

# National Energy Environment Data Specification

## C. Governance

July 2026

Version 001

This report has sponsored by the **Local Net Zero Hubs** and has been published by the **North West Net Zero Hub** supported with funding from the **Department of Energy Security and Net Zero**.

The report is provided for the purposes of knowledge transfer across the public sector. It aims to raise awareness of good practice approaches to delivering projects that support the net zero agenda. The **North West Net Zero Hub** is not liable for any decisions adopted by organisations based on the recommendations contained in this report.

Funded by:

Commissioned by:



Delivered by:



The logo for BURO HAPPOLD, featuring the text "BURO HAPPOLD" in a bold, black, sans-serif font, centered between two horizontal yellow lines.



## Contents

|                                                                                                               |    |
|---------------------------------------------------------------------------------------------------------------|----|
| Introduction.....                                                                                             | 5  |
| General data governance principles .....                                                                      | 6  |
| NEEDS data classification .....                                                                               | 7  |
| Governance considerations across steps 3 to 6 .....                                                           | 10 |
| Step 3: Data inputs.....                                                                                      | 10 |
| Step 4: Modelling requirements .....                                                                          | 13 |
| Step 5: Data outputs .....                                                                                    | 15 |
| Step 6. Reporting and dissemination.....                                                                      | 16 |
| The Future .....                                                                                              | 18 |
| Appendices .....                                                                                              | 19 |
| Appendix A - Further reading.....                                                                             | 19 |
| Appendix B – Example of key NEEDS data (smart meter, OS, EPC) access routes, legislation and regulation ..... | 20 |
| Appendix C - Summary of key legislation impacting the access and use of smart metering data: .....            | 22 |
| Appendix D – GDPR .....                                                                                       | 23 |

| Term          | Description                                                      |
|---------------|------------------------------------------------------------------|
| AI            | Artificial Intelligence                                          |
| CNZ           | Centre for Net Zero                                              |
| DCC           | Data Communications Company                                      |
| DESNZ         | Department for Energy Security and Net Zero                      |
| DPA           | Data Protection Act                                              |
| DPIA          | Data Protection Impact Assessments                               |
| DT            | Digital Twin                                                     |
| EPC           | Energy Performance Rating                                        |
| EV            | Electric Vehicle                                                 |
| GDPR          | General Data Protection Regulation                               |
| HH            | Half hourly                                                      |
| IP            | Intellectual Property                                            |
| ITT           | Invitation to Tender                                             |
| LA            | Local Authority                                                  |
| LAEP          | Local Area Energy Plan                                           |
| LBSM          | London Building Stock Model                                      |
| LSOA          | Lower layer Super Output Area                                    |
| ML            | Machine Learning                                                 |
| MHHS          | Market-Wide Half-Hourly Settlement                               |
| MPAN          | Meter Point Administration Number                                |
| NEEDS         | National Energy Environment Data Specification                   |
| OS            | Ordnance Survey                                                  |
| Personal data | Any data that can identify an individual, directly or indirectly |
| SMEDR         | Smart Meter Energy Data Repository                               |

## Introduction

Robust data governance is essential for the responsible, secure, and lawful use of data across the energy and environmental project lifecycle. It must be embedded from the outset and remain adaptable to evolving legal, technical, and regulatory requirements.

This guidance supports local authorities in applying governance best practice throughout the National Energy Environment Data Specification (NEEDS) – a national framework and toolkit that standardises how energy and environment data is specified, managed and shared to support local decarbonisation planning. It covers the following key stages: data inputs, modelling, outputs, and dissemination. It explains common data types (personal, commercial, licensed) and highlights key considerations including access, consent, ownership, output formats, and secure sharing.

Governance, in the context of energy and environmental planning, refers to the frameworks, policies, and practices that ensure the responsible, effective, and ethical use of data throughout the planning lifecycle. It encompasses how data is acquired, managed, shared, and applied to support decision-making, collaboration, and public accountability.

Robust data governance is an essential component of any project involving data analysis to ensure compliance with the relevant legislation and regulation and, in doing so, to maintain public trust. This includes managing requirements arising from personal data protection (e.g. GDPR), data licensing conditions, funding obligations, and audit and accounting requirements, all of which may place specific constraints on how data is accessed, used, shared and retained.

The sections that follow first outline general data governance principles that should be considered as part of data governance best practice, then walks through governance considerations for each stage of the NEEDS toolkit, namely:

- 1. Data inputs**
- 2. Modelling requirements**
- 3. Data outputs**
- 4. Reporting and dissemination**

At each stage, real world examples are highlighted using Energy Performance Certificate (EPC), Ordnance Survey (OS) and smart meter data. These have been selected due to their prevalence as a data input across a wide range of NEEDS applications. While smart meter data offers a useful example because of its high value, yet relatively complex data access and usage framework owing to its sensitive nature.

