Access to data arrangements: evaluation

For the avoidance of doubt, these materials reflect the assessment undertaken by Baringa and are not intended to represent the views of GEMA

CLIENT: Ofgem

DATE: 4 June 2018

Version History

Version	Date	Description	Prepared by	Approved by
V1.0	29/03/18	Final Draft	Emma Burns Ysanne Hills Dan Golding	Duncan Sinclair
V2.0	04/06/18	Amendments for publication	Emma Burns	Ysanne Hills

Contact

Emma Burns (emma.burns@baringa.com)

Ysanne Hills (ysanne.hills@baringa.com)

Copyright

Confidentiality and Limitation Statement

Contents

Executive summary

Introduction

GEMA is considering whether to create a regulatory obligation to require the use of half-hourly (HH) interval data, available as the result of the smart meter rollout, for the purposes of electricity settlement. In conjunction with this, it is also considering changes to the existing settlement arrangements (and supporting institutions) to deliver market-wide half-hourly settlement (HHS) – the Target Operating Model. Baringa Partners has provided support to build the evidence base to feed into Ofgem's decision on access to data for settlement. This document provides a summary of the analysis conducted.

The existing regulatory arrangements

The Data Access Privacy Framework (DAPF) states that suppliers must obtain opt-in consent from their domestic customers to access smart metered HH consumption data. This currently includes data taken for the purposes of settlement in the electricity market.

Using consumers' HH consumption data in the calculation of suppliers' settlement positions would improve the efficiency of the market by moving away from the use of consumer profiles (the accuracy of which is diminishing over time), thus creating the incentives on suppliers to offer tariffs which more accurately reflect the costs of supplying energy at different times, and allowing customers to benefit from adjusting their consumption behaviours. By reducing peak consumption, the total generation and network capacity needed in GB could be reduced, thus reducing the cost of energy in GB as a whole.

GEMA's decision and GDPR

GEMA is considering whether to place a regulatory obligation on energy suppliers (or another appropriate party) to process their domestic and SME[1] customers' energy usage data on a HH basis for the purposes of settlement. We note that HH data is already used for larger SME and industrial customers.

As any data linked to Meter Point Administration Numbers (MPANs) and Meter Point Reference Numbers (MPRNs) are considered personal data[2], upcoming General Data Protection Regulation (GDPR) will reinforce consumers' rights to protect this data. GDPR regulations place greater emphasis on consumer control over their personal data.

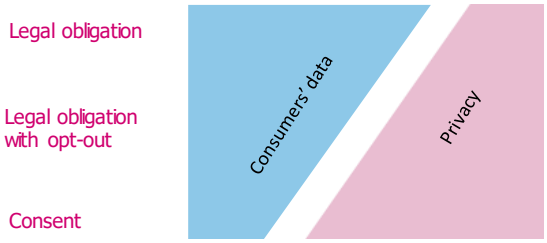
GEMA is therefore considering a number of options for access for processing consumers' HH data for settlement. These range from placing a legal obligation on suppliers (or another party) to collect all consumers' HH data for settlement, to allowing consumers to opt out of data processing for settlement, to retaining the status quo where consumers opt in to using HH data for settlement.

[1] Customers in Profile Classes 1-4, covered by the smart meter rollout.
[2] As per the ICO ruling in 2016.

The access to data arrangements will therefore have implications for the control that consumers have over their data and the proportion of consumers that are HH settled (Figure 1).

GEMA is also considering whether it should introduce additional enhanced privacy interventions to mitigate any concerns related to HH data to use in settlement for domestic and SME customers, and strengthen customer privacy. This is alongside another key policy decision about whether suppliers should have access to HH data for other purposes (e.g. forecasting).

Figure 1 - Access to data high-level trade-offs



Under GDPR, a core consideration will be whether GEMA has struck a fair and proportionate balance between the rights of individual consumers and the legitimate aim served by processing of personal data for the purpose of settlement. In general, the greater the number of stringent safeguards put in place to protect individuals from misuse of their data, the more likely it will be that the processing in question will be considered proportionate. However, there is a balance between cost and complexity, as well as security and privacy risks to consumers' data on the one hand, and the realisation of the potential benefits of smart meters on the other.

TOMs and the nature of settlement functions

Meanwhile, industry has developed a number of potential Target Operating Models (TOMs) showing how key electricity settlement processes (including data processing and data aggregation) could be redesigned for market-wide HHS. These consider different configurations of settlement activities, including centralising some or all of the roles.

In addition to a decision on the TOMs, GEMA will make a decision about the degree of centralisation of settlement functions.

