



# Data Privacy Plan

## *Northern Powergrid's approach*

### INTRODUCTION

- Paragraph 10A.2 of standard licence condition 10A of our electricity distribution licence (SLC10A) prohibits us from obtaining any Electricity Consumption Data in respect of Relevant Premises, which relates to a period of less than one month, unless the requirements of any of paragraphs 10A.4, 10A.6, 10A.7 or 10A.8 of SLC10A are satisfied.
- This document, called Northern Powergrid's Data Privacy Plan ('DPP'), constitutes our proposal to the Gas and Electricity Markets Authority under paragraph 10A.4 of SLC10A, regarding the practices, procedures and systems that Northern Powergrid will implement to ensure that, so far as is reasonably practicable, the outcome described at paragraph 10A.5 of SLC10A is achieved. Namely, that Electricity Consumption Data, which is obtained by us and relates to a period of less than one month, ceases (through aggregation with other Electricity Consumption Data or by means of any other process) to be data which is capable of being associated with a Domestic Customer at Relevant Premises so far as is reasonably practicable.
- Whilst we are still confident our previous proposal did meet the requirements of SLC10A, protected customers' privacy and retained utility of the data, we acknowledge Ofgem's opinion and interpretation of the licence condition. We remain ambitious to ensure that our customers receive the maximum benefits available from access to half-hourly electricity consumption data provided by smart meters. Prompted by Ofgem, in February 2020 we wrote to BEIS formally requesting a review of the SLC10A licence obligation and we remain committed to working with BEIS and Ofgem on revising the wording of this licence obligation to protect and enhance the benefits available for customers.
- In developing our DPP, our current proposal is to:
  - Aggregate half-hourly Electricity Consumption Data immediately on collection;
  - Automatically and permanently delete the source half-hourly Electricity Consumption Data as soon as it has been aggregated, without it ever having to be stored;
  - Associate the aggregated data with the relevant distribution substation, low voltage feeder or low voltage feeder section reference as an identifier; recognising that only c2.25% of our feeders have fewer than five MPANs associated with them; and
  - Use data masking, where the number of premises on a particular feeder is insufficient to enable half-hourly Electricity Consumption Data to be aggregated, in order to reduce the risk of associating that data with Domestic Customers. We will do this by storing the relevant data with its feeder reference, rather than its MPAN, as an identifier. Currently, only 0.58% of our feeders (totalling approximately 22,300 premises) have just one premises connected to the relevant feeder.
- We believe that these arrangements will deliver the outcome described at paragraph 10A.5 of SLC10A. That is to say, they will prevent, so far as is reasonably practicable, half-hourly Electricity Consumption Data obtained by us from being associated with a Domestic Customer at a Relevant Premises.

## Contents

Data Privacy Plan .....	0
1. Explain clearly what electricity consumption data will be accessed .....	2
2. Explain how smart metering data compares favourably against traditional electricity consumption data .....	8
3. Provide assurance that any commercial use of the data by the DNO or third parties is excluded from these purposes, both before and after the data anonymisation.....	9
4. Explain clearly how, where, when and by whom collation, maintenance, use and deletion of the data would take place securely and cost-effectively.....	9
5. Demonstrate that consideration has been given to the best available techniques for minimisation, aggregation, anonymisation and/or other treatment of data.....	10
6. Be accompanied by a Privacy Impact Assessment, consistent with the ICO's code of practice .	12
7. Demonstrate the conformity of the adopted IT security process to the ISO 27001:2013 and ISO 27005:2018 standards .....	13
8. Demonstrate that, in developing its privacy plan, the DNO has engaged constructively with relevant stakeholders .....	14
Appendix A: Glossary of Terms .....	17
Appendix B: Process Documentation.....	19
Appendix C: Benefits Assessment.....	19
Appendix D: Data Retention .....	19
Appendix E: Importance of access to consumption smart metering data .....	19
Appendix F: Privacy Documents - Data Privacy Statement & Data Privacy Impact Assessment.....	19
Appendix G: ISO27001:2013 Certificate & Scope Document .....	20
Appendix H: Consumer Research and Stakeholder Consultation Activity.....	20

## 1. Explain clearly what electricity consumption data will be accessed

1. For the purposes of this DPP, we have adopted the definition of personal data used in the Data Protection Act 2018, i.e. personal data is 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, and in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person. Consequently, the disaggregated half-hourly Electricity Consumption Data (Service Requests 4.8.1 – Read Active Import Profile Data and 4.8.2 - Read Reactive Import Profile Data) that we obtain (via Service Requests 4.8.1 – Read Active Import Profile Data and 4.8.2 - Read Reactive Import Profile Data) from premises associated with an identified or identifiable living individual is personal data.
2. Only aggregated half-hourly Electricity Consumption Data will be stored and hence only aggregated half-hourly Electricity Consumption Data can be extracted from our secure, ISO27001:2013 certified Smart Metering Gateway system. The only exception will be in the limited circumstances where only one premises is connected to a feeder, in which case we shall employ data masking in respect of those premises and store that masked data against the relevant feeder reference. We will deal with masked half-hourly Electricity Consumption Data in the same way as we will deal with aggregated half-hourly Electricity Consumption Data for the purposes of this DPP.
3. In summary, for the purposes of Standard Licence Condition 10A, our proposal is as follows:
4. Once a smart meter is successfully commissioned, we will initiate a process to obtain half-hourly Electricity Consumption Data, initially on a monthly basis (via Service Requests 4.8.1 – Read Active Import Profile Data and 4.8.2 - Read Reactive Import Profile Data);
5. Immediately on receipt, we will (i) aggregate the half-hourly Electricity Consumption Data with half-hourly Electricity Consumption Data from other smart meters associated with the same distribution substation, feeder or feeder section, as appropriate; (ii) calculate high level metadata; (iii) store the aggregated data and metadata in the Gateway; and (iv) automatically and permanently delete the source half-hourly Electricity Consumption Data as soon as it has been aggregated;
6. Access to the aggregated half-hourly Electricity Consumption Data and associated metadata will only be made available when it is required to support authorised business activities;
7. We will store the following, which is derived from disaggregated half-hourly Electricity Consumption Data:
  - a. Aggregated half-hourly Electricity Consumption Data for each distribution substation;
  - b. Aggregated half-hourly Electricity Consumption Data for each feeder;
  - c. Aggregated half-hourly Electricity Consumption Data for each feeder section;
  - d. Masked half-hourly Electricity Consumption Data in circumstances where only one premises is connected to a feeder;
  - e. For each MPAN, metadata including:
    - i. The total monthly consumption value ;
    - ii. The highest consumption value each month and the associated date / time;
    - iii. The lowest consumption value each month and the associated date / time;
    - iv. Mean of the maximum daily half-hourly Electricity Consumption values over a month ;
    - v. Standard deviation of the Maximum daily half-hourly Electricity Consumption values over a month;
    - vi. Mean of the minimum daily half-hourly Electricity Consumption values over a month; and
    - vii. Standard deviation of the Minimum daily half-hourly Electricity Consumption values over a month;
8. Access to aggregated half-hourly Electricity Consumption Data and metadata will be limited through access controls, separation of duties and authorisations based on approved tasks. Gateway users will only have the access necessary for them to undertake legitimate business tasks for the purpose of their role. The processes

