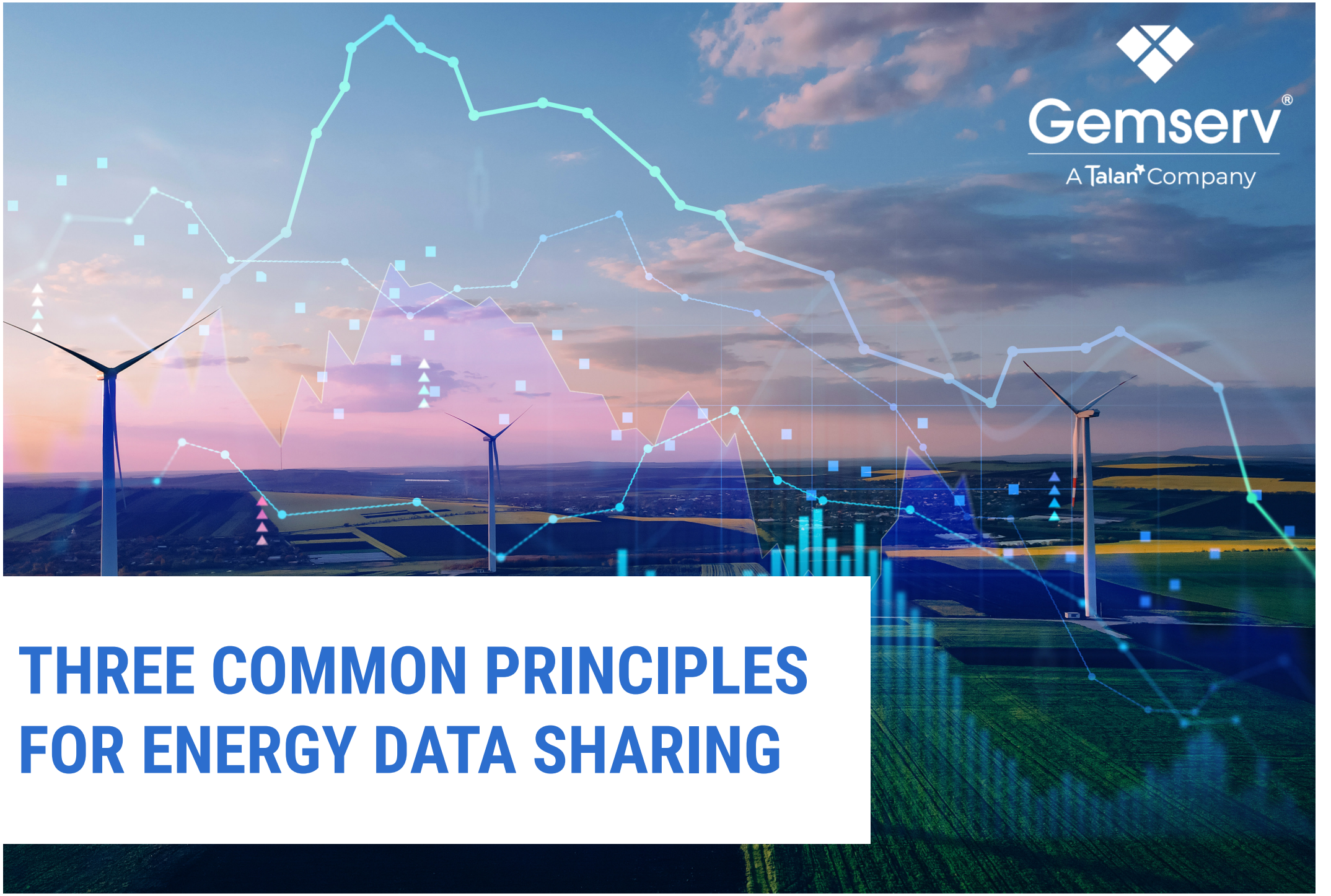


THREE COMMON PRINCIPLES FOR ENERGY DATA SHARING

CONTENTS

THE CHALLENGES PREVENTING ENERGY DATA SHARING 2

CHALLENGE 1: DIFFERENT APPROACHES ARE IN PLACE ACROSS ENERGY DATABASES 2

CHALLENGE 2: TERMS AND DEFINITIONS ARE NOT HARMONISED 3

CHALLENGE 3: DATA SHARING RULES CAN BE CONFUSING FOR INNOVATORS AND CONSUMERS 4

CHALLENGE 4: CLEAR AND TESTED PRACTICES FOR SHARING AGGREGATED DATA ARE NEEDED 5

OUR APPROACH: COMMON VS LOCAL RULES 6

GEMSERV'S PROPOSED COMMON PRINCIPLES FOR DATA SHARING 7

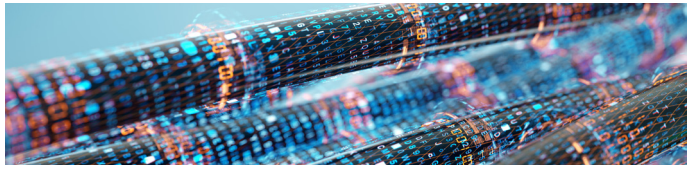
THE CHALLENGES PREVENTING ENERGY DATA SHARING

Data sharing is becoming ever more vital to driving both Net Zero goals and energy innovation. The energy industry has rich sources of data, including information about the performance of networks and grids, and data on the energy efficiency of premises. New systems and technologies like electric vehicles, heat pumps and internet of things (IoT) sensors are also being added to consumers' homes and the energy grid. To get the best value from this information, it needs to be open and accessible. Currently, data of different types is stored across a variety of systems, with rules for access and usage that are often confusing.

Gemserv notes that Ofgem is now consulting on a governance framework for its proposed Data Sharing Infrastructure (DSI). Ofgem plans to put into place a "decentralised" software package or solution to allow data sharing across systems. This will be supported by a 'trust framework' containing a "process of agreeing to rules for data sharing" to allow information held by the industry to be able to flow more freely. The project aims to allow willing parties in the energy industry to "exchange data in a standardised format" rather than storing data in a central database.

Gemserv recommends that a common set of principles are adopted to guide data sharing. We set out the ways in which lessons learned from existing practice in energy Codes and market arrangements can be made 'common' across the industry. Adopting these principles across industry should bring the trust and certainty needed for effective data sharing.

This position statement first sets out the current challenges with energy data sharing. These issues include a lack of consistent terminology or transparent rules that exist to access the various databases in the industry. It then outlines three 'common principles' for data sharing that we believe should be followed.



CHALLENGE 1: DIFFERENT APPROACHES ARE IN PLACE ACROSS ENERGY DATABASES