Baringa's support

Baringa has been supporting Ofgem to develop its thinking about the potential application of enhanced privacy mechanisms (specifically anonymisation and pseudonymisation), for customers who may not have consented for their data to be used in HHS.

We have developed two strawmen for anonymising and pseudonymising HH consumption data for use in settlement.

On the basis of our assessment, and given the technical constraints, it appears that it would be necessary to centralise part of the settlement processes for all customers, or all settlement processes for some customers:

- To achieve effective **pseudonymisation** it would be sensible that the data retrieval processes were centralised, in order to achieve effective privacy protections; and
- To achieve effective **anonymisation**, all settlement arrangements would effectively be centralised for a subset of (non-participating) customers.

We also note that many of the privacy benefits of the anonymisation strawman could be achieved by full centralisation of settlement functions, so we do not consider additional enhanced privacy to add significant value if all settlement functions are centralised.

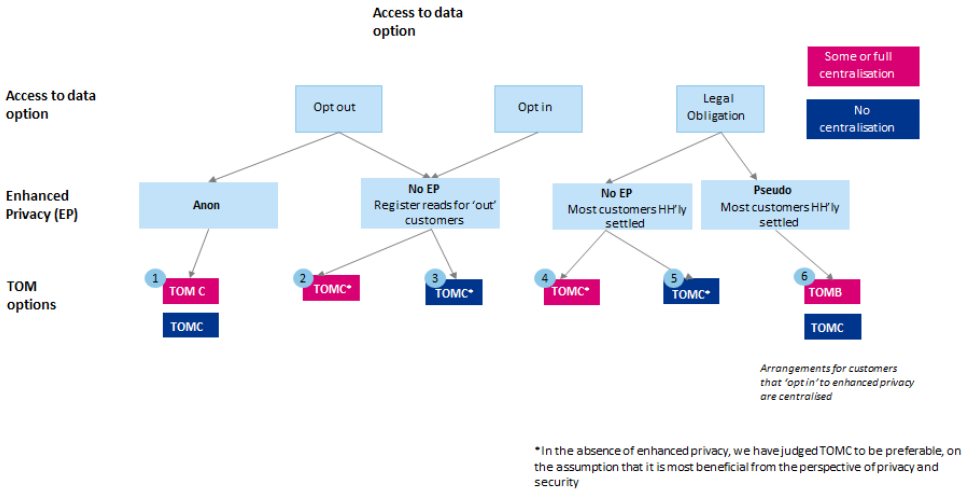
We assessed coherence of the enhanced privacy options with the access to data options, ruling out a number of the combined options. There were five feasible combined access to data and enhanced privacy options left following our assessment, these set out in the table below.

	Participating group	Non-participating group
Legal Obligation	No enhanced privacy	-
Legal Obligation	Pseudonymisation	-
Opt-out	No enhanced privacy	Anonymisation
Opt-out	No enhanced privacy	Settled on register reads
Opt-in	No enhanced privacy	Settled on register reads

We then considered the coherence of the TOMs and the enhanced privacy strawmen, concluding that:

- It would appear that TOM B[3] would be most suitable to achieve effective pseudonymisation, while allowing competition for the other settlement processes.
- It would appear that TOM C[4] (or TOM E[5]) would be most suitable to achieve anonymisation for non-participating (or opted out) customers, as there would be less difference in the approach taken for anonymised and non-anonymised customers.

On this basis, we present six possible options when considering the choice of TOM alongside the feasible access to data and enhanced privacy combinations, these are shown in the figure below.



Conclusion

[3] Combined Data Collection and Data Aggregation, but separate Data Retrieval
[4] End-to-end competitive services separated for smart metered and advanced metered customers
[5] End-to-end competitive services together for smart metered and advanced metered customers

In conclusion, we consider that the decision on whether to implement enhanced privacy (and if so the best type of enhanced privacy to implement) is nuanced, and finely balanced.

There are two high-level enhanced privacy strawmen that are potentially technically viable, and either (or both) of these could be further developed and assessed as part of the detailed design of the HHS arrangements for domestic and SME customers.

We note that the assessment of the relative merits of these two strawmen is highly dependent on the decisions that Ofgem is yet to make on the approach to data access, which TOM is selected and the degree of centralisation in the settlement functions.

In addition, if the approach to data access allows consumer choice on participation, namely the option to opt in or opt out, then the proportion of non-participating customers will be a key consideration, and should the number be at the lower end of the range, then the additional costs associated with enhanced privacy may be harder to justify.

If enhanced privacy is not taken forwards, and Register Reads (RRs) are to be used for non-participating customers, then it will be important to consider further how to ensure that demand profiles continue to be fit for purpose (such that they accurately reflect the expected consumption pattern of the group of customers that they are being used for).