for gaining access to extracts of aggregated half-hourly Electricity Consumption Data are documented in Appendix B, together with illustrative use cases;

9. The aggregated half-hourly Electricity Consumption Data sets will be deleted on a rolling basis following expiration of a seven year retention period from the date of aggregation.

#### **Frequency of collection**

10. Our justification for collecting disaggregated half-hourly Electricity Consumption Data initially on a monthly basis is that Reactive Import Profile data is only held in the meter for three months.
11. A less frequent collection period increases the risk, impact and management overhead if the DCC's service responses fail. As meter volumes and message traffic increase over time, smaller message payloads will most likely have a higher chance of successful delivery.
12. In obtaining half-hourly Electricity Consumption Data we will:
  - a. Monitor the DCC's service responses to check for missing data;
  - b. Enable auto-retry processes, if required; and
  - c. Set the timing of service requests and follow-up tasks to spread the data traffic on the DCC's infrastructure and discuss that timing with the DCC's representatives before commencing data processes.

#### **Access Control Processes**

13. Only authorised users will be able to access aggregated half-hourly Electricity Consumption Data extracts. Access controls will limit the functionality available to the individual. User profiles and individual account controls will determine the level of access provided to the individual. All user activity will be monitored via audit logs.

#### **Submitting requests for an aggregated extract of half-hourly Electricity Consumption Data**

14. As the process of aggregating disaggregated half-hourly Electricity Consumption Data is entirely automatic, the disaggregated half-hourly Electricity Consumption Data will not be written to disk and only held temporarily whilst it is being aggregated. Consequently, it will not be possible for a user to access the disaggregated half-hourly Electricity Consumption Data.
15. Only business users with legitimate business justification will have access to aggregated half-hourly Electricity Consumption Data.

#### **Monitoring and validating requests for an aggregated extract of half-hourly Electricity Consumption Data**

16. Details of each request will be retained in the Gateway's audit log of user activity.
17. A business rationale for needing access to the aggregated half-hourly Electricity Consumption Data and the relevant line manager's approval must be provided before a user will be able to access aggregated half-hourly Electricity Consumption Data.

#### **Providing an aggregated extract of half-hourly Electricity Consumption Data**

18. An authorised user of the Gateway will be able to access the aggregated half-hourly Electricity Consumption Data extracts. The input required for the request will be distribution substation, feeder or feeder section, Service Requests and the Time Period.
19. The extracted aggregated half-hourly Electricity Consumption Data will be given an appropriate data confidentiality classification and will be provided to the requestor electronically. The aggregated half-hourly Electricity Consumption Data extract will only contain details of the times and dates that the extract covers, the aggregated half-hourly Electricity Consumption Data relating to each 30-minute window in the period

covered by the extract and the number of data points (i.e. MPANs) aggregated in each time period. The aggregated half-hourly Electricity Consumption Data extract will not include any MPANs.

### Safeguards and Compliance

20. The following safeguards will be implemented to ensure that our customers' privacy is protected and that we comply with Data Protection Law and the appropriate standard conditions of our electricity distribution licence.
21. We have a contract in place with \_\_\_\_\_ for the provision of the Gateway and associated maintenance and support services. On receipt of confirmation that our data privacy plan has been approved by Ofgem and before we obtain any half-hourly Electricity Consumption Data, we will agree a variation to that contract with \_\_\_\_\_ such that the contract complies with the requirements of Article 28 of the GDPR, as necessary. This will ensure that appropriate obligations will be placed on \_\_\_\_\_ regarding the security of the half-hourly Electricity Consumption Data within the Gateway.

### Lawful basis for processing Personal Data

22. The General Data Protection Regulation (GDPR) and The Data Protection Act 2018 allow organisations to process personal data as long as they do so in a lawful, fair and transparent manner. Article 6 of the GDPR recognises that processing is only lawful if there is a lawful basis for doing so.
23. We have, therefore, considered on which lawful basis we will be processing the disaggregated half hourly Electricity Consumption Data. Although we can see arguments that the lawful basis may be for the performance of a task carried out in the public interest/exercise of official authority, we have concluded that the most appropriate lawful basis for processing the disaggregated half-hourly Electricity Consumption Data is for the pursuit of the legitimate interests of Northern Powergrid, as the data controller, or by third parties, with such third parties being other customers connected to the network.
24. In reaching that conclusion, we have conducted a legitimate interests assessment as follows:

a) **Purpose:**

The purpose of the processing is to facilitate compliance with our principal statutory duty under the Electricity Act 1989, which is to develop and maintain an efficient, co-ordinated and economical system of electricity distribution. We will only process disaggregated half-hourly Electricity Consumption Data in order to anonymise that data by means of aggregation, as explained elsewhere in this DPP, and will only use the aggregated half-hourly Electricity Consumption Data so created for the purpose of improving our electricity distribution network for the benefit of our customers.

b) **Necessity:**

Being able to process disaggregated half-hourly Electricity Consumption Data for the purpose set out above will have significant long-term benefits for both Northern Powergrid and its customers. Those benefits are discussed in this DPP and additional supporting information is provided in Appendix C.