Great Britain's energy sector contains a wide span of databases that hold a variety of different information. For example, retail market data is held in systems such as the Electricity Enquiry Service (EES) managed by RECCo: electricity network data is collected from sensors around the grid and held by distribution network operators (DNOs); smart meter data, stored mainly in the memory of the meters, requires use of DCC systems and meeting Smart Energy Code (SEC) controls for access.

The different types of data on the systems, separate use cases, and technical architecture for its collection and storage have resulted in differing sets of access rules. For example, smart metering consumption data connected to specific domestic premises is considered to be personal data by the Department of Energy Security and Net Zero (formerly BEIS), within its Data Access and Privacy Framework (DAPF). As such, it is subject to requirements for consumer consent for data usage, under licence obligations and the Smart Energy Code. By contrast, operational network data held by DNOs, such as on grid outages or energy forecasting, is considered less sensitive, and Ofgem encourages it to be shared with other energy parties. This has led to DNOs providing portals on their websites to make this information publicly available.

The disparate types of data and systems held by the industry has led to different rules for access emerging. As a result, organisations wishing to use data insights to drive new services – such as those that want to identify the demand for renewable energy usage – have to work their way through this patchwork of rules to get access to the data they need. Principles of 'open' data sharing should be more consistently applied across systems, to allow information to flow to, and be used by, the 'innovators' best placed to make use of it.

To solve these issues, within its Data Best Practice guidance, Ofgem aims to make sure that data access can be made easier across the industry. For example, Ofgem states that system data held by energy licensees should be treated as "Presumed Open". This means that the data must be made available for all "to use, modify and distribute" without any restrictions. However, for data classed as having a "sensitivity", Ofgem requires the data owner to consider how to mitigate risks with, and limit, its sharing. This includes data types such as commercially confidential or personal data. Part of the challenge the industry faces is having a 'common' understanding of these terms. Organisations need to know what types of data should be 'Presumed Open' or 'Sensitive' – and thus what data sharing rules should apply.