## General data governance principles

A review of Government and Local Authority (LA) data governance guidance (see Appendix A) highlights ten common, overarching best practice principles for LAs to consider when using and sharing data. These should be considered alongside the NEEDS 'commissioning decisions' guidance, which helps determine existing levels of data governance readiness and maturity:

1. **Data governance framework:** establish a comprehensive data governance framework that includes policies, procedures, and guidelines for data management (underpinning all subsequent principles). Regularly review and update to adapt to changing needs and regulations.
2. **Transparency and accountability:** ensure that data collection, storage, and usage processes are transparent. Clearly define roles and responsibilities for data management and establish accountability mechanisms.
3. **Data quality and integrity:** maintain high standards of data quality by ensuring accuracy, completeness, and reliability of data. Implement regular data validation and cleansing processes.
4. **Data security and privacy:** protect data assets from unauthorised access, breaches, and other security threats. Comply with data protection regulations such as General Data Protection Regulation (GDPR) and ensure that personal data is handled with the utmost care.
5. **Interoperability and standardisation:** use common data standards and formats to ensure interoperability between different systems and datasets. This facilitates data sharing and integration across departments and organisations.
6. **Data accessibility and usability:** make data easily accessible to authorised users while ensuring that it is presented in a user-friendly manner. Provide adequate training and support to staff to enhance data literacy.
7. **Ethical use of data:** ensure that data is used ethically and responsibly. Avoid any practices that could harm individuals or communities and ensure that data usage aligns with public interest.
8. **Stakeholder engagement:** engage with stakeholders, including citizens, businesses, and other public sector organisations, to understand their data needs and ensure that data governance practices meet their expectations.
9. **Data lifecycle management:** Implement effective data lifecycle management practices, including data creation, storage, usage, archiving, and disposal. Ensure that data is retained only for as long as necessary and disposed of securely.
10. **Continuous improvement:** Foster a culture of continuous improvement in data governance practices. Regularly assess and enhance data management processes to ensure they remain effective and efficient.

These principles are designed to help local authorities manage their data assets effectively, ensuring that data is used in a way that is secure, ethical, and beneficial to the public.

## NEEDS data classification

Open Energy has created a data classification system which categorises data into one of five classes based on its level of personal, commercial and security sensitivity. Here, personal sensitivity relates to privacy and consumer protection associated with ‘personal data’, as defined by the UK Data Protection Act (DPA) 2018. Personal data can be highly useful across a large number of projects that fall within the NEEDS framework. This ranges from actual consumption data at a property level from smart meter information to health data. This more detailed information allows far greater insight and as result more targeted and accurate outputs and actions. Whilst it is unlikely projects will report this information at individual household level it still requires handling and storage of GDPR sensitive data.

Commercial sensitivity considers intellectual property and commerciality, while security sensitivity relates to cybersecurity and critical national infrastructure (Icebreaker One) <sup>1</sup>. This provides a useful framework to categorise all NEEDS’ datasets. When selecting and integrating any dataset into a NEEDS project, applying this framework helps the user balance the value of any dataset against the friction associated with accessing and using it.

---

<sup>1</sup> [Icebreaker One Sensitivity Classes](#)

Table 1 sets out these primary data classification categories, providing examples of smart metering data and other commonly used NEEDS datasets. All datasets within NEEDS will fall into one of these categories, generating several upfront questions for the organisation to consider at the data input stage of a project (refer to NEEDS decision tree tool).

In some instances different kinds of data presented in Table 1 will be combined within projects. This presents risks about ensuring suitable levels of governance are considered. This is explored further in a later section (Step 4. Modelling requirements).

**TABLE 1 NEEDS DATA SENSITIVITY CATEGORISATION, ADAPTED FROM IB1'S DATA SENSITIVITY CLASSES TABLE (DATA SENSITIVITY CLASSES – ICEBREAKER ONE)**

| Data category |              | Description                                                                                                                                                                                                                                                                             | Smart meter data example                                                                                | Other examples                                                                                                                                                                                                                                                                                                                                                                                                                       | Sensitivity level (indicative) <sup>2</sup>    |
|---------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>Open</b>   |              | Full open access, under an open data licence. Free to use, by anyone, for any purpose.                                                                                                                                                                                                  | No of smart meters rolled out, aggregated smart meter half hourly (HH) consumption data (by DNO region) | Lower layer Super Output Area (LSOA) ID, Digest of UK Energy Statistics, Ordnance survey (OS) Open data, London Building Stock Model version 2 (LBSM2), , Open EPC data                                                                                                                                                                                                                                                              | Personal - L<br>Commercial - L<br>Security - L |
| <b>Shared</b> | Personal     | Datasets which <b>include personal data</b> , requiring appropriate consent to share, or other legal bases to data processing, as defined by the EU GDPR.                                                                                                                               | Smart meter consumption data (household, HH)                                                            | Some temperature preferences, protected characteristics or special category data (e.g. dependence on power due to health conditions), individual Electric Vehicle (EV) charging records, detailed EPC data                                                                                                                                                                                                                           | Personal - H<br>Commercial - M<br>Security - H |
| <b>Shared</b> | Via contract | Datasets which do not include personal data and which can/could be shared, but currently <b>require bilateral contract negotiation</b> . May include aggregated data about individuals, subject to best practice adherence (e.g. Information Commissioner's Office anonymisation code.) | Smart meter system data, daily smart meter installations                                                | Public EV charge-point performance, generation asset performance, aggregated microgeneration export profiles, 'Investment grade' data (e.g. suitable granularity for financial decision-making), sensitive asset data. Includes many third party procured datasets (Eg EPC derived. Cotality [previously Parity projects] operates a SaaS [Software-as-a-Service] model for its retrofit analytics platforms [Portfolio, Pathways]). | Personal - M<br>Commercial - M<br>Security - M |
| <b>Shared</b> | Restrictions | Datasets which can/could be shared, but which <b>require the user to agree to 'light touch' T&amp;Cs to access and use</b> (e.g. non-commercial clauses such as those under CC-BY-NC).                                                                                                  |                                                                                                         | OS National Geographic Database, Network capacity, outage data, weather predictions, European space agency data, geolocation information for non-sensitive assets (e.g. Renewable Assets, EPC certificates).                                                                                                                                                                                                                         | Personal - L<br>Commercial - M<br>Security - L |
| <b>Closed</b> |              | Limited to internal organisational access only or limited, bespoke bilateral contracts under specific circumstances. May be subject to hard legal barriers to sharing. May be security-critical information                                                                             |                                                                                                         | Business-critical proprietary information or Intellectual Property (IP), critical asset locations, classified information.                                                                                                                                                                                                                                                                                                           | Personal - H<br>Commercial - H<br>Security - H |