Our proposed means of processing the disaggregated half-hourly Electricity Consumption Data is reasonable in that disaggregated half-hourly Electricity Consumption Data will be temporarily held, but not stored, in the Gateway whilst being aggregated before being stored in the Gateway in aggregated form for 7 years) such that the processing will only be undertaken in order to create the aggregated half-hourly Electricity Consumption Data that will be used for network analysis and design purposes.

The processing of the disaggregated half-hourly Electricity Consumption Data will not intrude on, adversely impact or disturb the data subjects in any way.

c) **Balancing of interests:**

The data subjects are the customers connected to our network and, as a result of the smart meter roll-out, half-hourly Electricity Consumption Data from their smart meters will be used for settlements and billing purposes. Consequently, it is reasonable to assume that customers would expect this data to be used as part of the process of providing them with a supply of electricity. This assumption is supported by the stakeholder engagement and consumer research we have undertaken on the subject, details of which can be found in Appendix H.

As noted above, the processing of the disaggregated half-hourly Electricity Consumption Data will not intrude on, adversely impact or disturb the data subjects in any way. The way in which we will process the disaggregated half-hourly Electricity Consumption Data will not cause the data subjects any harm. The opposite is, in fact, true; i.e. the processing will benefit the data subjects by supporting improvements to the electricity distribution network that powers their everyday lives.

25. Having conducted the above legitimate interests assessment, we have also concluded that the legitimate interests being pursued are not overridden by the fundamental rights or freedoms of the data subjects concerned but that our legitimate interests and those of our customers are aligned because the purpose of the processing is to facilitate the provision of a more efficient, economical and efficient electricity network.
26. We will review this legitimate interests assessment as part of the regular review of this DPP in order to ensure that the conclusions continue to hold good. We will make any changes considered necessary by such reviews.
27. We are already a trusted and experienced controller of personal data and special category personal data, including maintenance of our Priority Services Register in accordance with standard licence condition 10.

#### **Accountability**

28. The disaggregated half-hourly Electricity Consumption Data we obtain will be subject to our Data Protection Law Compliance Policy, which includes the processes by which we will respond to individuals exercising their rights under Data Protection Law e.g. providing personal data to data subjects, if it is requested.

#### **Accuracy**

29. The disaggregated half-hourly Electricity Consumption Data being aggregated will be accurate because it will be received directly from the relevant smart meter via the DCC.

#### **Aggregation**

30. We will anonymise disaggregated half-hourly Electricity Consumption Data through aggregation.
31. A distribution substation, feeder or feeder section reference will be provided by the data requester. Aggregated half-hourly Electricity Consumption Data would only be provided in response if aggregated data is available. The count of the number of data points aggregated as part of the aggregation process will be returned with the results. The aggregated half-hourly Electricity Consumption Data will not include details of individual meters, MPANs, premises or customers.

#### **Confidentiality**

32. Disaggregated half-hourly Electricity Consumption Data will be processed but not stored in the Gateway. Direct access to the Gateway's administrative functionality will be limited to authorised users who have been given security clearance following a background check in line with BS7858:2019. Gateway access controls will limit the functionality available to the user, user profiles and individual accounts will determine the level of access afforded to the user and all user activity will be monitored via audit logs.

#### **Integrity**

33. All disaggregated half-hourly Electricity Consumption Data received from the DCC will be temporarily held, but not written to disk, whilst it is being aggregated with other disaggregated half-hourly Electricity Consumption Data received that is associated with the same distribution substation, feeder or feeder section. In a small number of cases, where the network topology is such that there are only a small number of customers

connected to a feeder or feeder section, it is possible that half-hourly Electricity Consumption Data associated with small numbers of customers will be aggregated. This will only be the case in a small number of cases. Further details are provided at paragraph 90. Aggregated half-hourly Electricity Consumption Data will be stored in the Gateway with a distribution substation, feeder or feeder section reference. Access to the Gateway database for update purposes is restricted to authorised technical support personnel only.

#### **Limitation of purpose**

34. Disaggregated half-hourly Electricity Consumption Data will only be obtained, aggregated and used in order to comply with our principal statutory duty under the Electricity Act 1989 to develop and maintain an efficient, co-ordinated and economical system of electricity distribution.

#### **Oversight**

35. All user requests for access are recorded in the Gateway within the Audit Log. User access to aggregated half-hourly Electricity Consumption Data will be overseen by our Smart Metering Security Working Group. This group already oversees smart metering IT security matters, including compliance with ISO27001:2013 and adherence with the Smart Energy Code (SEC)'s security obligations. Consequently, including data privacy matters and the continued maintenance of this DPP within that Group's remit fits well with its existing obligations.

#### **Regular review**

36. This DPP will be subject to regular review in order to ensure that it remains fit for purpose.
37. The frequency of the reviews will be determined by the Smart Metering Security Working Group and will be at least every 3 years or any occasion when we plan a material change to our arrangements for the collection and/or aggregation of disaggregated half-hourly Electricity Consumption Data.

#### **Rights of data subjects**

38. Given that we will only store data that is anonymised, either by aggregation or data masking, it is unlikely that we will have to take action in response to data subjects seeking to exercise their rights under Data Protection Law. However, our approach is set out below in the event that we do have to take such action.

#### **Right of access**

39. Under Data Protection Law, data subjects have the right to obtain from us confirmation of whether or not their personal data is being processed and for access to the personal data we hold. Any such requests will be handled in accordance with the process set out in our Data Protection Law Compliance Policy and we will provide the data subject with the personal data we hold that has been requested.

#### **Right to erasure**

40. Under Data Protection Law, data subjects have the right to have personal data erased. These requests will be handled in accordance with the process set out in our Data Protection Law Compliance Policy. When we receive such a request, we will block future receipt of disaggregated half-hourly Electricity Consumption Data associated with the data subject's MPAN, irrespective of whether one of the grounds for erasure set out in Article 17 of the GDPR actually applies. We will not be able to erase disaggregated data from a stored, aggregated dataset.

