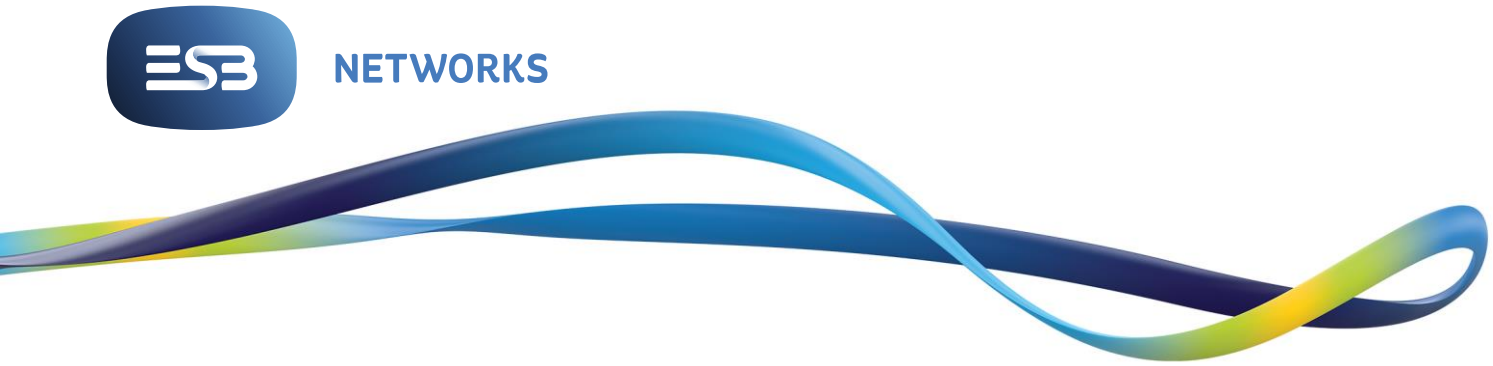

CONSULTATION ON THE SMART METER DATA ACCESS CODE

ESB Networks Response on CRU's Consultation on the Draft Version of the Smart Meter Data Access Code (CRU/202265/a)

21st September 2022

Contents

1. Executive Summary

ESB Networks welcomes the opportunity to respond to the CRU Consultation on the Smart Meter Data Access Code (SMDAC).

Smart meter data is a key enabler of the European Union's Clean Energy Package which aims to provide final customers with safe, secure, sustainable, competitive and affordable energy.

The legislative package seeks to enhance consumer participation by empowering them to manage their energy consumption on an equal basis with other market participants. It also requires the future electricity system to make use of all sources of flexibility, particularly demand side solutions and energy storage, and through digitalisation, integrate new technologies and services.

Smart meter data is fundamental to meeting these objectives.

The transition from an energy market which has traditionally operated on the basis of just 6 customer meter readings per year to one that has over 17,500 readings per year must be managed. It is right that this consumption data is protected by legislative and regulatory controls to ensure it is protected and used purely for legitimate purposes.

As set out in S.I. No. 37 of 2022 (SI 37/2022), the SMDAC is intended to provide assurance to customers that their smart meter data is being managed in compliance with the requirements of GDPR and within rules that specify which parties have access to which data and for what legitimate purpose.

The SMDAC therefore plays a crucial role in assuring customers that the use of smart meter data in the electricity industry is appropriately governed.

ESB Networks favours a governance model that, in meeting these requirements, facilitates customer participation, ensures efficient operation of the code and provides for on-going Regulatory approval of necessary modifications.

ESB Networks supports the objectives of the code as set out in SI 37/2022 but is of the opinion that the detailed drafting of the code can only be completed once a decision is made on the governance framework to be adopted.

Once a governance framework is decided upon a full review and assessment of implications for enacting roles and responsibilities can be completed. This can then enable full drafting of the code and further consultation prior to publication of the final code.

ESB Networks' working assumption is that the Code applies to the Smart Metering Data System with existing Advanced Metering Infrastructure ("AMI") and Retail Market Systems and processes being out of scope. ESB Networks has the role of Data System Provider (DSP) and the role of User of Smart Meter Data. ESB Networks therefore has made responses to the consultation from both perspectives.

This response highlights five key areas for further consideration:

1. Scope of the Smart Meter Data Access Code as set out under SI 37/2022:

- The scope of the code needs to be focused and appropriately set out, to ensure delivery of the provisions within SI 37/2022.
- ESB Networks' view is that the code should specify the rules on the access to smart meter data by eligible parties as set out in SI 37/2022.

- The code requires more clarity in these areas and consideration is required on the data protection and data security requirements, some of which already exist under existing legislation.

2. Code responsibilities with respect to GDPR:

- There is significant overlap between the provisions of the code and existing GDPR and Data Protection Act 2018 legislation. Clarity on how the provisions of the draft code are to be enacted with respect to GDPR is required. It is our understanding that legislation takes precedence over the code, this is followed by license obligations and then the code provisions.
- The draft data code overlaps with GDPR in areas including data control, data privacy, data security and breach management.
- ESB Networks is of the view that the draft data code potentially creates duplication of data controller roles between existing ESB Networks data controller responsibilities and the proposed CRU Data Code Manager and Data Code Panel.
- Our view is that the data code needs to have a focussed scope and have clear provisions set out to avoid duplication of roles or introduce potential conflicts with existing GDPR legislation.

3. DSO License Changes:

- It is expected that changes will be required to DSO licence to enact the provisions for the code. In particular, the role of the Data System Provider (DSP) will be established under license.
- ESB Networks is of the view that license changes are required to implement the requirements of the data code as outlined under SI 37/2022 including the collection and provision of smart meter data to users/eligible parties.
- In particular the DSP role (as proposed in the draft) needs to be established under license.

4. Governance Model:

- ESB Networks supports the implementation of a governance model that provides consumers with confidence and assurance that smart meter data is being, and will continue to be, used for legitimate purposes.
- ESB Networks' preference is for an efficient, agile and proportionate governance arrangement which is appropriate for the size and structure of the Irish electricity market and which uses familiar proven governance arrangements.
- ESB Networks currently operates several existing ringfenced entities responsible for the management of market registration processes and the processing / aggregation of meter data.
- With existing responsibilities for data management, ESB Networks is suitably positioned to undertake the role of Data Code Administrator with respect to smart meter data.
- ESB Network's preference is therefore for a governance option based on Option 5, whereby data code administration is assigned to a ringfenced entity within ESB Networks.