<sup>2</sup> L – Low, M – Medium, H – High

## Governance considerations across steps 3 to 6

In each of the sections below, best practice governance considerations are mapped against each stage of the NEEDS toolkit, with real world case examples highlighted in each.

### Step 3: Data inputs

#### Summary points to consider:

- Technical ease of accessing data (including timescale for getting access)
- Regulatory or legal barriers to accessing the data (e.g. consent requirements to access the data)
- Cost of data access / use
- Potential restrictions on use / risk of proprietary lock-in
- Constraints on data sharing, reuse and onward dissemination of outputs
- Data types and granularity

Selecting appropriate data inputs is a critical first step in any NEEDS project. Commissioners must consider not only the relevance of each dataset but also the practical, legal, and financial implications of accessing and using it. Importantly, input selection should also be informed by intended use cases and how outputs will be shared, reused, or integrated into future work, as this may affect whether open or restricted datasets are appropriate.

Accessing data can be straightforward or complex depending on where it comes from (some examples are provided in Appendix B). Some datasets such as synthetic or aggregated data are easy to access through open platforms, while others, such as household-level smart meter data, often involve more time-consuming steps like securing consent and integrating with secure systems. It is therefore important for LAs to plan and make sure data access timelines fit with their project schedules.

Regulatory and legal barriers must also be assessed particularly in relation to processing personal data. Personal data may require explicit consent, and its use is governed by frameworks such as the Information Commissioners Office (ICO) guidance<sup>3</sup>, UK GDPR and sector specific guidance such as the Data Access Privacy Framework (DAPF)<sup>4</sup> in relation to smart metering (Appendix C-E provide context on these issues around smart meter data and GDPR more generally)

A proportionate legal assessment should be conducted for each dataset to confirm the lawful basis for processing and whether a Data Protection Impact Assessment (DPIA) is required. Depending upon the scenario this may involve structured checks—such as confirming data ownership, licensing terms, consent requirements, and alignment with relevant guidance (e.g. UK GDPR and ICO guidance). Links with further detail on legal and regulatory requirements can be found at the ‘Further Reading’ section of this guidance (Appendix A). Relevant legal, licensing and governance considerations may also be documented within the project’s data catalogue to ensure transparency, consistency, and ease of reuse across future applications.

Cost of access is an equally important factor to be considered and incorporated into project budgets and procurement planning. Open data is generally free but may lack detail whilst commercial or proprietary datasets can involve licensing fees and usage restrictions.

---

<sup>3</sup> [Information Commissioners Office \(ICO\) guidance](#)

<sup>4</sup> [Data Access Privacy Framework \(DAPF\)](#)

This may also lead to lock-in to a particular dataset if commercial terms and conditions do not allow sufficient flexibility to process, re-use, or onward share specific datasets. Similarly, specific data sets such as smart meter data may incur onboarding and operational costs. Further detail regarding onboarding with the Data Communications Company (DCC) can be found [here](#)<sup>5</sup>.

When considering data granularity, whether in terms of location detail or time intervals, it is important to find the right balance. More detailed data can improve modelling accuracy, but it also brings greater privacy risks and more complex governance requirements. Commissioners should aim to use only as much detail as needed for each use case, and wherever possible, use aggregated or anonymised data to keep things simple and compliant.

It's essential that all of these considerations are understood and weighed up at the onset of a project. No matter what the data set is – be it personal data, system-level metadata, synthetic datasets, or third-party sources like EPC ratings or vulnerability indicators - each comes with its own rules and responsibilities, depending on how sensitive it is and what the intended use is.

### Case example: Smart meter data

The smart metering network transmits around **3 billion messages monthly**, with smart meter **consumption** and **system data** offering high value for local authorities' Net Zero planning and monitoring activities. Several data access routes exist, with the preferred route dependent on the scale, granularity and frequency of data required, as well as the LAs available resources. Today, accessing household level data requires **consumer consent** and compliance with the **Smart Energy Code (SEC)** and **Data Access and Privacy Framework (DAPF)**. Where suitable, **aggregated, anonymised, or pseudonymised data** may be used without individual consent and should be explored where household level data is not essential. Data access could be managed on an open or shared basis, subject to its characteristics, sensitivity classification and applicable governance controls. Several industry reviews are currently considering how aggregated datasets could be shared; relevant material is signposted in the Further Reading section below.