#### **Right to be informed**

41. In order to provide transparency over the way in which we will process half-hourly Electricity Consumption Data and meet our obligation to provide 'fair processing information' to data subjects, our privacy policy is posted on our website at (<http://www.northernpowergrid.com/privacy-policy>). We have drafted the changes needed to inform customers of the collection and processing of disaggregated half hourly Electricity Consumption Data should our DPP be approved (see Appendix F).

**Right to rectification**

42. Where individuals advise us that their disaggregated half-hourly Electricity Consumption Data is inaccurate or incomplete, we will either rectify that data in accordance with the process set out in our Data Protection Law Compliance Policy or erase it.

**Right to restrict processing**

43. Under Data Protection Law, data subjects have the right to restrict processing of their personal data. These requests will be handled in accordance with the process set out in our Data Protection Law Compliance Policy.
44. Where we are notified by data subjects that they would like us to restrict our processing of their disaggregated half-hourly Electricity Consumption Data, we will deal with that request in compliance with Article 18 of the GDPR and restrict that processing accordingly.
45. In the event that we verify that the data subject's disaggregated half-hourly Electricity Consumption Data is inaccurate, we will either rectify or erase the data concerned.
46. For the reasons set out elsewhere in this DPP, we believe that we have a lawful basis for processing the data subject's disaggregated half-hourly Electricity Consumption Data, which means the data subject's right to restrict the processing of their personal data under Article 18(1)(b) and Article 18(1)(d) of the GDPR may not apply. We would, however, give appropriate consideration to each request, taking account of the particular circumstances of that request.
47. If it becomes necessary to restrict processing, technical controls within the Gateway will be implemented. The Gateway will identify MPANs relating to any data subjects who have requested us to restrict the processing of their disaggregated half-hourly Electricity Consumption Data. Periodically we will determine whether the data subject still resides at the same premises and establish if they still require us to restrict processing.

**Right to object**

48. Under Data Protection Law, data subjects have the right to object to the processing of their personal data in certain circumstances, one of which is where the lawful basis for that processing is in the legitimate interests of the controller or a third party. Consequently, data subjects will have the right to object to our processing of their disaggregated half-hourly Electricity Consumption Data. Any such objections will be handled in accordance with the process set out in our Data Protection Law Compliance Policy.

If we receive such an objection, we will assess the reasons given by the data subject for the objection, taking account of the conclusions of the legitimate interests test we have carried out for the purposes of this DPP and the particular circumstances of the objection. In the event that we conclude that the objection is valid, we will erase the personal data in question from the Gateway.

**Rigorous approval process**

49. Segregation of duties will provide a strong review and approval process and ensure that rigorous control is exercised over access to aggregated half-hourly Electricity Consumption Data and, therefore, customers' privacy is respected.

**Storage limitation**

50. We propose to retain aggregated half-hourly Electricity Consumption Data in the Gateway for seven years, based on the expected five-year duration of future price control periods plus two additional years for network analysis and/or investment planning purposes. After this time, the data will be deleted.
51. A seven year retention period is consistent with our approach for retaining half-hourly network monitoring data from our SCADA system in a readily accessible form.



52. This approach is also consistent with the retention period in the Electricity Network Association's Generic Privacy Framework, which was ten years having been based on the duration of the current price control period (of eight years) plus an additional two years of data for network analysis and/or investment planning purposes.
53. Extracts of aggregated half-hourly Electricity Consumption Data that are provided to authorised users will be deleted after seven years. Additional information on our justification for the above retention periods including a copy of our Policy on the Retention and Destruction of Records is contained in Appendix D.

## 2. Explain how smart metering data compares favourably against traditional electricity consumption data

54. An extract from our Well Justified Business Plan showing smart metering programme benefits is included in Appendix C. An analysis of Ofgem's regulatory reporting requirements is also provided in Appendix C. The benefit categories dependent on gaining access to disaggregated half-hourly Electricity Consumption Data have been identified.
55. Additional evidence submitted to the BEIS Data Access and Privacy Framework review is included in Appendix E and explains the importance of access to disaggregated half-hourly Electricity Consumption Data for the purposes of operating an efficient, co-ordinated and economical electricity distribution network. The conclusions are summarised below.
56. Smart meters will increase the amount of data available about power flows at a granular level on our network. Access to half-hourly Electricity Consumption Data will enable us to plan and operate our network more efficiently. Demand for electricity and for the generation of electricity is expected to increase significantly, changing the way electricity networks are designed and managed. Perhaps most importantly, the ways in which generation is fed into our network will change moving away from a "top-to-bottom" model to a "leopard-spot" model of generation across the LV networks. Access to disaggregated half-hourly Electricity Consumption Data, ensures that networks can be accurately designed and operated, saving customers' money and enabling the increases in energy and generation uses away from the traditional models.
57. The historical method of designing LV networks was based on statistical forecasting methods, with little recognition of the impact of generation on the direction of energy flow. This approach has worked for decades due to the small amounts of generation at LV, but needs to be revised to use modern, computer-based load flow analysis which take account of the changes occurring to our network. Such analysis requires more detailed data than that currently used.
58. Low Carbon Technologies are already changing the energy flows on the LV network and demand for electricity is expected to rise significantly. These changes are being influenced by Government policy.
59. In future, electricity demand will be more unpredictable. Some houses might be importing large amounts of power, whilst at the same time others may be exporting large amounts of power. Where the LV network becomes stressed and power flows become more complicated, more detailed analysis is required and, therefore, access to more granular and specific data is vital.
60. To manage future energy flows, substantial investment will be required in both new equipment and in the operational measures necessary to ensure that voltages and electrical currents are kept within the capability of equipment and strict, regulated limits. Better network investment decisions can be taken, if detailed analysis of electricity consumption patterns can be undertaken.
61. Voltages and currents across the network are dependent on the energy flows. If we do not know the energy flow at key parts of the network, we cannot perform a detailed study known as a 'load flow' analysis. This type of analysis enables constraints on the network to be identified and possible mitigations to be developed, ensuring that the network meets the needs of our customers and also avoids potential asset failures or unplanned system outages.