5. Data:

- ESB Networks notes that the definition of the data under SI 37/2022 needs to be translated into the Smart Meter Data Access Code to provide clarity on the range of data to be provided through the Smart Meter Data System. ESB Networks looks forward to engaging with CRU and industry stakeholders on defining the data to be provided to users.

ESB Networks welcomes the commencement of the consultation and looks forward to collaborating with CRU and industry stakeholders on the future development of the Smart Meter Data Access Code.

2. Introduction

ESB Networks welcomes the opportunity to respond to the Commission for Regulations of Utilities' (CRU) consultation on the 'Draft Version of the Smart Meter Data Access Code'.

ESB Networks' primary function is the provision of universal, affordable access to electricity, providing capacity and reliability, via the electricity distribution system, to support social and economic development across Ireland. This is as defined within its DSO license.

ESB Networks is committed to protecting the rights and freedoms of individuals in the electricity retail market and is committed to keeping stakeholders informed as the National Smart Metering Programme delivers on its CRU mandate. ESB Networks, therefore, fulfils a number of roles within the industry and also within the scope of the SMDAC. As such, this response is structured to emphasise the impacts on specific roles of ESB Networks.

ESB Networks has responded to each of the consultation questions and has included wider concepts to illustrate some areas where the code may impact existing operations and compliance activities. This submission is made on behalf of ESB Networks DAC in its capacity as the distribution system operator (DSO) as stated in the DSO License (2009).

ESB Networks continues to engage extensively with the CRU and retail market participants (MPs) with a view to agreeing the steps and actions necessary to implement the Smart Meter Data Access Code (SMDAC) in the electricity retail market and considers that implementation of the SMDAC should remain the primary focus for the retail electricity market in the near-term.

ESB Networks appreciates the opportunity to respond to CRU's consultation and remains available to engage further with CRU regarding any elements of our consultation response at any time.

2.1 Role of ESB Networks

As Distribution System Operator (DSO), Distribution Asset Owner (DAO) and Transmission Asset Owner (TAO), ESB Networks works to meet the needs of all Irish electricity customers, providing universal access to the electricity system, and delivering and managing the performance of a system of almost 155,000 km of overhead networks; 23,000 km of underground cables; 640 high voltage substations; significant amounts of connected generation, including 4.75 GW of renewable generation connected to the Distribution and Transmission systems; 2.5 million demand customers; and now several thousand "active customers" – including but not limited to domestic premises with microgeneration (a rapidly increasing number), demand side management, houses with battery storage, etc.

ESB Networks is also a key party to the delivery of CRU's National Smart Metering Programme (NSMP). To date, ESB Networks has installed over 900,000 smart meters in homes and small business throughout Ireland.

ESB Networks also delivers a range of services to the Irish retail electricity market serving over 2.5 million customers. It manages relationships with market participants and provides data in a timely and accurate fashion on a daily basis. It supports the wider market through the ringfenced Meter Registration System Operator (MRSO) and Retail Market Design Service (RMDS) and supports the wholesale Single Electricity Market through the provision of aggregated meter data.

ESB Networks' role in Ireland's move to net zero is pivotal and its role in the National Smart Metering Programme will enable and support visibility of consumption and power across the electricity network and customers. The Smart Meter Access Code is a key enabler to support new services and insights to be created by existing and new stakeholders/market participants on the electricity system.

Smart meters play a key role within the Clean Energy Package, particularly around the modernisation of the electricity market design and its focus on distribution network digitalisation to support the development of demand side services. As such, new obligations are set out for the distribution system operator in the Clean Energy Package relating to:

- Its role to enable more efficient wholesale market operation, as a result of distribution connected customers' active participation in wholesale markets and ancillary services;
- Its role with respect to the integration of renewables;
- Its role with respect to enabling the activities of individual customers, and communities, in their interaction with the electricity system.

These obligations cannot be met without access to high quality, location and time-specific data, in near real time as well as ex-post, which is not available to the DSO today.

Directive (EU) 2019/944 on common rules for the internal market for electricity sets out in Article 23 requirements for data management. Specifically, in Article 23 (2), that "Member States shall organise the management of data in order to ensure efficient and secure data access and exchange, as well as data protection and security." ESB Networks looks forward to working with CRU and its advisors to meet this requirement through the Smart Meter Data Access Code.

3. ESB Networks' response to consultation questions

Our comments are provided noting that first drafts of 7 sections and 2 schedules have not been included in this consultation which means that only a partial analysis of the code can be carried out. ESB Networks' view on some aspects of the code are therefore provisional and may change when the full details are available. This is particularly relevant to the responses that relate to interaction with legislation and to the administration of the code.

3.1 Response to Question 1

Question 1: The CRU would welcome any views from interested parties on the most suitable way to access smart meter data in relation to their data requirements? Views on what type of data you would expect to have access to would also be welcomed.

Background & Context

The National Smart Metering Program (NSMP) is central to implementing the Clean Energy Package and Climate Action Plan, giving customers more control over their energy usage and their bills. Smart meters and the data they provide will facilitate reduced energy consumption and increased renewable energy on the electricity system, while also enabling ESB Networks to plan and manage network operations, reinforcements and upgrades more efficiently.

ESB Networks supports and is fully committed to working with the CRU and interested parties on the most suitable way to provide access to the smart meter data. Our response to this consultation question focuses on the following areas:

- ESB Networks' Access to Data
- Other Party and User Access to Data
- Methods of Access

ESB Networks' Access to Data

ESB Networks, based on its current statutory role as the Data System Operator (DSO), requires access to the smart meter data present in the Smart Meter Data System. Namely, the twenty-four-hour, day, peak and night register, half-hourly interval, event, and instrumentation data that is recorded by a smart meter.