### Case example: Ordnance Survey (OS) data

Ordnance Survey (OS) data is a valuable asset for local authorities, offering high-quality geospatial information to support effective planning and service delivery. Through the **Public Sector Geospatial Agreement (PSGA)**, authorities can access both OS OpenData and Premium datasets via the **OS Data Hub**, without incurring additional licensing costs. Data can be shared with other PSGA members and contracted third parties, provided the use directly supports public service functions. However, onward sharing for unrelated or commercial purposes is not permitted. To ensure compliance, local authorities must follow OS licensing terms, establish **Data Sharing Agreements (DSAs)** with third parties, maintain clear audit trails, and adhere to **UK GDPR** where personal data is involved.

---

<sup>5</sup> [Partnering with the DCC](#)

## Case example: Energy Performance Certificate (EPC) data

Energy Performance Certificate (EPC) data is publicly available in anonymised form for research purposes, but detailed records are restricted under UK GDPR and the **Energy Performance of Buildings Regulations**. Full certificate details, including property address, can only be accessed by the property's **owner, landlord, or occupier**, an **accredited energy assessor**, or a **third party with explicit consent**. Local authorities must ensure compliance with these regulations when requesting or sharing EPC data.

## Step 4: Modelling requirements

### Summary points to consider:

- Consent and data protection requirements associated with processing and sharing data (for what purposes is the data being used and how must it be stored)
- Project delivery partner (e.g. Local Area Energy Plan [LAEP] practitioner) adherence to data governance best practice (are the necessary systems and processes in place)
- Maintaining compliance when combining datasets

Modelling is the critical bridge between data inputs and outputs in LAEPs and other environmental data planning. It is where data is processed, interpreted, and transformed into actionable insights. However, this stage also presents heightened risks and responsibilities, particularly when personal data is involved. Organisations must ensure that both their internal teams and any commissioned practitioners adhere to robust data governance standards throughout the modelling process.

### Key consideration for organisations

There is a risk that workshops or other stakeholder engagement activities could inadvertently lead to the disclosure of personal data (e.g. household-level energy use, vulnerability indicators). To prevent this kind of data breach it is recommended to avoid displaying raw personal data in public forums and use aggregated or anonymised data wherever possible. All materials used or produced (e.g. slide decks, reports, images) should clearly state data sources, attribution requirements, and any restrictions on sharing or reuse to ensure compliance with licensing, legal, and governance obligations.

Organisations must also ensure that any practitioner or delivery partner has the necessary readiness measures in place, including secure systems for data storage and processing, documented procedures for handling personal data, and staff trained in data protection and ethical use. The following is a best practice checklist for data procurement:

- Compliance with UK GDPR and Data Protection Act 2018<sup>6</sup>
- Alignment with ISO/IEC 27001 (Information Security Management)<sup>7</sup>
- Use of DPIAs
- Secure data transfer protocols (e.g. encrypted channels) Clear data retention and deletion policies.

A further risk to be aware of comes from combining different data sets as these can transform non-personal data into personal data, especially when identifiers (e.g. postcode, MPAN) are added. For example, energy consumption data may be non-personal in isolation, but when linked with housing stock or vulnerability data, it may become identifiable. To mitigate this risk, it is advised that organisations conduct DPIAs (whether as a best practice or mandatory activity under GDPR) when merging datasets, avoid unnecessary linkage of identifiers and use pseudonymisation techniques where linkage is essential.

Data storage, as well as how it is imported and exported should also be carefully considered. When storing data organisations must use secure, access-controlled environments and any cloud-based solution must comply with UK data residency and security standards. For importing or exporting the data formats should be interoperable with the metadata preserved.

---

<sup>6</sup> <https://www.gov.uk/data-protection>

<sup>7</sup> <https://www.iso.org/standard/27001>

## Case example: Smart meter data

Combining datasets during modelling is common practice, but it introduces **identifiability risks** under **UK GDPR**. For example, when modelling to identify households at risk of fuel poverty, integrating smart meter, property, and vulnerability datasets can turn previously non-personal data into personal data. Smart meter data aggregated at substation level may be considered “open,” but when linked to address-level EPC and council records, individuals or households can be identified or inferred. Even if each dataset appears anonymised on its own, combining them can lead to **re-identification**.

## Step 5: Data outputs

### Summary points to consider:

- Project output requirements (what must the project outputs be able to show)
- Clarifying ownership and use
- What format (e.g. granularity) do stakeholders need the data outputs, and what if any governance needs considering as part of this?

Once data has been processed and modelled, the resulting outputs must be carefully managed to ensure they are usable, appropriately formatted, and governed in line with legal and ethical standards. To provide an illustrative example, this stage focuses on how data is used within the project to produce a LAEP, distinct from how it may be shared or maintained after the project concludes (covered in Step 6).

Data outputs should be structured in a way that supports clear interpretation, decision-making, and integration into the LAEP or any other environmental plan. This includes ensuring outputs are aligned with the original project objectives, data is presented in formats that are accessible to both technical and non-technical stakeholders, and metadata is comprehensive, standardised and clearly linked to project outputs.

Best practice would include the development of supporting artefacts such as a data catalogue (listing datasets, sources, licensing conditions and update cycles) and data dictionaries (defining fields, units, assumptions and methodologies), with clear referencing between these and the project outputs.

For example, a data catalogue entry might specify a building stock dataset, its source, spatial resolution, licensing constraints and refresh frequency, while the corresponding data dictionary would define each attribute (e.g. EPC rating, heat demand estimate), calculation methods and any assumptions applied.