62. There is a loss of detail and future flexibility associated with aggregation of data at predefined points on our network, e.g. at the start of each low voltage feeder and each feeder section, means that some approximations and engineering judgement will need to be applied during the network design process. However, we recognise that aggregation at such defined points is likely to be more acceptable from a data privacy perspective, at least initially. In the future it may be easier to present evidence that retaining the flexibility to aggregate stored disaggregated data in different ways will deliver customer benefits. At that time, a revised DPP could be submitted to Ofgem.
63. Currently, predicting load and growth with traditional Electricity Consumption Data is based around consumption profiles and growth profiles that include a number of assumptions. These methods of predicting load and growth have proven to be sufficient for many years but the increased availability of half-hourly Electricity Consumption Data from smart meters will eventually make them obsolete.
64. As Low Carbon Technologies become more common, the availability of data to accurately assess the strains on the network will become more important. For example, exports from distributed generation may create stress on the network or may relieve stresses caused by high levels of demand. If local demand and additional generation are not properly assessed and any issues mitigated, then power flow and voltage issues could occur.

### 3. Provide assurance that any commercial use of the data by the DNO or third parties is excluded from these purposes, both before and after the data anonymisation

65. We have no interest in selling additional services to data subjects. We will only use disaggregated half-hourly Electricity Consumption Data to comply with our principal statutory duty to develop and maintain an efficient, co-ordinated and economical system of electricity distribution and will not use any disaggregated half-hourly Electricity Consumption Data or aggregated half-hourly Electricity Consumption Data for any commercial purpose.
66. We will only provide aggregated half-hourly Electricity Consumption Data to third parties, if we are required to do so by our licence. For example, standard licence condition 52.2(b)(ii) requires us to facilitate competition in the Local Connections Market through providing Input Services on an equivalent basis to all Connection Parties that operate in the Local Connections Market. An Input Service means any essential input required to enable another party to connect to the licensee's Distribution System, as further clarified in the Competition in Connections Code of Practice. We will deem aggregated half-hourly Electricity Consumption Data to be an essential input only if it is expressly required by an Independent Connections Provider ("ICP") to design a connection. We will apply the control processes described in Appendix B to the ICP in those circumstances. We will not provide disaggregated half-hourly Electricity Consumption Data to any third parties.

### 4. Explain clearly how, where, when and by whom collation, maintenance, use and deletion of the data would take place securely and cost-effectively

#### Collation

67. Disaggregated half-hourly Electricity Consumption Data will be obtained periodically from the DCC. The collection of the disaggregated half-hourly Electricity Consumption Data will be initiated via service requests to the DCC for all MPANs that are registered within Northern Powergrid's Distribution Services Area, with the exception of any MPANs where we have decided not to request that data, i.e. where a data subject's request is being investigated or has been implemented.
68. Disaggregated half-hourly Electricity Consumption Data will be aggregated prior to storage in the Gateway, which is secure and ISO27001:2013 certified. Permission to access the Gateway is restricted to authorised

users based on access controls, assigned role profiles and account credentials according to business use. Only authorised users undertaking specific tasks will be afforded access to aggregated half-hourly Electricity Consumption Data.

#### **Maintenance**

69. As the disaggregated half-hourly Electricity Consumption Data is obtained directly from the smart meter, via the DCC, maintenance of the disaggregated half-hourly Electricity Consumption Data itself should not be required.

#### **Use**

70. Access to aggregated half-hourly Electricity Consumption Data will only be permitted in order to support activities required to meet our principal statutory duty under the Electricity Act 1989 to develop and maintain an efficient, co-ordinated and economical system of electricity distribution. Illustrative use cases are included in Appendix B.

#### **Deletion**

71. Disaggregated half-hourly Electricity Consumption Data will be deleted automatically on completion of the aggregation process.
72. We will retain aggregated half-hourly Electricity Consumption Data for seven years from the date of aggregation, after which time the aggregated half-hourly Electricity Consumption Data will be deleted. Aggregated half-hourly Electricity Consumption Data extracts that have been provided to authorised users will also be deleted after seven years.
73. For more information, please see Storage Limitation and Appendix D.

## **5. Demonstrate that consideration has been given to the best available techniques for minimisation, aggregation, anonymisation and/or other treatment of data**

74. Our proposed anonymisation approach has been informed by the UK Anonymisation Network's publication "The Anonymisation Decision-Making Framework".
75. Our proposed approach is to use a combination of data masking and anonymisation of the disaggregated half-hourly Electricity Consumption Data by means of aggregation to distribution substation, feeder or feeder section level..

#### **Guidance from the UK Anonymisation Authority**

76. The content of the UK Anonymisation Authority's "The Anonymisation Decision-Making Framework" is primarily intended for those who have data that needs to be anonymised with confidence, usually in order to share it. The report recognises that:
77. Anonymisation is a process to produce safe data but it only makes sense if what you are producing is safe, useful data. Zero risk is not a realistic possibility if the data is to remain useful data. The measures put in place to manage risk should be proportionate to that risk and its likely impact; and
78. Anonymisation is a heavily context-dependent process which should not only consider the data itself, but also the environment in which that data is stored and used. Anonymisation concerns keeping data confidential. It is not primarily about privacy. In general, guaranteed anonymisation is not practical if the data is to remain useful data.

79. We will not store disaggregated half-hourly Electricity Consumption Data. We will anonymise disaggregated half-hourly Electricity Consumption Data by aggregation such that only aggregated half-hourly Electricity Consumption Data will be stored in our secure environment and made available to users in compliance with the aggregation policy.

#### Data Masking

80. We will carry out a process of “data masking” in relation to the disaggregated half-hourly Electricity Consumption Data that we collect. Data masking involves stripping out obvious personal identifiers such as names from a piece of information, to create a data set in which no personal identifiers are present.
81. The aggregated half-hourly Electricity Consumption Data held in our Gateway will be depersonalised. Any identifiers such as MPAN or premises address will be stripped from the aggregated half-hourly Electricity Consumption Data when it is stored.

#### Achieving Aggregation

82. We will hold information defining which MPANs are associated with each distribution substation, feeder and feeder section references in the Gateway to enable the aggregation process to take place. This information will be updated periodically. Historically aggregated data sets will be flagged to indicate where the MPANs associated with a given distribution substation, feeder and feeder section have altered, but these data sets will not be changed or removed.