1 Introduction and context

1.1 Introduction

Under current data privacy rules, suppliers must obtain opt-in consent from their domestic customers to access their HH data for any purpose (and allow microbusiness customers the right to opt-out of sharing their HH data).

GEMA is considering changes to the regulatory regime that could change the rules for processing data for settlement. This could mean that domestic consumers have their data processed on a:

- Legal Obligation (or 'mandatory') basis;
- Legal Obligation basis with the option to opt-out of data processing ("opt-out"); or
- Consent basis with opt in ("opt-in").

In parallel, industry have developed a number of Target Operating Models (TOMs) for HHS. Ofgem will consult on the access to data arrangements and the HHS arrangements this year.

1.2 Existing regulatory arrangements

The energy sector's Data Access Privacy Framework (DAPF) currently states that:

- Suppliers may access monthly (or less granular) energy consumption data, without customer consent, for billing and for the purposes of fulfilling narrowly-defined regulatory obligations;
- Suppliers may access daily (or less granular) energy consumption data for any purpose except marketing, providing they notify the customer and provide them with a clear opportunity to opt out;
- Suppliers may only access consumption data which is more granular than daily if they have secured the explicit consent of the consumer to do so (opt-in);
- There is no explicit differentiation between data for settlement and data for other purposes within the existing regulations;
- Network operators will be able to access domestic consumers' energy consumption data for regulated purposes, provided they have put in place procedures that have been approved by Ofgem to aggregate or otherwise treat the data such that it can no longer be associated with a single premises; and
- Third party Data Communications Company (DCC) users can only access consumption data with the explicit consent of the consumer.

The DAPF would need to be amended if more granular consumers' data is to be used in settlement.

Customers with existing smart meters are covered by the existing regime. If they change tariff or supplier after any changes are made to the DAPF, they will become subject to the new regulatory regime.

1.3 GDPR

The GDPR came into force in May 2018 placing greater emphasis on individuals' control of their personal data. As the June 2016 ruling of the Information Commissioner's Offer (ICO) on the Electricity Central Online Enquiry Service (ECOES) determined that where data is linked to domestic MPANs and MPRNs it is likely to be personal data, GDPR will cover the processing of HH data for settlement.

GDPR requires that firms only process data for its intended purpose and where a lawful basis for processing exists. Further processing is only acceptable when it relates to the original purpose or where the data controller has a suitable lawful basis to justify the additional processing.

Suppliers are covered by GDPR in their role as data controllers, and Supplier Agents in their role as data processors[6].

1.4 Access to data options

There are three high-level access-to-data options that are considered in scope of this evaluation:

- **Legal Obligation** – where all consumers' data would be processed for settlement.
  - This option maximises the HH data used in settlement (and hence the potential benefits of smart meters in increasing accuracy and simplifying processing), but gives consumers the least control over whether their data is processed for settlement.
- **Legal Obligation with an option to opt out of data processing ("Opt-out")** – where consumers would be presumed to consent to their data being processed for settlement unless they explicitly opt out.
  - This option gives consumers greater control over their data compared to a Legal Obligation without an opt out.
- **Consent ("Opt-in")** – where consumers would need to opt in to having their data processed for settlement.
  - This option would give customers the most control over whether their data is used in settlement (but is likely to reduce the use of HH data in settlement, and hence reduce the benefits associated with smart meters).

1.5 Enhanced Privacy

The ICO guidance terms anonymised data as that for which the risk of re-identification is 'remote' – whereas GDPR appears to have a more stringent definition of anonymisation. In line with GDPR, and for the purposes of this project, we define:

- **Anonymisation** as the irreversible processing of personal data in such a way that the data can no longer be attributed to a specific data subject
  - This means anonymous data is not considered personal data

[6] A data controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller (GDPR).

- Processing of personal data may be required in order to anonymise it

- **Pseudonymisation** as processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information
  - The "additional information" must be "kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person"

This means that pseudonymised data can still be classified as personal data: "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person" (GDPR recital 26).

This also means that there is an inherent tension between anonymisation of data and suppliers' visibility of the data being submitted to their energy accounts for settlement – as allowing suppliers' visibility of individual consumers' HH data for any reason would undermine those consumers' anonymity.

1.6 Target Operating Models

The Design Working Group (DWG) has developed skeleton Target Operating Models (TOMs) for HHS settlement. The TOMs reflect different market function configurations for each of the settlement processes.