It is also important to clarify ownership and use as during the project, data outputs are typically managed by the delivery partner or practitioner. However, once the LAEP or environmental plan is complete, ownership of the outputs—including any derived datasets—transfers to the organisation. The commissioner should therefore plan for how outputs will be stored and maintained post-project, what rights and responsibilities they hold over future use and sharing, and whether any licensing or consent conditions apply to continued use (see stage 6).

The format and level of detail in data outputs should be tailored to the different stakeholder. For example, strategic stakeholders may require high-level summaries and visualisations, delivery partners may need more granular data to support implementation planning, and community engagement may benefit from simplified anonymised insights.

### Case example:

At the outset of an LAEP project, organisations should ensure the commissioning process considers the full range of stakeholders—including internal teams, delivery partners, data providers, and community representatives. Early engagement is essential to **define expected outputs, formats, and related data governance considerations covering licensing, consent, privacy, and compliance with UK GDPR. Clear definition at the commissioning stage** (and reflected in the Invitation to Tender [ITT] where feasible) helps ensure legal compliance, transparency, and effective project delivery.

## Step 6. Reporting and dissemination

### Summary points:

- Sharing project outputs (which project outputs be shared, to whom, and on what basis)
- Onward sharing wider project data (e.g. other valuable contextual datasets)
- Consider alternative analysis/dissemination approaches to minimise data governance risks (e.g. digital twins [DTs])
- Ensuring safe, secure and compliant storage, processing and dissemination of data post project (including if risk profile has changed depending on data processing / integration with other data sets).
- Applying anonymisation and pseudonymisation techniques when appropriate.

Once the LAEP or environmental plan is developed, organisations must consider what happens next with the data - whether it's raw figures, insights, or visualisations. That includes how data is stored, shared, and maintained, not just within the project team but also with commissioning bodies, delivery partners, and other stakeholders. Getting the governance right at this stage is key to making sure the data stays useful, secure, and compliant in the long run.

As stated previously, the level of granularity that can be shared depends upon whether data is personal (e.g. household-level energy use) or non-personal (e.g. aggregated or anonymised statistics). It is important to note that the purpose for sharing is also relevant as sharing for public engagement, policy development, or commercial innovation may require different levels of data sensitivity.

Consideration must also be given to ongoing data storage and security post project with data stored in secure environments with access controls and encryption. It is recommended that LAs conduct a post-project DPIA to reassess risks and mitigation strategies, including considering whether the risk profile has changed due to integration with other data sets, increased granularity, or expanded access or sharing.

When considering how to disseminate data, options such as digital twins and heatmaps can visualise insights without exposing raw data. Other techniques that remove the risk of revealing individual identities include anonymisation and pseudonymisation enabling broader data sharing, reducing legal and ethical risks, and supporting compliance with data minimisation and purpose limitation principles. Further information on these can be found at the following:

- **National Digital Twin Programme<sup>8</sup>**
- **ICO Guidance on Anonymisation and Pseudonymisation<sup>9</sup>**

Organisations should also have a firm plan for maintaining data governance beyond the project such as establishing a data stewardship model to manage ongoing access, licencing, updates, and compliance. This should also include defining retention periods to ensure secure deletion of personal data when no longer needed.

---

<sup>8</sup> [National Digital Twin Programme Guidance Collection – GOV.UK](#)

<sup>9</sup> [ICO Anonymisation and Pseudonymisation Guidance](#)

This stage of a project is when data is likely going to be handed over with greater onus on the public sector body rather than a contractor completing the work (who should have suitable procedures in place). Ensuring the 10 governance principles detailed are satisfied is a useful final cross check. Additionally the final three principles:

- Stakeholder engagement
- Data lifecycle management
- Continuous improvement

Are all likely key elements of the reporting and dissemination stage of a NEEDS project.

### Case example: Smart meter data

When considering how smart meter data can be shared and repurposed to unlock further value, it is important to consider licensing and consent alignment by reviewing Smart Energy Code (SEC) guidance and any Data Access and Privacy Framework (DAPF) conditions that govern onward use. This includes ensuring that any consent agreements match the intended use and audience of the shared data. For example, if data was collected for modelling purposes only, it cannot be repurposed for commercial use without updated consent. Organisations must carefully assess any new use of data beyond its original purpose, ensuring it **is lawful, clearly justified, and properly documented**, in line with UK GDPR and relevant data governance standards.

## The Future

A range of policy, regulatory, and technological drivers continue to reshape energy and environmental data use, with direct implications for the NEEDS framework and its governance. To remain effective, the framework and organisations use of it must remain flexible, with internal data policies under regular review. Key areas of development to monitor include:

- **Data access:** Efforts to simplify access to valuable data, including via Ofgem's Market-Wide Half-Hourly Settlement (MHHS) and Energy Data Best Practice (EDBP) programmes, and Department for Energy Security and Net Zero's (DESNZ's) Smart Meter Energy Data Repository (SMEDR) innovation programme
- **Data standardisation and licensing:** Work to improve interoperability and streamline licensing, including NESO's Data Sharing Infrastructure programme which seeks to establish a standardised approach for energy system data exchange
- **Data privacy and security:** Balancing open data access with consumer protection will remain critical, especially as new legislation (e.g. the Data Protection and Digital Information Bill) and a tool for centralised consumer consent emerges
- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML will further amplify the challenges and opportunities introduced in this guidance. The normalisation of predictive analytics, automated decision-making, and advanced data integration will present new risks, and require new governance arrangements to maintain trust, transparency and fairness in the use of data.