Access to this smart meter data is required to facilitate ESB Networks' compliance with Condition 3 (Operation Agreements), Condition 7 (Detection and Prevention of Theft of Electricity) and Condition 9 (Provision of Metering and Data Services) and Condition 11 (Distribution System Security and Planning Standards) of the DSO license issued by the CRU. In addition to facilitating compliance with the DSO license, the data is also required to assist ESB Networks' compliance with the distribution code and will enable the optimisation of security of supply in a time where dependency and loading on the network will continue to increase.

Other Party and User Access to The Smart Meter Data

ESB Networks is committed to protecting the rights and freedoms of individuals and has an operational GDPR capability in place across the organisation.

At present ESB Networks views its role as data controller of the smart meter data to be well defined. As such ESB Networks already processes data access requests for smart meter data which are executed in accordance with GDPR requirements. Data is only provided once a valid legal basis as defined per GDPR is provided.

With respect to providing a party (User, Data System User) with access to data from the Smart Meter Data System, ESB Networks welcomes further consideration on how the Smart Meter Data Access Code and its proposed processes will align with these already established processes.

ESB Networks also wishes to clarify that the smart meter data accessible via the Smart Meter Data System is not intended to be used for customer billing purposes. The existing Retail Market Systems and associated processes will continue to serve this purpose.

Methods of Access

ESB Networks, in its capacity as the DSO, will access data from the Smart Meter Data System via mechanisms such as application programming interfaces (APIs) and file transfer protocols (e.g., Secure File Transfer Protocol). ESB Networks has internal controls in place that are aligned with the principles of GDPR and ISO 27001 to ensure that the data is protected within our systems.

As the proposed holder of the newly created role of DSP (Data System Provider), ESB Networks is looking forward to engaging and working together with the other Data System Users (those outside of Customers and the DSO) to discuss the mechanisms for access to data from the Smart Meter Data System. It is important to first understand the data requirements of each User before designing the data access mechanism.

In the situation that a Data System User requires access to their customer's data before a data access mechanism has been delivered, it could request the data directly from the customer. With the delivery of the ESB Networks Customer Portal, the customer will be able to download their Harmonised Downloadable File (HDF), and should they wish, they can subsequently share this with the Data System User.

Summary

ESB Networks is supportive of working together with CRU and Data System Users on designing the most suitable way for users to access smart meter data from the Smart Meter Data System in relation to their data requirements. However, ESB Networks does welcome further consideration on how the Smart Meter Data Access Code and its proposed processes will align with the processes that ESB Networks already has in place for addressing data access requests. These processes are executed in accordance with GDPR requirements and ensure that data is only provided once a valid legal basis as defined per GDPR has been provided.

It should also be noted that the data available in the Smart Meter Data System may evolve over time as use cases are proposed, impact assessed, and approved through the processes of the Code. ESB Networks proposes that an initial Data Register is agreed and published alongside the Smart Meter Data Access Code to assist in the design and delivery of the Smart Meter Data System and the initial data requirements of Data System Users. The Data Register can then be updated when deemed necessary by the Code processes.

3.2 Response to Question 2

Question 2: The CRU would welcome any views on the annual compliance and assurance assessments placed on Users to the Code

ESB Networks agrees in principle with periodic compliance checks for adherence to the provisions of the Smart Meter Data Access Code. ESB Networks welcomes the opportunity to engage with CRU and relevant stakeholders in developing the scope of the proposed Annual Compliance Assessment and the associated Assurance Strategy.

Annual Compliance Assessment and Assurance Strategy

ESB Networks notes the proposals to conduct Annual Compliance Assessments for Users of the code. ESB Networks would welcome the opportunity for further engagement on the scope of the compliance assessments, the assessment frequency, and how these assessments will be implemented as part of the overall governance of the Smart Meter Data Access Code. Additionally, ESB Networks would welcome engagement on the application of the code and the interaction with the security compliance context for electricity providers through existing legislation (e.g. NIS-D). ESB Networks would also welcome further clarity on how these compliance assessments will interact with wider obligations under GDPR and License arrangements.

ESB Networks also notes the proposal for the development of an Assurance Strategy. ESB Networks would welcome the opportunity to engage and contribute to discussions with CRU and industry stakeholders on the development of this strategy and how it will be governed under the provisions of the code. Additionally, further detail is required on the scope and requirements for the Annual Information Security and Data Protection Assessment outlined in the consultation paper.

Further clarification would also be welcome on the role of the Code Compliance Officer in administering the Annual Compliance Assessments. ESB Networks would also welcome more detail on the role of the code panel in setting out the scope, and administration, of the Annual Compliance Assurance process.

Compliance Requirements

Compliance is a key element of the draft Smart Meter Data Access Code. ESB Networks is of the view that the compliance requirements need to be clearly defined in order to enable parties to fully assess their ability to achieve compliance with the provisions of the code. Further information is also required to specify what constitutes a “reasonable enquiry” as specified in the draft code. Furthermore, the draft code specifies the requirement for users to undertake self-certifications as part of the compliance process. ESB Networks would welcome clarification on the process for self-certification and how this interacts with the wider compliance provisions.

ESB Networks would also welcome further detail on how the compliance requirements interact with existing legislative and License requirements. ESB Networks currently aligns with a range of industry standards on data privacy and data security including ISO 27001, NIS-D and standards enforced by the Irish National Cyber Security Centre (NCSC). ESB Networks also implements processes to adhere to existing GDPR legislation. ESB Networks is of the view that clarity on how the provisions in the code will interact with these existing requirements and if the code will introduce an additional compliance obligation on ESB Networks as the DSP or as a User.

ESB Networks is of the view that the draft code should provide detailed requirements on the level of compliance checks that will be carried out on an annual basis. ESB Networks would welcome the opportunity to collaborate with CRU and industry parties to determine the detailed level of compliance certifications or standards required to meet the provisions of the code, including the periodicity of these checks. ESB Networks also notes that any additional processes or certifications required to comply with the code may result in additional resourcing and costs for Users and this will need to be fully assessed once the provisions of the code have been detailed.

Compliance and Assurance for the DSP Role

ESB Networks currently acts as a data controller for Smart Metering Data and is of the view that the role of DSP, as defined in the draft code, would align with its existing data controller responsibilities. The draft code requires greater clarity on the responsibilities of the DSP with respect to its data controller role and the compliance requirements for the DSP role.