Figures 1 and 2 below show the current number of premises or customer MPANs connected to a feeder for the entire customer base (3.83 million customers). 97.8% of our customers (3.74 million) are served by a feeder with more than five meters connected to it. This means that, in the vast majority of cases, we will be aggregating half-hourly Electricity Consumption data obtained in respect of at least five meters.

Premises per LV feeder	No of LV Feeders	% Total Number of LV feeders	Total Number of Premises	% Number of Premises
1	22,308	18.7	22308	0.58
2	10,029	8.4	20058	0.52
3	5,452	4.6	16356	0.43
4	3,590	3.0	14360	0.38
5	2,604	2.2	13020	0.34
>5	75,579	63.2	3742580	97.75
Total	119,562	100.0		

Figure 1 Premises per feeder

Premises per LV feeder	No of LV Feeders	% Total Number of LV feeders	Total Number of Premises	% Number of Premises
1	22,308	18.7	22308	0.58
2 or less	32,337	27.0	42366	1.11
3 or less	37,789	31.6	58722	1.53
4 or less	41,379	34.6	73082	1.91
5 or less	43,983	36.8	86102	2.25
>5	75,579	63.2	3742580	97.75
Total	119,562	100.0		

Figure 2 Premises per feeder (cumulative)

83. We recognise that there will be scenarios where the number of premises on a particular feeder is insufficient to enable half-hourly Electricity Consumption Data to be aggregated with any other data. Currently, only 0.58% of our feeders (totalling approximately 22,300 premises) have just one premises connected to the relevant feeder. In these circumstances we will reduce the risk of re-identification of individuals by additional anonymisation techniques, i.e. data masking. We will ensure that the data is stored against the feeder reference and not the individual MPAN.
84. We also recognise that there could be some scenarios where the number of premises on a particular feeder section is insufficient to enable half-hourly Electricity Consumption data to be aggregated with any other data. Although we have not yet been able to define feeder sections for all our 120,000 low voltage feeders, we propose to ensure that a feeder section has connections to at least five premises. This will ensure that a minimum of five half-hourly Electricity Consumption Data sets are aggregated per feeder section.
85. The content of “The Anonymisation Decision-Making Framework” makes it clear that aggregation is a low risk form of anonymisation.
86. Any anonymisation measures that are adopted need to be proportionate to the risk and impact of re-identification. There is a balance to be struck between the strength of the anonymisation and the utility of the anonymised data i.e. stronger anonymisation results in less useful data.
87. Taking into account the content of the UK Anonymisation Authority’s publication we consider that:
- i) Anonymisation by aggregation to create aggregated half-hourly Electricity Consumption Data before it is accessed by users is the most appropriate form of anonymisation for disaggregated half-hourly Electricity Consumption Data because it is accepted as being a strong anonymisation technique and will generally make it difficult to use the aggregated data to find anything out about an individual;
  - ii) The minimum aggregation level will be dependent on the number of customers connected to a feeder. In the vast majority of cases (97.5%) this will be a minimum of five. We will ensure that feeder sections contain a minimum of five customer connections. Aggregation will, therefore, result in aggregated half-hourly Electricity Consumption Data that is not capable of being associated with a Domestic Customer at Relevant Premises i.e. aggregation on this basis will mean that a living individual can no longer be identified from the aggregated half-hourly Electricity Consumption Data or from that data plus other information;
  - iii) We do not believe that a ‘motivated intruder’ would be able to reverse the aggregation to overcome this form of anonymisation; and
  - iv) Extraction of aggregated half-hourly Electricity Consumption Data from the secure environment will be automated and only undertaken by appropriated authorised users with a legitimate business requirement.
88. Given the security measures in place around the Gateway and the controls we will have in place, we believe that our aggregation approach will balance protecting the privacy of our customers with maximising the utility of the data by providing us with a flexible means of extracting value from the data.

## 6. Be accompanied by a Privacy Impact Assessment, consistent with the ICO’s code of practice

89. The original overall criteria for the assessment of Distribution Network Operators’ data privacy plans for access to household electricity smart metering data advised that DPPs must be accompanied by a Privacy Impact Assessment.
90. In May of 2018 when the GDPR and DPA 2018 were implemented the PIA was superseded by the Data Protection Impact Assessment (‘DPIA’). A completed DPIA is attached at Appendix F.

91. We believe that our ISO27001:2013-certified smart metering Information Security Management System, when coupled with aggregation and our strong data access controls, provides a control framework that is robust, privacy-focused and consistent with the approach of managing 'privacy by design'.

## 7. Demonstrate the conformity of the adopted IT security process to the ISO 27001:2013 and ISO 27005:2018 standards

92. The Gateway is the IT system we use to interact with the DCC's national infrastructure. The Gateway manages secure interactions with the DCC. It generates and submits service requests to the DCC, receives and processes responses to those requests and receives and processes alerts generated automatically by smart metering devices and the DCC.
93. Completion of the SEC's User Entry Process requires User Parties to confirm to the Smart Energy Code Administrator and Secretariat ('SECAS') that they have their SEC Security Assurance Status set as 'Approved'. This means that the User Party has complied with the SEC's security obligations for User Parties (SEC sections G3 to G6). These obligations include requirements for User Parties to:
94. Comply with the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes and its User Systems, known as ISO/IEC 27001:2013; and
95. Comply with the standard of the International Organisation for Standards in respect of information security risk management, known as ISO/IEC 27005:2018.
96. The SEC Security Assurance Status is set by the SEC Panel's Security Sub-Committee following a security assurance assessment undertaken by an independent security assurance provider, in this case, Deloitte.
97. We completed the SEC's User Entry Process in October 2017 and can, therefore, confirm that we have been independently assured as being compliant with both ISO27001:2013 and ISO27005:2018 with respect to the Gateway.
98. We subsequently completed an ISO27001:2013 certification programme that included the Gateway and can, therefore, confirm that we are ISO27001:2013 certified. Our ISO27001:2013 certificate and scope document are attached at Appendix G. We have now completed four SEC security assessments.
99. ISO27001:2013 covers the requirements for the establishment, implementation, maintenance and continual improvement of an Information Security Management System ('ISMS'). The adoption of our system was influenced by our needs and objectives, security requirements and organisational processes.
100. Our ISMS is designed to preserve the confidentiality, integrity and availability of information assets by applying a risk management process that gives confidence that risks are adequately managed.
101. Our ISMS requires us to follow a systematic approach to identifying and mitigating risks to confidentiality, integrity and availability of all smart metering assets. In this context 'assets' is a very wide definition and includes both the gateway and data stored and communicated through it, plus people accessing the smart metering system. I.e. the ISMS covers both the technical security controls covering the gateway itself and the organisation security controls covering the support team.
102. Technical security controls address items such as physical and environmental security; technical access controls including restriction of access to data; incident management; business continuity management; secret key management and anomaly detection.
103. Organisational security controls address items such as the screening of all users to BS7858:2019 or an equivalent; the procedures for managing access authorisation; the implementation of appropriate segregation of duties; security education, training and awareness; service provider compliance; and the maintenance of appropriate information classification arrangements.