## Appendices

### Appendix A - Further reading

TABLE A1 FURTHER READING

| Category                                               | Subcategory                     | Links                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>i) Public sector data governance frameworks</b>     |                                 | <ul style="list-style-type: none"> <li>- <a href="#">Data Sharing Governance Framework - GOV.UK</a></li> <li>- <a href="#">Data Principles - Office for National Statistics</a></li> <li>- <a href="#">A guide to the data protection principles   ICO</a></li> <li>- <a href="#">Data governance   Local Government Association</a></li> <li>- <a href="#">Data protection impact assessments   ICO</a></li> <li>- <a href="#">The PSGA   Government and public sector   OS</a></li> </ul> |
| <b>ii) Industry initiatives</b>                        | Data access                     | <ul style="list-style-type: none"> <li>- <a href="#">Digitalisation actions needed for Clean Power 2030 : Energy Sector Digitalisation Plan (NESO)</a></li> <li>- <a href="#">Market-wide Half-Hourly Settlement (MHHS) reform</a></li> <li>- <a href="#">Automatic Asset Registration Programme (AAR)</a></li> </ul>                                                                                                                                                                       |
|                                                        | Data standardisation & exchange | <ul style="list-style-type: none"> <li>- <a href="#">Digital spine feasibility study: exploring a data sharing infrastructure for the energy system</a></li> <li>- <a href="#">Energy Data Best Practice Guide expansion</a></li> </ul>                                                                                                                                                                                                                                                     |
|                                                        | Data privacy & security         | <ul style="list-style-type: none"> <li>- <a href="#">Centralised Consumer Consent solution</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>iii) Best practice guidance</b>                     |                                 | <ul style="list-style-type: none"> <li>- <a href="#">Ofgem Energy Data Best Practice</a></li> <li>- <a href="#">LAEP DataHub</a></li> <li>- <a href="#">ICO Data Protection Impact Assessments (DPIA)</a></li> </ul>                                                                                                                                                                                                                                                                        |
| <b>iv) Key legislation and regulatory developments</b> |                                 | <ul style="list-style-type: none"> <li>- <a href="#">General Data Protection Regulation (GDPR)</a></li> <li>- <a href="#">UK Data Protection Act (DPA)</a></li> </ul>                                                                                                                                                                                                                                                                                                                       |
| <b>v) Smart meter data</b>                             |                                 | <ul style="list-style-type: none"> <li>- <a href="#">Smart Meter Data Access and Privacy Framework (DAPF)</a></li> <li>- <a href="#">The Smart Energy Code (SEC)</a></li> <li>- <a href="#">Smart Meter Energy Data Repository (SMEDR)</a></li> </ul>                                                                                                                                                                                                                                       |

## Appendix B – Example of key NEEDS data (smart meter, OS, EPC) access routes, legislation and regulation

**TABLE B1 - CURRENT SMART METER DATA ACCESS ROUTES**

| Data type / source                                                                           | Description                                                                                                                                                                          | Data categories available                                                                                          | Spatial aggregation                                                  | Temporal aggregation                                                                                                                                                 | Access requirements                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Smart meter data – direct via DCC ‘Other User’ role</b>                                   | Direct Access via DCC’s ‘Other User’ role                                                                                                                                            | 25 SRVs/Half-hourly consumption for electricity and gas.<br>Export profile<br>Tariff profiles<br>Load control data | Household/ SME with explicit consent only                            | Up to 13 months half hourly data held on the meter<br>Export profile (up to 3 months historical data)<br>Sub 10 second power data available via pairing a CAD device | On-boarding to DCC and accession to the SEC. Requires completion of several steps including, administrative, security and data privacy assessments as well as technical integration to the system. The DCC is currently taking all steps (within the current licence and regulatory framework) to shorten this process, to ensure access via the DCC is as frictionless as possible                                                                                                                                               |
| <b>Smart meter data via the ‘Other User’ secondary market, or OU enabled tertiary market</b> |                                                                                                                                                                                      | 25 SRVs/Half-hourly consumption for electricity and gas.<br>Export profile<br>Tariff profiles<br>Load control data | Household/ SME with explicit consent only                            | Unknown – subject to OU data storage                                                                                                                                 | Bilateral agreements with the Other User, or an entity who have contracted with the Other user, who charge for smart meter access on a £/meter model. May provide access to processed SM data (e.g. aggregated) to bypass consumer consent considerations.                                                                                                                                                                                                                                                                        |
| <b>Smart meter data – aggregated via Distribution Network Operators (DNOs)</b>               |                                                                                                                                                                                      | Half-hourly consumption only<br>Voltage data<br>Alerts<br>Network data                                             | Aggregated to a minimum of 5 premises                                |                                                                                                                                                                      | Open data – portal registration only. Since Feb 2024, all distribution networks have been mandated by Ofgem to provide access to half-hourly consumption data in anonymised (aggregated) form. Each DNO has produced a privacy plan, approved by Ofgem, which articulates how data is anonymised.                                                                                                                                                                                                                                 |
| <b>Smart meter ‘system’ data via DCC</b>                                                     | System data sits outside the ‘message envelope’. Can provide insights related to fuel poverty, smart meter penetration, low carbon technology adoption and robustness of the network | Smart meter system data includes vending, meter tamper alerts, pre-pay top up and credit exhaustion                | Household/ SME with explicit consent only                            |                                                                                                                                                                      | Bi-lateral agreement with DCC. DCC must receive permission from Ofgem via a Permitted Purpose to carry out data sharing with approved organisations by Ofgem and the energy suppliers for a specific purpose (currently being done for fuel poverty initiatives). As energy suppliers are the data controllers, DCC must receive a Data Processing Agreement (DPA) from the energy suppliers to share this data. The organisations receiving the data must sign a Data Access Agreement (DAA) with DCC before receiving the data. |
| <b>Synthetic smart meter data via Centre for Net Zero (CNZ)</b>                              | Synthetic smart meter data provided by Centre for Net Zero.                                                                                                                          | Synthetic Half-hourly consumption data for electricity and gas                                                     | Household level with user-defined conditioning on various attributes |                                                                                                                                                                      | Open data – OpenSynth portal registration. The CNZ also provide a generative AI model trained on over 1.8 billion smart meter readings with access free to researchers, policymakers and DNOs.                                                                                                                                                                                                                                                                                                                                    |