Schedule 4 of the draft code outlines the requirement for the DSP to implement an Information Security Management System (ISMS) to manage data security and access to the Smart Metering Data System. ESB Networks currently employs a number of processes to align with industry standards, including ISO27001 and NIS-D, as well as GDPR legislation and would welcome the opportunity to engage with CRU on clarifying any additional compliance obligations required by the code. ESB Networks also seeks clarity on whether the Annual Compliance Assessment applies to the DSP and demonstrating alignment to the code requirements for the ISMS. ESB Networks would welcome the opportunity to work with CRU and industry stakeholders on developing hierarchy of processes.

ESB Networks' view is that the specifications for the DSP to comply should be fully documented within the provisions of the code. ESB Networks also is of the view that clarity is required on how the role of the DSP will be carried out with respect to other obligations under GDPR legislation and License obligations. Further clarity is necessary on how the requirements for the ISMS will be managed with respect to GDPR obligations.

ESB Networks is of the view that the scope of the provisions contained within Schedule 4 for the ISMS as well as the wider requirement for the Annual Compliance Assessment applies to the Smart Meter Data System and that the Retail Market systems and processes are not within scope of the code provisions.

ESB Networks will need to consider the required resource and budgetary requirements to undertake the annual compliance checks for the role of DSP. Full specification of the compliance criteria for the DSP role will be required in order for ESB Networks to conduct an assessment and ESB Networks would welcome the opportunity to engage with the CRU on these aspects and in relation to cost recovery for the role of DSP.

Summary

ESB Networks is supportive of compliance checks with respect to the provisions of the Smart Meter Data Access Code provided that these checks fulfil a demonstrated need, are clearly defined and operate within the wider context of GDPR requirements. ESB Networks is of the view that the compliance criteria and compliance processes for periodic Compliance Assessment be outlined fully within the code. ESB Networks view is that the compliance requirements for Users and the DSP role be specified clearly within the code. Clarity is also required on how the specifications for Annual Compliance Assessment will be administered with respect to other compliance standards and GDPR

requirements. ESB Networks looks forward to further engagement with the CRU and industry stakeholders on the scope and specifications of Compliance Checks.

3.3 Response to Question 3

Question 3: CRU would welcome any views on each of the options described for the governance and enforcement of the Smart Meter Data Access Code?

Smart meter data is a key enabler of the European Union's Clean Energy Package which aims to provide final customers with safe, secure, sustainable, competitive and affordable energy.

The legislative package seeks to enhance consumer participation by empowering them to manage their energy consumption on an equal basis with other market participants. It also requires the future electricity system to make use of all sources of flexibility, particularly demand side solutions and energy storage, and through digitalisation, integrate new technologies and services.

Smart meter data is fundamental to meeting these objectives.

The transition from an energy market which has traditionally operated on the basis of just 6 customer meter readings per year to one that has over 17,500 customer readings per year must be managed. It is right that smart meter data is protected by legislative and regulatory controls to ensure it is protected and used purely for legitimate purposes.

As set out in SI 37/2022, the SMDAC is intended to provide assurance to customers that their smart meter data is being managed in compliance with the requirements of GDPR and within rules that specify which parties have access to which data and for what legitimate purpose.

The SMDAC therefore plays a crucial role in assuring customers that the use of smart meter data in the electricity industry is appropriately governed.

ESB Networks supports the implementation of a governance model that provides consumers with confidence and assurance that smart meter data is being, and will continue to be, used for legitimate purposes.

Customers will be reassured that, as the Competent Authority, CRU will retain final authority regarding the SMDAC. In this context, ESB Networks favours a governance model that:

- allocates clear responsibilities and accountability to code parties
- can be implemented quickly, so that the benefits of smart meter data can be realised swiftly
- will facilitate agility and flexibility to meet security of supply concerns and the requirements of the CEP,
- is operationally economic and efficient, and,
- leverages familiar proven governance arrangements.

ESB Network's preference is for a governance option based on Option 5. This option, which was envisaged in our PR5 submission in 2019, is discussed further below along with our initial comments on the options presented.

<u>Option 1: Special Purpose Vehicle (SPV)</u>

ESB Networks notes that this option has been used in other jurisdictions where there are more complex market arrangements, for example where there are multiple entities responsible for smart meter systems. In those jurisdictions an SPV can be a vehicle to provide for common rules and technology protocols.

Given the structure and size of the Irish electricity market this option does not appear to be proportionate, economic or efficient.

ESB Networks therefore agrees with the CRU conclusion that the cost, complexity and timelines required to establish an SPV would be excessive and does not consider this option worth pursuing.

Option 2: Code Administrative Service

ESB Networks notes that this option has been used in other jurisdictions where there are more complex market arrangements. Given the structure and size of the Irish electricity market this option does not appear to be proportionate, economic or efficient.

ESB Networks agrees with the CRU conclusion that the cost, complexity and timelines required to establish and operate a CAS would be excessive and does not consider this option worth pursuing.

Option 3: In-House

We note that this option would require the establishment of an in-house Code Manager within CRU as well as support for data security, assurance, compliance, and enforcement.

Our review of the consultation document and draft code, as well as the discussions at the workshops held by CRU and Gemserv, confirmed that this option, and Option 6, require CRU to become a Data Controller with regard to smart meter data.

Our view is that this option creates an unnecessary overhead between CRU and the DSO as Joint Controllers or Controller-Processor which is not necessary to meet the requirements of SI 37/2022. Rather, it is for CRU, as Regulator, to set the rules for certain processing activities, within the scope of its statutory limit, and for the DSO to function as the Data Controller. This is explained further in our response to Question 9.

Establishing CRU as a Data Controller and/or Joint Controller of smart meter data would have significant implications for the timescales associated with implementation of the SMDAC, the operational cost and efficiency of this option.

ESB Networks' preference is to progress a governance option based on Option 5 and to defer further consideration of Option 3.

Option 4: Outsource to DSO

We note that this option has been used in other jurisdictions where the market arrangements and size are similar to those in Ireland e.g. the Flemish market.

Outsourcing code management is common within Ireland's energy sector. Other electricity codes, such as the Grid Code, Trading & Settlement Code and Distribution Code are maintained and managed by Licensees on behalf of CRU. These codes are also supported by panels, made up of relevant experts with final approval of modifications and regulatory oversight retained by CRU.