104. The outputs from the risk management process include the selection and implementation of an appropriate set of risk treatments (i.e. controls and business processes) that allow us to manage the identified risks in a manner that complies with our overall corporate risk appetite.
105. These controls and risk treatments are both preventative and detective and have been designed to ensure that only trusted individuals, who have been subject to screening to BS7858:2019 or an equivalent, can access the Gateway.
106. Disaggregated half-hourly Electricity Consumption Data will not be stored in the Gateway. Consequently, re-association of aggregated half-hourly Electricity Consumption Data to a specific premises would not be possible.
107. We believe these arrangements meet the requirements because:
- To access the Gateway, unauthorised individuals would have to successfully breach all layers of a multi-layer security model;
  - A breach of the control environment would lead to serious disciplinary action being taken against those concerned; and
  - The detective controls we have in place would detect any such unauthorised activity and allow for preventative action to be taken.

## 8. Demonstrate that, in developing its privacy plan, the DNO has engaged constructively with relevant stakeholders

108. We have undertaken considerable engagement with a range of internal and external stakeholders throughout the process of preparing the DPIA and DPP, as follows:
- a. We have worked with other DNOs and the Energy Networks Association ('ENA'), our Stakeholder Panel and other industry parties;
  - b. We submitted additional evidence to the BEIS Data Access & Privacy Framework Review;
  - c. We sponsor a Public Interest Advisory Group; and
  - d. We have also commissioned our own study to establish customer attitudes to the use of aggregated half-hourly Electricity Consumption Data, acted on the feedback provided, added extra information to our Privacy Policy and taken on board concerns.
109. We have published an educational video on our website explaining the importance of accessing disaggregated half-hourly Electricity Consumption Data from smart meters. This video described the flexibility and the additional benefits associated with accessing and storing disaggregated data, which is not part of our current DPP. Supplementary material in respect of the above is provided at Appendix H.
- Ipsos MORI research study report (16 March 2017) – “Consumer attitudes to DNO access to Half Hourly Electricity Consumption Data”**
110. We supported qualitative research conducted in March 2017 by Ipsos Mori aimed at understanding customer views around access to disaggregated half-hourly Electricity Consumption Data from smart meters. A copy is attached at Appendix H.
111. Consumers generally fitted into four segments:
- a. Happy to share;
  - b. Depends whose asking;
  - c. Quid pro quo; and
  - d. Big brother.
112. However, the nature of the research meant that the proportions falling into each category was unknown.

**Northern Powergrid Stakeholder Panel**

113. At the panel's meeting on 28 June 2017, the members received a presentation on smart metering in the UK explaining how it had arisen and how it was expected to benefit consumers. Panel members were asked to consider the question of the DNOs having access to, and using, aggregated half-hourly Electricity Consumption Data. Panel members requested us to generate material to explain the benefits to the DNOs of having access to disaggregated half-hourly Electricity Consumption Data, which was prepared subsequently.
114. At the panel's meeting on 24 January 2018, the members received an updated presentation on smart metering in the UK with more details being provided regarding the development of the DPP. The panel was asked two questions:
- a. Is there anything we haven't explained well enough or you would like to know more about? and
  - b. Do you have any comments that will help us develop our DPP?

115. The panel acknowledged the complexity of the topic and the importance of educational material, although noting this was not necessarily a responsibility for Northern Powergrid.

**ENAs Generic Privacy Framework document "Safeguarding Electricity Consumption Data from Smart Meters"**

116. In addition, at various stages during the production of the Generic Privacy Framework document, regular reviews were held with Ofgem regarding the content of that document and the direction being taken. Our DPP is consistent with ENA's proposal.

**UK Anonymisation Network (UKAN)**

117. As part of the Generic Privacy Framework-related engagement and having spoken with the ENA, Ofgem asked the ICO for support regarding customer anonymity and how to deliver it. As a result, the ICO guided the DNOs to speak to the UK Anonymisation Network (UKAN).
118. ENA supported by Northern Powergrid consulted UKAN regarding the most appropriate way to anonymise disaggregated half-hourly Electricity Consumption Data whilst still being able to retain the maximum value from that data.

**Sustainability First**

119. Realising benefits from smart metering data whilst ensuring data privacy is the topic of a major multi-partner project currently being led jointly by Sustainability First and the Centre for Sustainable Energy.
120. The project involves a programme of research, analysis, stakeholder engagement and a process of dialogue with the Public Interest Advisory Group, the membership of which includes a wide mix of academics, companies, trade bodies, government, non-government organisations and consumer bodies.
121. The issues are complex and involve balancing valid privacy concerns with wider public interest considerations. We are part of the sponsoring group for this project and have been an active member of working groups.

**Impact Utilities study report (October 2018) - Customer attitudes to the sharing of smart metering data with DNOs**

122. We commissioned Impact Utilities to conduct consumer research within our licence areas, both quantitative and qualitative, which included customer panels and an online survey. The final report is provided at Appendix H.
123. The report's findings were that, following education, around 80% of customers are happy to share their data with us in some way, with around eight in ten of these customers being happy for us to have their smart meter data at individual household level. Just 12-13% of customers would prefer not to share their data with us, whilst the remaining 7-8% of customers are undecided.
124. Of 1,008 consumers surveyed, they responded as follows:
- a. Around six in ten (61%) were willing to share their individual household level data;
  - b. Almost two thirds (66%) were willing to share data either as an individual household, or when combined with a neighbour;



- c. Up to a further two in ten (22%), including a number who had previously indicated that they would not share data or weren't sure, would be willing to share data at a neighbourhood level; and
- d. The remaining 12% would prefer not to share their data at all.