|                                             |                                                                                                                                                                                                                                                                                                                       |                                                                               |                                                                                                      |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ordnance survey (OS)</b>                 | High-quality geospatial data about Great Britain's geography, addresses, and infrastructure. Provides LA insight across planning, infrastructure, and service delivery, especially when combined with address and street-level data.                                                                                  | OS Open Data<br>OS Premium                                                    | British National Grid Aggregation Build-Up Areas (BUAs)<br>Administrative and Statistical Boundaries |  | Under the Public Sector Geospatial Agreement (PSGA), authorities can access OS Open Data and Premium datasets via the OS Data Hub without additional licensing costs. Data sharing is permitted with PSGA members and contracted third parties where use directly supports public service functions; onward sharing for unrelated or commercial purposes is prohibited. In addition, the publication of "derived data" is permitted under specific conditions set out by Ordnance Survey, enabling certain outputs (e.g. aggregated or transformed datasets that do not expose licensed source data) to be shared more widely, subject to compliance with those guidelines. Authorities should refer to OS guidance on derived data to ensure that any such outputs meet the criteria for lawful publication. |
| <b>Energy Performance Certificate (EPC)</b> | An Energy Performance Certificate (EPC) provides a standardised assessment of a building's energy efficiency. EPCs can be used to target retrofit programmes, support fuel poverty initiatives, inform planning and policy for net zero strategies and coordinate funding applications with evidence-based targeting. | Property details<br>Energy Efficiency Ratings<br>Building Fabric and Services | Household level                                                                                      |  | Energy Performance Certificate (EPC) data is publicly available in anonymised form for research purposes, but detailed records are restricted under UK GDPR and the Energy Performance of Buildings Regulations. Full certificate details, including property address, can only be accessed by the property's owner, landlord, or occupier, an accredited energy assessor, or a third party with explicit consent. Local authorities must ensure compliance with these regulations when requesting or sharing EPC data.                                                                                                                                                                                                                                                                                       |

## Appendix C - Summary of key legislation impacting the access and use of smart metering data:

**TABLE C1 KEY LEGISLATION IMPACTING THE ACCESS AND USE OF SMART METERING DATA**

| Legislation                                              | Description                                                                                                                                                                            |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">UK GDPR and Data Protection Act 2018</a>     | Smart meter data is considered personal data if it can identify an individual, even indirectly. Consent is required for access to half-hourly data unless anonymised or aggregated.    |
| <a href="#">Data Access and Privacy Framework (DAPF)</a> | Developed to complement GDPR, the DAPF governs access to smart meter data by suppliers, network operators, and third parties. It defines mandatory, opt-out, and opt-in access levels. |
| <a href="#">Smart Energy Code (SEC)</a>                  | A multi-party agreement that governs technical and commercial arrangements for smart meter data access and device pairing.                                                             |
| <a href="#">Smart Meters Act 2018</a>                    | Provides the legal basis for the smart meter rollout and the operation of the Data and Communications Company (DCC), which manages secure data transmission.                           |
| <a href="#">Data Use and Access Act 2025</a>             | Introduces Smart Data Schemes and a new lawful basis for processing personal data.                                                                                                     |

**TABLE C2 AN ILLUSTRATIVE EXAMPLE OF HOW REGULATIONS AND DATA LEGISLATION IMPACT DATA ACCESS AND USAGE ACROSS A RANGE OF SMART METER DATA CATEGORIES.**

| Data type                                                                     | DPAF           | UK GDPR        | SEC     |
|-------------------------------------------------------------------------------|----------------|----------------|---------|
| Energy consumption data – half hourly household level energy consumption data | Applies        | Applies        | Applies |
| Other personal (non-consumption) energy data (e.g. MPAN, some system data)    | Does not apply | Applies        | Applies |
| Non-personal energy data (e.g. voltage, export, some system data)             | Does not apply | Does not apply | Applies |

## Appendix D – GDPR

General Data Protection Regulation ([GDPR](#)) - implemented through the UK Data Protection Act ([DPA](#)). Personal Data is defined as any data that can identify an individual, directly or indirectly (e.g. energy usage at household level).