CHALLENGE 2: TERMS AND DEFINITIONS ARE NOT HARMONISED

Open data sharing in the energy industry runs into hurdles when it touches on data that may be considered 'sensitive'. For example, the ICO considers that "consumption data linked to a particular Meter Point Administration Number (MPAN) is personal data when it relates to a domestic customer or a sole trader". However, Gemserv notes, on the basis of communications at industry committees and code manager events, that the industry remains divided on whether the MPAN itself would constitute personal data (as opposed to an identifier). For example, within a house of multiple occupancy (HMO), multiple meters may be connected to a single MPAN, and consumption data linked to an MPAN may represent multiple residents.

Determining whether data used by the energy industry can allow individuals to be identified, and constitute personal data, has implications for data sharing. For example, DESNZ's Data Access and Privacy Framework (DAPF) has strict controls for the usage of smart meter data at a 'personal' level. Consumer consent is needed for most uses of consumption data from their smart meter, although some exceptions exist for licenced activities. This hurdle may prevent suppliers and other energy parties from collecting or sharing smart meter data, for fear of doing so without a suitable legal basis in place. Research organisations such as the UCL Energy Institute have published a paper raising concerns with the onerous nature of obligations requiring them to collect consent from every consumer for innovation studies using smart meter data.

What is considered indicative of ''vulnerability', which helps licenced entities identify 'vulnerable' consumers at risk and provide them with priority services, also varies across the industry. For example, a 2020 Report from Citizen's Advice found that different utility suppliers have their own "specific definition of vulnerability" – ranging from data of the elderly age of consumers, to their physical or mental conditions – that can lead to them being treated differently by each organisation. Previously, Ofgem, Ofwat and the UK Regulators Network (UKRN) published a report calling for better data sharing of vulnerable customers details, across sectors, to

aid priority support. However, the lack of 'common' definitions can make it difficult for organisation to share and interpret information on vulnerable consumers, and lead to consumers who are vulnerable not being sufficiently identified and provided with the vital support they need.

Data termed 'commercially sensitive' or 'confidential' may also be seen in different ways by industry operators, based on their risk appetite. Organisations in the energy industry, such as Open Innovations and UK Power Networks, are concerned with the sharing of network data, for example, due to the risk that vulnerable points in grids could be made public. These weaknesses could then be used to target cyber attacks at critical network systems. To remedy this issue, Open Innovations argue for an energy 'Data Spectrum' to be used, that would classify different types of data (both personal and commercial) based on the sensitivity of such information. Under this approach, figures on electricity demand levels would be considered the least sensitive, and should be made freely able to any entity that requests it. On the other hand, sharing smart meter data specific to consumers' premises would need a specific contract with a named entity to access it. To bring greater trust and allow data to flow, we would like to see a similar series of common-sense rules that all data users are required to follow to access 'open' and 'sensitive' data.

CHALLENGE 3: DATA SHARING RULES CAN BE CONFUSING FOR INNOVATORS AND CONSUMERS

Industry bodies have also voiced their unease around the lack of clear or common governance rules for sharing data. This includes the Energy Systems Catapult (ESC) and Data Communications Company (DCC), who issued a paper in October 2023 titled 'Data For Good'. In the paper, they argued that many layers of licence obligations, legislation and other rules for data access act to limit new uses of smart meter data. In their view, requirements for consumer consent to access data also favour access by energy suppliers, who have a direct relationship with consumers. The authors outlined that better "personal data definitions" and a "more consistent, transparent approach" towards consumer consent will unlock more effective data flows. They also suggested a central body is needed to manage access to data and govern the various data access rules across the industry.

From the consumer's side, Citizens Advice also note in a recent position that consumers feel a "lack of control" with their inability to restrict uses of their data from their smart meters. In their report, Citizens Advice outline that consumers often do not know "who is accessing their data, when, and in what detail". This is due to the fact that smart meter data is often used by a web of organisations across the industry, beyond the data owner or supplier or consumer-facing party that has the consumer's consent. This lack of clarity impacts on consumer trust in the data sharing process. This may lead to a 'chilling effect', where consumers are put off using smart meters, or innovators avoid working with smart meter data, which may threaten the ability for the energy industry to achieve its Net Zero goals.

