RETAIL ENERGY CODE

REC PERFORMANCE ASSURANCE – OVERVIEW OF DATA PROCESSING

1 DOCUMENT PURPOSE

The REC Performance Assurance Report Catalogue (PARC) details a range of data collected by the Code Manager from REC Parties and other industry participants to support Performance Assurance activities. This document provides a summary of the purpose and usage of the data collected, as well as key process and technical controls that apply.

This document is intended to provide REC Parties and other interested stakeholders with the information necessary to understand the rationale for data collection and usage. This document should assist relevant parties in completing appropriate activities under data protection legislation including completion of Data Protection Impact Assessments (DPIAs) where required.

Note that this document considers data set out in the PARC which is collected and processed on a regular basis. The Code Manager may request and collect additional data and information on an ad hoc basis (for example through application of the Request for Information Performance Assurance Technique (PAT) or during an RPA Assessment of a Party) which may be subject to manual review or application of structured data analysis techniques. Whilst many of the same principles apply in such circumstances, the exact information and data required and analysis performed will depend on the specific circumstances giving rise to the application of the PAT.

2 A DATA DRIVEN APPROACH

The REC represents a step-change for the industry with a mission to focus on customer outcomes through promoting innovation and competition. It puts consumer outcomes at the heart of the arrangements and introduces new robust technical and performance assurance frameworks for industry Parties.

The approach to REC Performance Assurance supports the consumer-centric and digitalised principles, and represents a change from predecessor codes – both in the breadth of Performance Assurance obligations and the greater use of data to proactively monitor risks and use this data to identify where further PATs need to be applied.

The decision to make significantly greater use of data in the approach was driven by a number of factors, notably:

- The breadth of the REC means that a traditional assurance approach would be much more time-consuming, inefficient and costly. The only viable alternative to the current approach would be a significantly higher level of manual assurance activity including on -site assessments and direct testing. This would include a need to perform a greater level of testing to confirm the absence of retail risk rather than focusing primarily on potential exceptions and non-compliance.

  We acknowledge that data provision is not without cost to parties but we consider this to be a proportionate approach, particularly in light of the significantly larger disruption and

higher cost the increased manual assurance activity including on-site assessments noted above would entail, the substantial cost of exception handling / issue resolution, or the potentially far greater compliance costs that may arise if risks are not adequately managed and mitigated at a code level and prompt subsequent regulatory intervention.

- We anticipate that the root cause of many of the issues facing industry relate to poor data quality or process failure caused by one Party resulting in impacts which other Parties then have to deal with. The only real way to address this is with targeted interventions based on assessing the related data.
- The role of the Code Manager is to measure and mitigate industry risks. Whilst some of these relate to the poor performance of individual Parties, others may actually relate to cross-industry problems, issues with REC services, or problems with the drafting of the Code itself. Our approach allows us to build the evidence base to address the wider drivers of risk in a way that party-by-party assessments can't.
- Feedback and criticism of similar and predecessor regimes has been the slow pace of change, with annual cycles, and a focus on symptoms rather than underlying causes. Our approach means that we can identify and act on emerging risks on a more timely basis rather than address well after the fact.

Whilst we believe a data driven approach will be very powerful we recognise there are areas where it may not be suitable or there are particular sensitivities with, or challenges in, obtaining the necessary data. We have been flexible in areas where an alternative approach is more appropriate in development of the Performance Assurance methodology to date and this is something we will continue to do, bearing in mind both the value that assurance work brings, as well as the different types of costs on Parties.

3 PURPOSE OF DATA PROCESSING

3.1 DELIVERY OF REC PERFORMANCE ASSURANCE

In line with the above all data is collected and processed to deliver the requirements on the Code Manager under the REC to monitor REC Parties against Retail Risks defined within the REC Risk Register and implement PATs agreed with the Performance Assurance Board (PAB). More specifically, this includes:

a) Identifying, measuring and monitoring individual retail risks. This includes directly assessing compliance with specifically measurable Code Obligations – for example completion of processes within the required timescales – and broader indications of Retail Risk and compliance – for example significant changes in the volume of failed switches or a volume of failed switches that is outside the norm for peer Parties.

b) Informing the PAB in setting thresholds to be applied when assessing Retail Risk, based on establishing reasonable expectations of the level of deviations and exceptions observed.

c) Assessing the impact of issues identified, including measurable Code Obligations per (a) above, in terms of impact on consumer outcomes and other REC Parties (as per the REC definition of Retail Risk). This will be used both to prioritise application of PATs but also to identify Code requirements that do not contribute to reducing Retail Risk and hence could be considered for removal (for example a requirement to complete

processes within a timescale that is often not achieved but which has no subsequent impact on consumers or other parties).

d) Informing the identification of new and emerging risks, for example though analysis to identify where significant volumes of complaints are being made on a specific topic area but where existing related Risk Metrics have not identified potential issues or through ad-hoc analysis to confirm if an issue identified during an RPA Assessment is more pervasive. Aggregated data does not provide the necessary data resolution and nuance to identify and distinguish genuinely new risks from existing known issues.

e) To directly apply or monitor the application of certain Performance Assurance Techniques – specifically to create Peer Comparisons, monitor applicable Action Plans or for monitoring of compliance with Specific Conditions including Controller Market Entry Conditions.

f) Where specific prescribed Performance Assurance activities are included within the REC – for example monitoring of Smart Meter Installation Surveys.

3.2 ACTIVITY NOT IN SCOPE

For the avoidance of doubt, data collected by the Code Manager as defined in the PARC is collected solely for the purpose of delivering REC Performance Assurance. The data will not be used to assess compliance of Parties with other industry codes or regulation, even where the same information is obtained for REC and these other obligations (the reuse of existing reporting has been adopted for some REC Performance Assurance activities to reduce burden on Parties). Performance Assurance activities will however be developed recognising the context of wider industry risks and processes, recognising there may be opportunities to reduce holistic risk through activities taken under the REC.