Concerns over potential conflicts of interest are managed effectively for these other codes. Typically, through business separation, ringfencing and the application of Licence conditions. An example would be SEMO who operate the TSC and the East-West Interconnector which is a market participant, yet both are part of the EirGrid Group.

ESB Networks currently operates several existing ringfenced entities on behalf of the retail market. With the MRSO responsible for the management of market registration processes and the processing / aggregation of meter data. Any concerns regarding the DSO role in regard to the SMDAC can be addressed through ringfencing or through Condition 12 of the DSO License.

ESB Networks' preference is therefore to progress a governance option based on Option 5 which considers outsourcing to RMDS as a ringfenced function of ESB Networks.

Option 5: RMDS as Code Manager

This option assigns the code manager role to RMDS which is a ringfenced function of ESB Networks.

RMDS perform an important function in the Irish electricity market with regard to Retail Market Design Governance, Assurance and New Market Entrants. These functions support the on-going development of the retail market which will continue to require focus and priority in support of the NSMP and wider CEP requirements.

ESB Networks is of the view that the operation of the SMDAC and administration of smart meter data can be best delivered through a similar arrangement by a ringfenced entity within ESB Networks.

ESB Networks' Alternative Option 5a: Ringfenced Unit within ESB Networks

ESB Networks' preference is for an efficient, agile and proportionate governance arrangement which is appropriate for the size and structure of the Irish electricity market and which uses familiar proven governance arrangements.

- ESB Networks currently operates several existing ringfenced entities responsible for the management of market registration processes and the processing / aggregation of meter data.
- With existing responsibilities for data management, ESB Networks is suitably positioned to undertake the role of Data Code Administrator with respect to smart meter data.

ESB Networks anticipated the regulations emerging from the Clean Energy Package and that are now transposed in SI 37/2022. In our PR5 submission a new Data Management Office was proposed. The Data Management Office would be responsible for:

- Maintaining Code Processes, Access Agreements and the Data Register.
- As chair of a Code Advisory Panel, engages with Advisory Panel membership and records minutes, actions and recommendations from the panel.
- Reviews smart meter data applications, Code modification requests and breaches of the Code.
- Makes recommendations to the CRU for approval.

Our view is that this alternative provides a better way forward and has the following benefits:

- Can be implemented quickly by leveraging the existing ringfencing arrangements that function within ESB Networks so that the benefits of smart meter data can be realised swiftly
- Avoids complexity of Joint Controller or Controller-Processor arrangements between CRU and the DSP
- Avoids placing CRU in an operational role for smart meter data management
- Is operationally the most economic and efficient of the options
- Will facilitate agility and flexibility to meet security of supply concerns and the requirements of the CEP
- Aligns with industry custom and practice for code governance (e.g., Distribution Code, Grid Code, Trading & Settlement Code), and
- Addresses any conflict of interest issues by utilising proven ringfencing arrangements

Option 6: Hybrid (In-house Code Manager plus Code Administrative Service)

ESB Networks notes CRU's preference for this model which relies on an In-House Code Manager and a Code Panel made up of Parties to the code.

There are a number of areas which require further clarity:

- How do the proposed functions interact with existing roles and requirements of GDPR, some of which appear to have been replicated or paraphrased?
    - We are concerned that there may be duplication and/or overlap inadvertently introduced that create potential confusion and inefficiency
- Whether the role of the Code Manager (CRU) is expected to be that of a Controller and therefore subject to all the requirements of GDPR?
    - ESB Networks' view is that this is not necessary to meet the requirements set out in SI 37/2022 which is explained further in our response to Question 9.
- We would welcome further clarity on the envisaged role of the Code Panel
    - We are concerned over the role of industry parties in assessing and vetting the applications of other parties and users, particularly where the parties are competing market participants
    - The draft code does not accommodate customers on the panel which we suggest should be reconsidered in the next iteration of the Code
- Whether the Code Manager (CRU) and/or the Code Panel (Parties) will be a Joint Controller or with the DSP or have a Controller / Processor relationship?
    - In either case, further draft schedules laying out the roles and responsibilities of the Joint Controllers/Processors for dealing with, amongst other things, liabilities and disagreements would be required.

ESB Networks considers that significant further detail of this option is required to better understand the roles and responsibilities of the Code Manager (CRU), the DSP, Users and Parties.

The proposed governance model will be unique in Ireland's energy market and distinct from existing proven governance arrangements, as such they are likely to require significant implementation effort.

ESB Networks is also concerned that the proposed processes would not be agile or flexible enough to meet security of supply concerns and the requirements of the CEP.

There is significant cost introduced in this option making it less economic and efficient than alternatives.

ESB Networks' preference is therefore to progress a governance option based on Option 5 and to defer further consideration of Option 6.

Conclusion

ESB Networks supports the objectives of the code as set out in SI 37/2022 but is of the opinion that the detailed drafting of the code can only be completed once a decision is made on the governance framework to be adopted.

Once a governance framework is decided upon a full review and assessment of implications for enacting roles and responsibilities can be completed. This can then enable full drafting of the code and further consultation prior to publication of the final code.

ESB Networks welcomes the governance options presented in the Consultation and is supportive of a clear governance model that supports the provision of smart meter data transparently, that is responsive and operates economically and efficiently.

We would welcome the opportunity to work with CRU to develop further detail on Option 5 whereby code management and smart meter data administration would be assigned to a ringfenced entity within ESB Networks.

3.4 Response to Question 4

Question 4: The CRU would welcome any views from interested parties on the remediation steps outlined above when a breach of smart meter data has occurred.

Background & Context

ESB Networks is cognisant of the high impact and negative consequences of a data breach at a national scale and are fully supportive of the principle that such breaches require a commensurate national level of remediation. ESB Networks currently employs a breach management process which is compliant with the provisions of GDPR. This is further reinforced through the application of the NIS-D framework to the smart metering solution. To this end ESB Networks continues to follow a security and privacy by design approach to all the Smart Metering Programme deliverables.

Implications of a breach

A smart meter data breach has the potential to include Personally Identifiable Information (PII) and as such a clearly defined breach management process that is aligned with GDPR is required for all users of the data. ESB Networks is of the view that full consideration of breach implications and responses is required to ensure that the provisions of the Smart Meter Data Access Code align with existing GDPR processes.