We believe that data sharing rules should be simple, fit for purpose and easy for consumers. A regime similar to Open Banking would allow customers to see, and easily share different types of energy data with each trusted third party. Ofgem, in its recent call for input paper on Consumer Consent, discusses that an 'Open Banking' structure and approach would allow consumers to "opt in or opt out" of sharing data with suppliers and "grant third party access". This 'common' model or set-up, if used by all code managers and data owners, would allow innovators to use consumers' data and give the power and oversight to consumers to allow this. We believe this model would permit existing industry databases to remain in place, but remove the need for a chain of complex rules and arrangements with organisations that wish to access data.

CHALLENGE 4: CLEAR AND TESTED PRACTICES FOR SHARING AGGREGATED DATA ARE NEEDED

Some concerns with sharing personal data could be solved by giving access to more data in an aggregated or anonymised form.

- Anonymised data, under the UK GDPR, is "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". This means that single consumers can no longer be identified by the data.

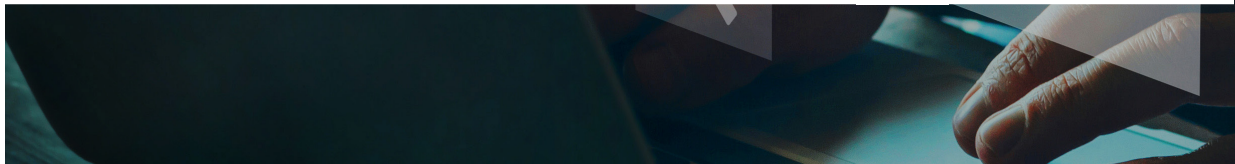
- Aggregated data is data from many premises, which is grouped together and expressed in a summary form. This means it can be used for statistical analysis.

The Information Commissioner's Office, in its recent guidance, notes that aggregated information (such as data at a postcode level) poses less of a privacy risk than data held at an individual-level (such as on a specific MPAN basis). This is because the ICO holds that the risk of being able to re-identify consumers with aggregated data is "relatively low". However, this depends on the sample size and level of detail of the data. The reality is that what data can be considered 'anonymous' or no longer personal is a moving target and should be viewed on a spectrum. Ofgem should thus take a role in providing guidance on what aggregation or anonymisation should be required for certain types of data sharing activities.

An example can be seen with consumption data held by Distribution Network Operators (DNOs). DNOs have access to aggregated consumption data, at a half-hourly level, which they use for licence purposes. These include analysing load profiles on the network, identifying demand and maintaining the efficiency of the electricity grid. They can also give access to such data for use by the wider industry. Ofgem, within its latest Data Best Practice guidance, outlines that system data which energy licensees hold should be treated as "Presumed Open". This also covers consumption data at an aggregated level.

Gemserv notes, however, that opinions differ between network operators and the public sector on what level of data is viewed as 'aggregated'. The National Grid, in its recent 2024 Smart Meter Data Privacy Plan, outlines that it would only consider consumption data to be no longer personal if it was grouped to a feeder station covering 5 or more MPANs. However, it notes that aggregation will only anonymise data for 99% of domestic consumers. A similar approach is taken by other DNOs such as Scottish and Southern Electricity Networks (SSEN), which claims to have tested this level of grouping to allow customer anonymity in different geographic areas, whilst still allowing the data to be useful to identify trends. By contrast, other DNOs such as Western Power Distribution have not committed to such a level, due to, in its opinion, the inability for such aggregation to completely anonymise its domestic consumers. The Office for National Statistics also uses a different standard, publishing information from DECC (now DESNZ) aggregated to postcodes with 6 or more meters.

It is not clear to Gemserv how these levels of aggregation were arrived at, or whether it needs to be further tested to see if individuals can be re-identified in specific circumstances. For example, how effective aggregating consumption data to the feeder station level is will vary between feeder stations in rural and urban locations. Even data aggregated to 5 or more MPANs may allow specific premises, or individuals, to be identified if energy usage readings are distorted by particularly large consumption from one premise. This could occur if a feeder station supplies a mansion belonging to a celebrity in a particular area, for example. To define suitable practices for sharing aggregated data, more research is needed into sufficient levels of aggregation, supported by regulatory guidance. This would provide more certainty to network operators that wish to share data at this level.

