.

Customer access to smart meter data is covered by their right to access their personal data from both ESBN and suppliers as per GDPR and Data Protection legislation. Your rights to access will be included in the Smart Meter Data Access Code.

What currently happens to my smart meter data?

Smart Meter Data is currently stored by ESB Networks to allow customers to access their data through their online account. For customers who have signed up to smart meter tariffs, your smart meter data is shared with your supplier for billing purposes.

Some customers can opt in for smart services with certain suppliers i.e., sign up with a preview of a smart tariff whilst remaining on their current non-smart tariff. In this instance, these suppliers will have access to your smart meter data to provide insights to you on the costs of these smart tariffs and what savings you could potentially make if you make changes to your energy usage patterns.

Will my smart meter data be secure?

Yes, the Smart Meter Data Access Code has rules around the security and privacy of smart meter data. These rules have been consulted with the Data Protection Commission (DPC) to ensure the data is secure and used in the correct way.

What happens if my smart meter data is compromised?

There will be enforcement provisions included in the Code that may involve suspension or removal of access to smart meter data for parties who have breached with respect to smart meter data. Where your personal smart meter data is concerned, the Data Protection Commission (DPC) will be notified and will carry out enforcement to parties found in breach of your personal smart meter data.

Appendix B – Summary of Questions

A summary of all questions the CRU is seeking views on throughout this consultation paper are presented below.

Question 1: The CRU would welcome any views on the proposal on access to smart meter data ahead of the Code going live.

Question 2: The CRU would welcome any views on the proposed entry, annual and ad-hoc assessments placed on all Code entities.

Question 3: CRU welcomes views on the minded to model for the governance and enforcement of the Smart Meter Data Access Code.

Question 4: The CRU would welcome any views from industry and interested parties on the most suitable governance framework to implement the rules and procedures of the implementing regulation.

Question 5: The CRU would welcome any views on the proposed onboarding and access processes required for both Code Parties / Other Users to gain entry to the Code and to access smart meter data.

Question 6: CRU welcome any views on the proposed security incident management and breach processes in the event of an incident or breach of smart meter data.

Question 7: CRU welcome any views on the proposed schedule relating to Code Parties exiting the Code.

Question 8: Do respondents have any other comments on other aspects of the updated version of the Code and the proposals discussed in this paper?