ESB Networks would also welcome clarification on the role of the DSP in supporting the enforcement of breach investigations under the code. Clarity is required on how investigations under the code will be conducted with likely parallel investigations by the DPC in relation to GDPR. As such, the interactions between code-related investigations and GDPR investigations need to be fully considered.

ESB Networks would welcome further engagement on the breach management process outlined in the code.

Breach remediation

These investigations can carry significant costs for the DSP, and these costs will require a cost recovery mechanism for both the cases when a User was at fault and also when there was no User at fault.

From the perspective of the DSP, ESB Networks would anticipate that breaches of its internal systems are minimised as far as possible by good system architecture and design practice, and good operational controls including delivery of access management systems. Processes are, however, in place to monitor for breaches and potential breaches, and these processes are in alignment with ISO 27001 requirements.

From the perspective of ESB Networks as a user of the data, controls of the availability of data are a prime resource towards minimising the effects of a breach.

Noting that:

1) The scale and repeatability of the breach will dictate the urgency of the remediation
2) The data types will dictate the consequences of the breach
3) Urgent “shut down” of data processing facilities may have consequences more severe than the breach

ESB Networks notes that formalising remediation processes is a complex task and further engagement is required to develop this as part of the code. It may also be worth considering an emphasis on good practice, continuous improvement, and alignment with common processes and compliance for GDPR to ensure that organisations:

1) Can act in a professional manner, in line with GDPR legislation, when breaches occur
2) Avoid conflicting internal breach remediation procedures that attempt compliance with existing legislation and with the code provisions.

Summary

ESB Networks as both the potential DSP and a User recognises that the area of breach management is critical. Further to this we look forward to exploring the breach management process and consequent remediation processes with a clear understanding of the roles and process applicable across the various impacted bodies both as part of the proposed Code governance and compliance and within the greater industry. Key to this process will be the alignment of breach management with GDPR and the formalisation of the notification and remediation monitoring processes within existing GDPR provisions.

3.5 Response to Question 5

Question 5: The CRU would welcome any views on Users' data security assessments required to access smart meter data. CRU would also welcome views from Parties of the Code who will be Users in relation to the provisions in place to access the data.

Background & Context

ESB Networks is committed to ensuring that the National Smart Metering Programme is delivered in compliance with applicable data privacy laws and that all ESB Networks customer data is safe and secure. ESB Networks' access to smart meter data is tightly controlled and multiple layers of cyber security are employed on ESB Networks' IT systems and business processes. The smart meters being deployed have been independently tested from a cyber security perspective and ESB Networks' Retail Market Systems are also subject to regular independent testing and review.

ESB Networks Obligations under the Smart Meter Data Access Code

ESB Networks understands that it has two sets of obligations, one as the DSP and the other in the role of a User (DSO) of smart meter data. As the DSP, ESB Networks will make best endeavours to comply with a set of policies and procedures to be known as the DSP Information Security Management System. As a Code Party User, ESB Networks will make best endeavours to comply with a set of policies and procedures to be known as its User Information Security Management System.

Scope of Data that can be accessed

ESB Networks believes that the provisions as set out in Schedule 4 apply to the Smart Meter Data System only and are not in reference to any other part of the Smart Metering solution including the AMI and Retail Market Systems. To this extent, only access to the Smart Meter Data System is considered in this response.

Compliance to a recognised Information Security standard

ESB Networks aligns itself to the ISO 27001 ISMS framework which helps us establish, implement, operate, monitor, review, maintain and continually improve our ISMS.

In the Smart Meter Data Access Code under Obligations on Users there is reference to "compliance to a recognised information security standard" and "certification to ISO/IEC 27001:2013". However, no such obligation is called out for the DSP.

ESB Networks would suggest a review on the feasibility of the requirement that all users looking to access smart meter data are expected to be compliant to a recognised information security standard. Continued compliance and the cost and effort that goes with that may cause difficulties for some users, especially smaller ones. Regular formal internal reviews and/or third-party audits of the DSP and Users' alignment with a recognised information security standard should be considered as it may be an appropriate control here.

ESB Networks proposes that the full requirements regarding compliance/alignment to a recognised information security standard should be clearly and formally called out for the DSP ISMS and User ISMS.

Information Security Incidents

While the Obligations on Users calls out the need to notify the Code Manager of security incidents, it does not place a similar obligation to also notify the DSP. In the event of a serious security breach affecting a user, the DSP would take all actions necessary to protect the Smart Metering Data System including possibly the complete removal of all access for that user. It would be imperative that the DSP is notified as quickly as possible in order to trigger the appropriate incident response procedures in a timely manner. The DSP would consider any serious incident e.g., Ransomware, anywhere within a user's infrastructure to be of concern, not just a breach affecting the smart metering data they hold or their process for retrieving the data from ESB Networks.

Whilst there are Obligations called out for Users to notify the Code Manager of security incidents, there does not seem to be an obligation called out for the DSP to notify the Code Manager of similar incidents.

Finally, as the Data Access Code calls out that Security Incident levels need to be properly classified, a formal clear definition covering the levels of classification needs to be agreed by all parties.

Summary

ESB Networks is focussed on ensuring the privacy and security of all smart metering data. We continue to operate and continuously improve our ISMS capabilities in alignment with the evolving nature of the cyber risk management. In both the role as the DSO and future DSP we are committed to working closely with the CRU to further explore and define the information security requirements both from an IT and OT perspective as these are further defined and explored under the Code within the context of the greater industry regulatory governance landscape.

3.6 Response to Question 6

Question 6: CRU would welcome any views on the data privacy obligations for data controllers and processors set out in this section and their adequacy in ensuring security of customers personal data.

Background & Context

The data privacy obligations, primarily contained in Schedule 5 to the draft Code, should be viewed in the context of the requirements of SI 37/2022, in particular Regulation 6(3), referenced in the table below.

We have mentioned in our response to consultation Question 3, in Section 3.3 that the governance model preferred by ESB Networks is that where ESB Networks itself performs the role of Code Manager. The comments below are based on the assumption that that governance model is adopted by CRU, but will apply to a greater or lesser extent to any other model.