**TABLE D1 KEY GDPR PRINCIPLES**

| Principle                                     | Description                                                                                                                                                            |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Lawfulness, fairness, and transparency</b> | Organisations must process personal data in accordance with the relevant legislation and regulation.                                                                   |
| <b>Purpose limitation</b>                     | Data should only be collected and used for clearly defined, legitimate purposes.                                                                                       |
| <b>Data minimisation</b>                      | Only the minimum necessary data should be collected and processed. Aggregated or anonymised data should be used where possible to reduce privacy risks.                |
| <b>Accuracy</b>                               | Organisations must ensure that personal data is accurate and up-to-date, especially when used for planning or policy decisions.                                        |
| <b>Storage limitation</b>                     | Personal data should not be kept longer than necessary. Organisations must define retention periods and ensure secure deletion.                                        |
| <b>Integrity and confidentiality</b>          | Data must be protected against unauthorised access, loss, or damage. This includes encryption, access controls, and secure data sharing protocols.                     |
| <b>Accountability</b>                         | Organisations must be able to demonstrate compliance with all data protection principles, including maintaining records of processing activities and conducting DPIAs. |

Under the UK GDPR, there are **six lawful bases** for accessing and processing personal data. Local authorities and their practitioners must identify and document which basis applies before using any personal data in environmental planning

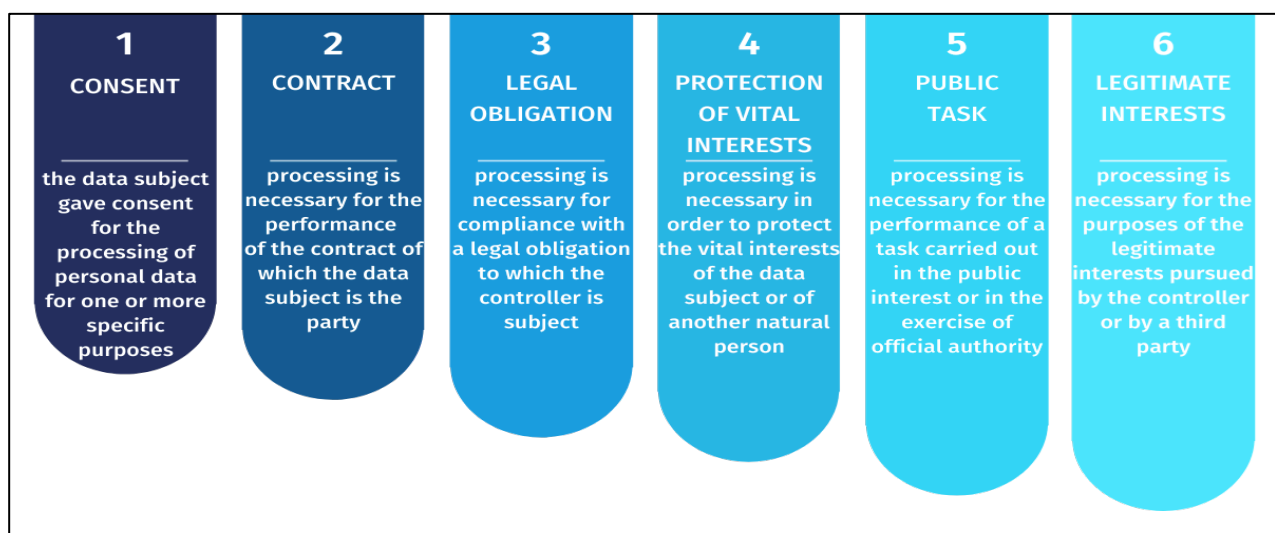


**FIGURE D1 GENERAL DATA PROTECTION REGULATION (GDPR) SETS OUT SIX LEGAL BASES OF DATA ACCESS**

## Appendix E – Smart meter data access and privacy framework

The [DAPF](#) is a regulatory framework designed to govern access to smart meter energy consumption data in a way that protects consumer privacy while enabling legitimate use by authorised parties.

### Purpose

- To complement UK GDPR and the Data Protection Act 2018.
- To ensure consumers retain control over who can access their energy consumption data, how often, and for what purposes.

**TABLE E1 ACCESS LEVELS DEFINED BY DAPF**

| Access Level | Name             | Description                                                                                                                                                                                                                      |
|--------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1            | Mandatory access | <ul style="list-style-type: none"><li>- Granted to energy suppliers and network operators for regulated purposes (e.g. billing, network management).</li><li>- Does not require consumer consent.</li></ul>                      |
| 2            | Opt-Out Access   | <ul style="list-style-type: none"><li>- Consumers are informed and given the option to opt out.</li><li>- Typically applies to daily consumption data for certain operational uses.</li></ul>                                    |
| 3            | Opt-In Access    | <ul style="list-style-type: none"><li>- Requires <b>explicit consumer consent</b>, especially for more granular data (e.g. half-hourly readings).</li><li>- Applies to third-party access and non-regulated use cases.</li></ul> |

### Key Restrictions

- **Legitimate Interest** is **not** a valid lawful basis under DAPF for accessing smart meter data.
- Consent must be **specific, informed, and freely given**.
- Data must be **aggregated and anonymised** for use without consent (e.g. by DNOs under Ofgem-approved privacy plans).

### Implications for Local Authorities

- Household-level smart meter data can only be accessed with explicit consent, whether directly or via a trusted intermediary.
- Aggregated or synthetic data should be used where possible to reduce compliance burdens.
- Any use of smart meter data must align with both DAPF and UK GDPR requirements.