125. Educational materials, including a video, have a positive impact on trust with a 32% of the survey group increasingly happy to share their disaggregated half-hourly Electricity Consumption Data after viewing the video. Sub-group differences in willingness to share data greatly even out once consumers have watched the video, with smart meter owners being statistically significantly more likely to be happy to share.

126. We have listened to concerns relating to storage and security and have drafted a revised version of our Privacy Policy for publication on our website. A copy is attached at Appendix F. We recognise the key role of explaining to customers the benefits of accessing disaggregated half-hourly Electricity Consumption Data and have added the educational video to the smart metering page on our website. A copy is attached at Appendix H.

## Appendix A: Glossary of Terms

Term	Definition
Aggregation	The process in which data relating to two or more meter points is gathered together and expressed in a summary form as a single data item
Anonymisation	The process of turning data into a form which does not identify individuals and where identification is not likely to take place
Data Protection Law	The Data Protection Act 2018 and the General Data Protection Regulation
DCC	Data Communications Company (also known as the 'Smart DCC') – the company that built Great Britain's smart metering data and communications infrastructure
Distribution Services Area	As defined in standard licence condition 1 of the electricity distribution licence
DNO	Distribution Network Operator
Domestic Customer	As defined in standard licence condition 1 of the electricity distribution licence
Domestic Premises	As defined in standard licence condition 1 of the electricity distribution licence
DPIA	Data Protection Impact Assessment - a process that assists an organisation systematically analyse, identify and minimise the data protection risks of a project or plan.
DSO – Distribution System Operator	An organisation responsible for securely operating and developing an active distribution system comprising networks, demand, generation and other flexible distributed energy resources
Electricity Consumption Data	As defined in standard licence condition 10A of the electricity distribution licence
EnergyIP	Northern Powergrid's Smart Metering Gateway system
Feeder	A low voltage circuit to which customers' premises are connected
Feeder Section	Part of a Feeder that has connections to five or more customers' premises
Information Security Management System	A set of policies, procedures, processes and systems that manage information security risks
Motivated Intruder	A person who starts without any prior knowledge and who wishes to identify an individual from personal data. The person is assumed to be reasonably competent but not assumed to have any specialist knowledge, have access to specialist equipment or will resort to criminality to gain access to data that is kept securely
MPAN	Meter Point Administration Number
Northern Powergrid	Northern Powergrid (Northeast) plc and Northern Powergrid (Yorkshire) plc

Term	Definition
Personal Data	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 identify of that natural person
PIA	Privacy Impact Assessment - a process which assists organisations in identifying and minimizing the privacy risks of new projects or policies
Relevant Premises	As defined in standard licence condition 10A of the electricity distribution licence
Schema	A structured framework or model for the organisation of data
SECAS	The organisation providing SEC administrative and secretarial activities
SEC Panel	The group that manages the SEC and ensures that the SEC is delivered in a way that is efficient, fair and does not discriminate between Parties or classes of Parties
SEC Security Assurance Status	The status of a User Party's smart metering security arrangements, as determined by the SEC Panel Security Sub-Committee, following a SEC security assessment; being either 'approved', 'approved, subject to', 'provisionally approved, subject to' or 'deferred, subject to'
Security Sub-Committee	The group established by the SEC Panel to oversee, review and provide advice on SEC security arrangements
Service Request	An electronic request for smart meter information made to the DCC from a User Party. The request will be made via a User Party's Smart Metering IT Gateway System
Smart Energy Code (SEC)	The multi-party industry agreement which defines the rights and obligations of energy suppliers, network operators and other relevant parties involved in the end-to-end management of smart metering in Great Britain
Smart Metering IT Gateway System	Software that supports electronic communication, in the form of Service Requests and automated Alarms and Alerts, between IT systems used by SEC User Parties and the DCC
The Anonymisation Decision-Making Framework	A book developed by the UK Anonymisation Network (UKAN) to address a need for a practical guide to anonymisation
UK Anonymisation Network (UKAN)	An organisation set up in 2012 as a means of establishing best practice in anonymisation; it offers practical advice and information to anyone who handles personal data and needs to share it
User Entry Process	The process which must be completed by a User Party in order to receive live DCC services
User Party	A person (i.e. corporate legal personality) that has agreed to be bound by the SEC and that has completed the User Entry Process

## Appendix B: Process Documentation

## Appendix C: Benefits Assessment



Smart Metering Programme - Benefits- Comparison of tradi



Benefits Assessment

## Appendix D: Data Retention

The ENA's Generic Privacy Framework proposed a retention period of 10 years for half-hourly Electricity Consumption Data, i.e. for an eight year price control period plus two additional years for network analysis and/or investment planning purposes.

It is our intention to store half-hourly power flow data, gathered by remote monitoring equipment (not smart metering data), on our high voltage system for a minimum of 5 years. This data will be accessible via a data historian system, called PI, with the expectation that data will be retained for longer if permitted by the size of the server. Once the server is full, half-hourly data will be archived. Archived data will still be accessible, although not as readily as data stored in PI. In the previous PI system half-hourly data was stored for 3 years before being archived; the business recognised in the specification for the new PI system the need to access half-hourly data for longer periods than before to facilitate investment planning.

Extracts of aggregated data requested will be subject to the Company's Policy on the Retention and Destruction of Records.

## Appendix E: Importance of access to consumption smart metering data



Additional Evidence -  
Data Access and Privi

## Appendix F: Privacy Documents - Data Privacy Statement & Data Privacy Impact Assessment

Additional words identified in black font.



Privacy Statement  
July 2020 v2.0.docx

## Appendix G: ISO27001:2013 Certificate & Scope Document



ISO27001  
Certificate.JPG

## Appendix H: Consumer Research and Stakeholder Consultation Activity

<http://www.northernpowergrid.com/smart-metering> or [Education Video](#)