Summary of current processes

There is already in place in Ireland a comprehensive suite of data protection legislation, principally GDPR, the Data Protection Act 2018 and the ePrivacy Regulations (collectively "DP Law"), all overseen by the Data Protection Commission (DPC). ESB Networks, and indeed all market participants, already have comprehensive processes and controls in place to manage all personal data held and processed by them in compliance with the DP Law. ESB Networks is continuously updating its' Records of Processing (ROPs) and Data Protection Impact Assessments to demonstrate its commitment to continued compliance in relation to smart meter data.

Data Protection Obligations and the Code

The processing of personal data is, as mentioned above, regulated by the DP Law, administered by the DPC. It is not the role of the CRU, or even of the legislature, to displace, or even duplicate, the role of the DPC in this regard. Rather, SI 37/2022 mandates that the Code should deal with certain matters which supplement, rather than override or replace the DP Law.

Large portions of Schedule 5 repeat, or paraphrase, the provisions of GDPR. ESB Networks believes that this is likely to create the potential for double regulation, where the CRU (or Code Manager) and the DPC would both appear to have jurisdiction over aspects of processing of personal data. Also, where the terminology of the Code and GDPR do not exactly match, there will be confusion as to the extent of any particular obligation, and the potential that a particular practice could be in breach of the Code but not GDPR, or vice versa.

It is ESB Networks' view that (a) the Code should not be a vehicle for duplicating DP Law and (b) there is in any event no benefit to CRU or indeed the consumer in creating a parallel or supplementary regime for the processing of personal data.

Rather, ESB Networks submits that the Code should take the opportunity offered to it by SI 37/2022, to further define and refine the roles and responsibilities of market participants and others in the context of smart meter data in the electricity industry, which is the province of the CRU. This can be done by reference to the detailed requirements of Regulation 6(3):

Item	ESB Networks Comment
(a) specify the point at which data shall no longer be considered personal data,	Whether or not any data is personal data is determined by GDPR and therefore an attempt to exclude certain data from the definition of personal data is likely to lead to challenge. Notwithstanding, it may still be possible to identify in the context of the specific industry or market sector, data that is not regarded as personal data.
(b) establish a clear definition of non-personal data, in accordance with the applicable European Union legal framework, that may be stored by eligible parties without the requirement for customer consent,	Where certain data is not personal data, it could be within the scope of the Code to determine rules for the retention or processing of such data, where a benefit for such regulation can be identified.
(c) clearly specify the purposes for which the electricity distribution system operator shall collect and process smart meter data,	Specifically addressing this issue, and defining the permitted purposes with clarity will be beneficial to all parties. In particular this is an opportunity to determine the lawful basis for the processing of personal data.
(d) specify the rights of access to data for final customers and third parties acting on their behalf,	The rights of access to data for final customers is already established by Data Protection Law. Where the CRU intends (in promoting the objectives of the Clean Energy Package or otherwise) that other parties should have access to the data, the Code can provide the rules for determining who should have access and under what conditions. In the governance model proposed, it is envisaged that ESB Networks would manage this area, subject to the criteria set out in the Code.
(e) specify the basis for the provision of smart meter data to electricity suppliers, SEMO and the transmission system operator,	As with (b), appropriate provision in the Code will provide the lawful basis for this category of processing.
(f) specify the smart meter data that may be transferred to eligible parties and the conditions under which such data may be stored by those parties,	See comment at (d) above

Item	ESB Networks Comment
(g) require that suppliers obtain each final customer's consent before that customer is switched to a dynamic electricity price contract, in accordance with Article 11(3),	This is a matter for suppliers, but would seem to be a relatively straightforward provision
(h) specify rules for the use of data by the distribution system operator for its systems planning and operational purposes, and	As with (b), appropriate provision in the Code will provide the lawful basis for this category of processing.
(i) specify the manner in which eligible parties are to have access to data and the reasonable and duly justified charges which shall be payable by the eligible parties.	See comment at (d) above

3.7 Response to Question 7

Question 7: CRU welcome any views on the steps outlined above in the event of a breach of smart meter data.

Background & Context

ESB Networks welcomes the opportunity to engage with CRU in relation to the provisions in the Smart Meter Data Access Code for breaches. ESB Networks currently has detailed operational processes in place to deal with operational system breaches and these are well established and formally agreed with ESB Networks IT partners. ESB Networks would welcome the opportunity to explore how these existing processes could support the implementation of the breach process outlined in the draft code.

In addition, at the data level, ESB Networks' existing GDPR breach processes are well established and fully implemented. ESB Networks would welcome clarity as to how the breach process outlined in the code will interact with existing breach processes required for GDPR compliance.

DSP and DSO context

ESB Networks currently acts as a Data Controller for Smart Metering data and is of the view that the role of DSP, as defined in the draft code, would align with the existing data controller responsibilities. ESB Networks therefore requires clarity on the responsibilities of the DSP with respect to breaches in smart meter data and how this relates to existing obligations as a Data Controller.

ESB Networks would expect that many of its existing process would form the basis for IT and data incident management. Any additional responsibilities necessary for the DSP would need to be recorded in the Code and would require updates to the incident processes currently employed. Data code governance and roles will need to be clearly defined to cover the responsibilities of the DSP regarding breaches.

Within the context of the DSP and any role required in the execution of remediation/consequences of breach needs to be further explored. Clear roles and responsibilities would need to be agreed and any required legal basis finalised before such actions can be taken. ESB Networks would welcome the opportunity to collaborate with CRU and industry stakeholders to further develop these considerations for the code.

Interdependency of breach processes and consequences

The interdependency across various regulatory obligations is not clear at this point in the code. ESB Networks will welcome further discussion on the hierarchy of regulation to be applied. As with any breach, the parties impacted by the breach need to be able to prepare for such an eventuality. Further detail would be required for all parties to update their incident management processes.

In addition, the scope and impact of the consequences need to consider that 'Operator of Essential Services (OEM)' nature of some of the data types involved. The DSO may well need to have special consideration in executing its responsibilities under the license and ensure national security of supply.

Summary

ESB Networks is committed to the ongoing operation of the Smart Metering solution. Breach and incident management remains at the centre of this focus.