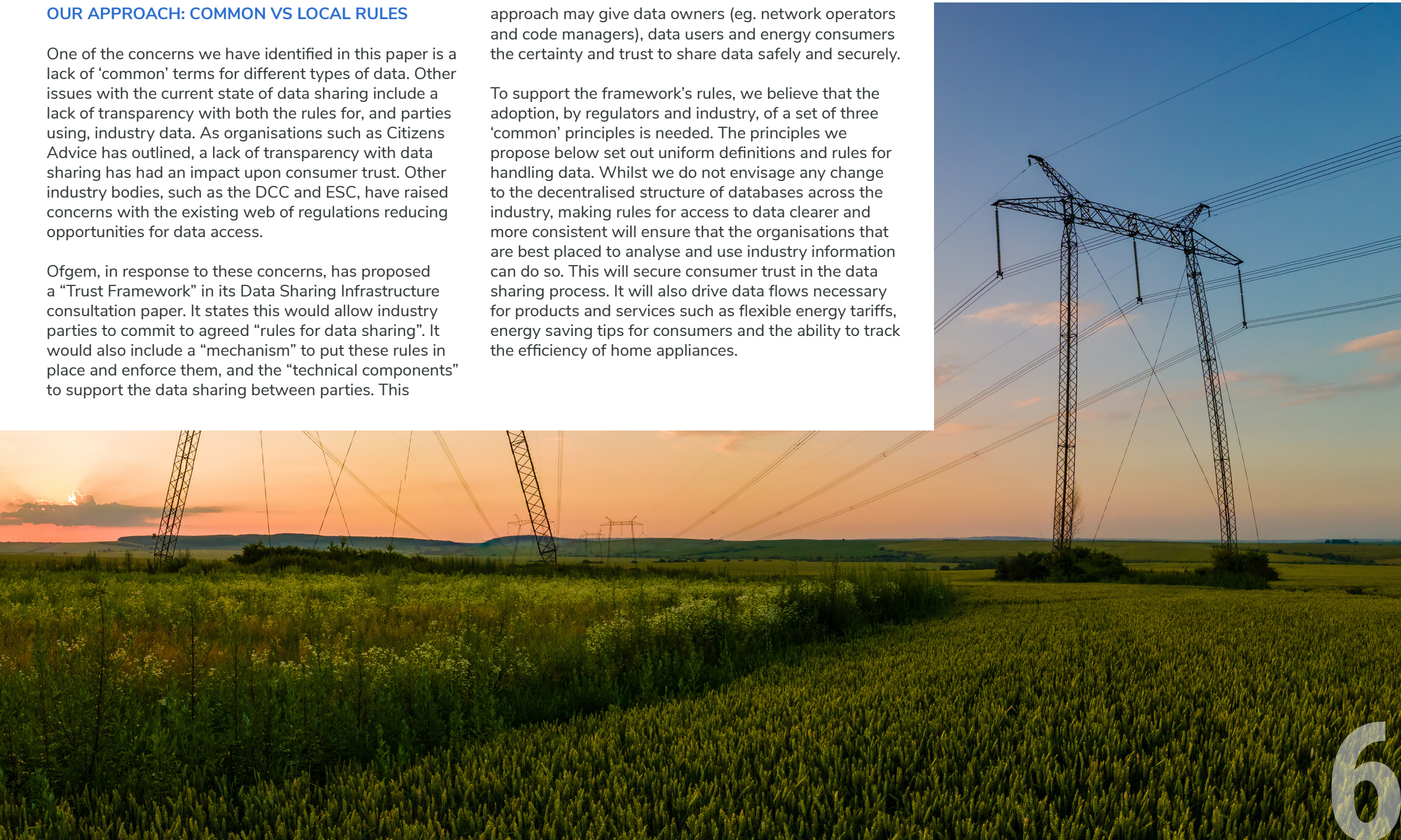


OUR APPROACH: COMMON VS LOCAL RULES

One of the concerns we have identified in this paper is a lack of 'common' terms for different types of data. Other issues with the current state of data sharing include a lack of transparency with both the rules for, and parties using, industry data. As organisations such as Citizens Advice has outlined, a lack of transparency with data sharing has had an impact upon consumer trust. Other industry bodies, such as the DCC and ESC, have raised concerns with the existing web of regulations reducing opportunities for data access.