For example, data regarding complaints will not be used to assess compliance with complaints handling standards, which is already subject to separate monitoring by Ofgem. Similarly performance charges would not be applied for the same criteria as already apply for Guaranteed Standards of Performance to avoid creating a ‘double jeopardy’ scenario.

3.3 USE OF METER POINT LEVEL DATA

Part of the change in approach to Performance Assurance outlined in section 2 is a greater use of more granular data. Whilst we have sought to utilise existing aggregated reports wherever possible, these would not be sufficient to fulfil the design principles of the PAF as set out in the Performance Assurance Methodology (available here) and facilitate evidence-driven improvement to retail processes. The granular data includes some items of personal data, principally the meter point (MPAN or MPRN, collectively MPxN). Although considered personal data it is important to note that no REC Performance Assurance data analysis is performed in respect of individuals – data is however required at an MPxN level in order to calculate, triangulate and follow-up on many of the specific retail risk metrics. The reasons for the use of granular data, including MPxN, are expanded upon below:

- Permit differing data sources and the results of different individual analysis (e.g. monitoring of different retail risks) to be linked. MPxN is an existing industry-wide masterdata item that supports this requirement and hence was selected for use. Linking data in this way supports activity including:

  - linking indicators of adverse consumer outcomes (e.g. erroneous transfers, complaints) with known exceptions (e.g. data quality issues, process failures) to support assessing the impact of issues identified;
  - identifying potentially related process failures, potentially across different Parties and Party types (e.g. non-timely update of meter details and a delayed switch); and
  - Identifying meter points with repeated exceptions, indicating a deeper underlying issue or inappropriate remedial action taken by Parties.

- Reduce the frequency and breath of follow-up enquiries of Parties (which would otherwise be required if potential issues were identified in aggregate-only data in order to confirm and pinpoint issues). Given the breath of Performance Assurance activities and monthly cadence of Performance Assurance risk assessment and PAB reporting the use of RFIs in this way, given the likely lead time required by Parties, would create a significant lag in Performance Assurance activities and would impose a unpredictable and potentially sizeable reporting burden on Parties.
- Permit more targeted and specific RFIs to Parties when they are required – i.e. if potential issues are identified the specific meter points and exceptions can be provided to Parties to facilitate analysis and follow-up activities.
- Facilitate root cause analysis of exceptions identified – for example allowing analysis to identify a significantly greater level of switching issues due to poor address quality for a given DNO but independent of suppliers – indicating the underlying cause may be due to the DNO rather than supplier Party activity and hence directing the focus of Performance Assurance activity. Whilst this analysis could in principle be undertaken with aggregated data (but including a greater level of attribute breakdown than is currently reported by Parties) this would still require changes to reporting requirements and a pre-determination of the attributes that may be of interest. By obtaining MPxN data there is greater flexibility of the integration of causal attributes without requiring changes to the majority of data collection.
- Enable earlier identification of new and emerging concerns, particularly where the data does not fit the pattern of existing known issues which are subject to monitoring. With the magnitude of changes in the industry (smart meter rollout, faster switching, new and innovative products, new business models), a forward view on emerging issues is vital for the protection and enhancement of consumer outcomes.
- Provide Parties with direct and actionable visibility of the data used for Performance Assurance monitoring – thus supporting and encouraging parties to proactively improve performance to the benefit of consumers.

RETAIL ENERGY CODE

4 PERFORMANCE ASSURANCE DATA PROCESSING CONTROLS

In developing and executing the Performance Assurance approach the Code Manager has and will apply a number of process and technical controls to manage the risks to the processing of high volumes of data, including personal data items. These include:

Performance Assurance Data Processing Control	Overview
Data Minimisation	In developing the Performance Assurance Report Catalogue the extent of personal data collected was minimised as much as possible. For example the capture of full data flows was rejected due to inclusion of unnecessary personal data, complaint narrative was excluded due to the risk of including sensitive customer details, customer name was not included in any new data items and an alternate approach was taken to assuring PSR processes (direct assurance) given the sensitivity of the related data.
Manage personal data retention periods	Data Retention and associated Data Lifecycle rules are applied by the Code Manager. Data retention periods range from 14 – 28 months, driven by the need to support annual performance reporting, tracking of trends and patterns over time and reflecting existing timescales for resolution of certain issues particularly relating to meter data.
Pseudonymise personal data (applied to Data Transfer Service data only)	All the MPAN data obtained from Electralink uses a pseudo anonymised MPAN by default (although it is possible to 'de-anonymise' the data if required to link to other data).
Encryption of data at rest and in motion	Data is encrypted on upload to the portal and is encrypted at rest and in any further data transfer as part of the Performance Assurance Data Analysis.
Manage persons within the organization who have legitimate access	Access to all data is limited to Code Manager personnel providing the specific Performance Assurance services as part of normal identity and access management processes. This includes periodic reviews of access.
Manage third parties with legitimate access to personal data	Access by third-party providers to the Code Manager is controlled and managed through the contracts in place between RECCo and the Code Manager providers.

Performance Assurance Data Processing Control	Overview
	Outside of the Code Manager access to detailed (MPxN) level data is limited to the REC Party to which it relates – i.e. no MPxN data is provided as part of wider peer comparisons or to PAB members.
Data Protection by design / Data Protection by default	These requirements are built into the Code Manager processes for the design and implementation of the Code Manager Performance Assurance analytics environment, and were assessed through completion of the DPIA process.
Awareness and Training	All Code Manager Performance Assurance Personnel are required to complete and refresh a range of data protection training and awareness initiatives as part of standard compliance activities.