We would recommend that existing processes and controls surrounding breaches be used as the basis for improvements where these are necessary. The level of risk and potential impact on security of supply requires that any breach process enhancements be clearly documented and communicated across all parties involved. In identifying proposed breach improvements, these need to take cognisance of existing ESB Networks GDPR and Cyber Security processes to avoid any areas of conflict or confusion.

We note that updates to the breach and incident processes are dependent on the overall Code design. These would then need to be reviewed once the Code has been developed further.

3.8 Response to Question 8

Question 8: CRU would welcome any views on Ceasing to be a Party of the code.

Background & Context

A new Schedule 7: Party Exit and Party Breach is referenced which has not been drafted. ESB Networks is of the view that aligning this process with other defined processes for the industry could be beneficial. For example, the process for a supplier exiting the market may have some procedures that would align with ceasing to being part of the code.

There may be a need for some obligations to be included within this schedule to ensure the return of terminal equipment, destruction of security credentials, operational data (e.g., API details, SFTP references) that should be securely managed (notwithstanding the GDPR requirements). Similarly, if the Party was a Code Panel or Subcommittee member, they may be party to confidential information. As such obligations under the code should not cease immediately but endure until all termination requirements are met.

Summary

ESB Networks welcomes the opportunity to support the development of and provide further views on Schedule 7 once a draft is made available.

3.9 Response to Question 9

Question 9: Do respondents have any other comments on other aspects of the draft code or its proposed governance?

Background & Context

Given there are several components of the code that are not yet drafted, ESB Networks' response to this consultation is subject to change until subsequent drafting is consulted upon. At this point in time, in addition to the responses to questions 1-8 above, ESB Networks wishes to provide comment on two further aspects, the Role of Controller within the SMDAC and the DSO License considerations proposed by CRU in section 3 (License Obligation Considerations) of the Consultation paper.

Role of Controller

In the draft code, there are various references to the CRU being a Data Controller (since GDPR, the term is simply "Controller"), or possibly a joint controller. ESB Networks believes that this results from a possible misunderstanding of the role of Controller under DP Law.

GDPR defines a Controller as the person, authority, agency or other body "which, alone or jointly with others, determines the purposes and means of the processing of personal data".

As a Regulator, the CRU is not -either alone or jointly with others – determining the purposes and means of processing. This is not the role of any regulator, and other regulators, such as the DPC or the Central Bank, do not see themselves as Controllers of the personal data managed by the bodies they regulate. The role of the CRU is to regulate the industry on the terms of its statutory mandate, which is contained in primary legislation.

Although the CRU, as regulator, has a significant role in determining the rules for how smart meter data is managed, it does not have access to the data on a day to day basis, and only ever sees the personal data of electricity users on an occasional basis, such as dealing with complaints. It is ESB Networks which has management control over its database of electricity customers and the data which flows through its systems due to its role as DSO. This is the case for traditional meters and meter data, and this does not change simply because the volume of smart meter data is much greater.

It should be noted that if CRU were to be a controller, then it would be (solely or jointly) responsible for all matters of compliance in relation to all smart meter data, and potentially liable in the case of any data breach or other breach of DP Laws. ESB Networks submits that this is not a responsibility that CRU needs or requires.

It should be noted also that the definition of controller in GDPR further provides that "where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". As the Code ultimately will derive its validity from SI 37/2022, which in turn is a vehicle for transposing parts of the Clean Energy Package, ESB Networks suggests that it is therefore open to CRU to designate ESB Networks as the controller for the purposes determined by the Code.

DSO License Considerations

CRU is considering licensing obligations that may need to be updated in order to ensure that License holders are required to adhere to the Code and to establish the CRU's compliance and enforcement responsibilities as set within the Code.

With respect to the DSO License, CRU have proposed two options, the first being a direction issuance to the DSO in relation to Condition 9 (Provision of Metering and Data Services), and the second a license modification with respect to Condition 9. 1 (e).

ESB Networks is of the view that license changes are required to implement the requirements of the Smart Meter Data Access Code as outlined under SI 37/2022, including the collection and provision of smart meter data to users/eligible parties. In particular the DSP role (as proposed in the draft) needs to be established under license.

Summary

ESB Networks is of the view that further consideration of the roles and responsibilities outlined in the code require further consideration and clarification. In particular, the role of the Data Controller under GDPR and how this is to be enacted needs to be further considered.

ESB Networks also notes the requirement of Licence changes to support the implementation of the code. ESB Networks welcomes further opportunity to engage with CRU on these proposals and considers that a change of licence may be warranted to support the enactment of the data code.

ESB Networks highlights that it may have additional comments on aspects of the Code that are yet to be drafted and would welcome the opportunity to do so once the content is available. ESB Networks looks forward to engaging with CRU and industry parties on the aspects of the code that have yet to be fully developed.

4. Conclusion

The power sector is undergoing transformative change under the Clean Energy Package, Climate Action Plan and changing consumer preferences. Data Privacy and Security will play a part in customer access to quality information derived from their smart meter data, empowering customers to make changes to manage their energy usage as per the provisions of SI No. 37 of 2022.

ESB Networks has a central role to play in facilitating this transformation. We aim to support customers in the transition towards being active participants in the energy system.

ESB Networks welcomes the consultation from CRU regarding the Smart Meter Data Access Code, which is a key enabler of facilitating the benefits of the wider NSMP. ESB Networks acknowledges the proposals put forward by CRU in this consultation. In particular, ESB Networks considers CRU's proposed requirements regarding leveraging of smart meter data and centrality of smart meter data, eligibility criteria and data access management as sensible suite of proposals to facilitate introduction of the Smart Meter Data Access Code.

ESB Networks considers that implementation of the Smart Meter Data Access Code should remain the primary focus for the retail electricity market in the near-term and we support CRU's position outlined in its consultation paper that an overarching requirement of the Smart Meter Data Access Code should be a straightforward and practical framework which can be implemented quickly and easily.

ESB Networks looks forward to working closely with both CRU and Market Participants to ensure the successful implementation of the 'Smart Meter Data Access Code' in the retail electricity market.

ESB Networks appreciates the opportunity to respond to this consultation and we remain available to discuss any element of our response with CRU at any time.