Ofgem, in response to these concerns, has proposed a "Trust Framework" in its Data Sharing Infrastructure consultation paper. It states this would allow industry parties to commit to agreed "rules for data sharing". It would also include a "mechanism" to put these rules in place and enforce them, and the "technical components" to support the data sharing between parties. This approach may give data owners (eg. network operators and code managers), data users and energy consumers the certainty and trust to share data safely and securely.

To support the framework's rules, we believe that the adoption, by regulators and industry, of a set of three 'common' principles is needed. The principles we propose below set out uniform definitions and rules for handling data. Whilst we do not envisage any change to the decentralised structure of databases across the industry, making rules for access to data clearer and more consistent will ensure that the organisations that are best placed to analyse and use industry information can do so. This will secure consumer trust in the data sharing process. It will also drive data flows necessary for products and services such as flexible energy tariffs, energy saving tips for consumers and the ability to track the efficiency of home appliances.



GEMSERV'S PROPOSED COMMON PRINCIPLES FOR DATA SHARING

Gemserv believes that high level, common principles should be put in place by regulators for data sharing across the energy industry. They should be supported, as appropriate, by specific local principles used by code managers and data owners, that can be used on different data sets and that do not contradict these central rules.

Gemserv believes the following principles should be applied:

- **Common framework:** A common trust framework, as proposed in Ofgem's Data Sharing Infrastructure paper, should be further defined by regulators such as Ofgem. This framework should:
  - Set out principles for data access. This should cover the processes for new industry parties to get access to data. It should also outline the situations where the principles are expected to apply – such as for data sharing between suppliers and research organisations, or to database access provided by code managers.
  - Put the energy consumer at the centre of any data sharing. As with Open Banking, consumers should be able to tell the data owner who they want their data shared with, which data, and how long for. Data owners – such as code managers or network operators – should be required to provide a means for consumers to see, and control, how their data is being used.
  - Be supported by suitable enforcement tools for regulators, to ensure the framework's adoption. Whilst governance should not be centralised, ensuring the principles are followed by users wishing to access information will provide certainty to data owners. This is needed to allow investment in data sharing – both within and outside the energy industry.
- **Common catalogue:** Gemserv considers that information must be easy for users of the data to understand. This should be ensured by using a single, industry data catalogue, building on Ofgem's Data Best Practice guidance. This should:
  - Address terms such as 'personal data', 'commercially sensitive data' and 'aggregated data'. Definitions under laws such as under the UK GDPR and FOI Act should be used, to avoid any confusion of terms. A lack of clear terminology can lead data owners to shy away from data sharing, due to the risks of disclosing the wrong sort of information.
  - Provide guidance on sharing data of different types likely to be used by innovators. A spectrum should be used to identify what types of uses and controls should be allowed for data of varying 'sensitivity'. The guidance should also permit aggregated or anonymised data to be shared more easily, given the lower risks it presents. This could include guidance on what data can be considered 'aggregated' or 'anonymous'.

- **Common sense:** A trust framework should also be supported by suitable local rules for different energy systems. Based on the framework's principles, local rules should:
  - Reflect common sense applied in specific situations. Code managers and data owners should consider what use cases are relevant for the data they hold – and apply suitable rules for data access. On a case-by-case basis, they should be able to limit the sharing of certain personal data or other 'sensitive' data.
  - Require data sharing to be mapped out and data lineage described. Being able to see where data is going and how it is used allows suitable controls to be applied. Data owners should be required to map out the most critical data flows and make sure that backups of data, or other measures, can be used in case of a system crash or security incident.
  - Involve controls for safe access and handling of data from energy databases. This can include system-specific access controls, as needed in light of the sensitivity, scope or frequency of data to which access is being sought. Data owners should be able to apply suitable measures to reduce the risk of a data breach, or harm to individuals, depending on the profile of the data to which access is sought.


Gemserv®
A Talan Company
FIND OUT MORE
WWW.GEMSERV.COM