The TOMs were developed by mapping all the services that cover the end-to-end settlement process. The key services relevant for our evaluation are:

- **Data retrieval (DR)** – accessing and retrieving energy usage data (import and export) from meters and associated technical details;
- **Data processing (DP)** – validating and estimating meter data, converting RRs to Settlement period (SP) data, providing data to relevant parties and exception reporting;
- **Data Aggregation (DA)** – responsible for receiving and aggregating Settlement Period data for use in settlement, network charging and other purposes (e.g. flexibility); and
- **Registration** – registrar for all Metering Systems (and other related registration information) in Supplier Volume Allocation (SVA); a service currently undertaken by the Licensed Distribution System Operators.

The TOMs reflect different groupings of each of the DR, DP and DA functions, and are designed agnostic of Ofgem's policy decision on centralisation of settlement functions.

In Section 2, we describe the possible enhanced privacy options available in this context (for HHS), and then in Section 3, we outline all possible access to data/enhanced privacy combinations and how we developed a short list of options with Ofgem.

2 Enhanced Privacy strawmen

2.1 Introduction

The consideration of enhanced privacy mechanisms would aim to shift the balance of GEMA's decision in favour of protecting the rights and freedoms of consumers with regards to the privacy and security of their personal data whilst retaining the maximum possible benefit of more granular data being used in settlement.

We have developed two enhanced privacy strawmen for the electricity settlement arrangements. These were workshopped with ELEXON and Ofgem:

- **Anonymisation** – through the creation of a new anonymisation function; and
- **Pseudonymisation** – through the creation of a new pseudonymisation function.

In this section we outline our thinking in developing the strawmen, present an overview of key enhanced privacy processes and summarise key messages for the evaluation.

We also considered a number of potential enhanced privacy strawmen that were ultimately ruled out. These options are also described in further detail in this section, alongside the rationale for ruling them out.

In summary, it is noted that:

1. It is assumed that enhanced privacy would not affect uptake of HHS (consumers' willingness to opt in or not opt out), given that the question of using data purely for wholesale settlement purposes is a technically complicated one, which customers are relatively unlikely to engage with[7].
2. A degree of anonymisation can be achieved through separation (and centralisation) of settlement functions for a subset of customers, while pseudonymisation would require centralisation of data retrieval.
3. Anonymisation will reduce suppliers' visibility of the data that they are being settled against as effective anonymisation should preclude MPAN-level interrogation of the data by the suppliers.
4. Pseudonymisation could help facilitate competition in other settlement functions while providing an additional privacy safeguard.
5. We do not expect either of the technically feasible options that we have developed (as set out in section 2.4 and 2.4.1) to significantly impact data accuracy.

[7] We note that Ofgem is planning consumer focus groups to test this assumption.

2.2 Development of the Enhanced Privacy strawmen

In our initial workshop with Ofgem and ELEXON, we discussed a number of options for achieving anonymisation or pseudonymisation in the settlement arrangements, which are set out in Table 1. These were subsequently narrowed down to two options, which are set out in more detail in Section 2.4. Further detail on the options that were ruled out is provided below the table and in Section 2.3. 'At-the-meter' anonymisation was ruled out following discussions with Ofgem, ELEXON, DCC and BEIS

Table 1 - Overview of options considered

	Description	Notes
Options for anonymisation		
Option 1	Anonymisation 'at the meter' through the creation of new service requests, which would pull only anonymised data from the meter.	This option represented 'full' data anonymisation – i.e. where data is anonymised to the extent that it ceases to be personal data before it is processed in any way. We received informal representations from DCC and BEIS that suggested that it is not feasible to achieve the degree of anonymisation and confidentiality through anonymisation 'at the meter' so this option was ruled out of scope.
Option 2	New body registers as DCC User and provides data anonymising function	A new industry role (or organisation depending on the TOM) would be responsible for anonymising personal meter data. This option would mean that personal data needs to be processed in order to facilitate anonymisation.
Options for pseudonymisation		
Option 1	Existing unique IDs are replaced with a pseudonym	A new role (or organisation depending on the TOM) would be responsible for creating pseudonymised personal data. There are a number of options for how this could be done in practice (option 1b and 1c).
Option 1b	MPANs are pseudonymised and data aggregated, with disaggregation by exception	Variation on option 1, with additional aggregation. It was felt this was a design variant on option 1, rather than a separate option, so only option 1 was taken forward.
Option 1c	MPANs are pseudonymised, and half-hours within a settlement day are scrambled	Variation on option 1, with additional aggregation. It was felt this was a design variant on option 1, rather than a separate option, so only option 1 was taken forward.

on the basis that it is not feasible[8]. Specifically, BEIS and DCC raised concerns that removing unique identifiers from smart meter data could undermine the integrity of the arrangements. DCC suggested that the arrangements are designed so that "only genuine commands can be sent" and removing unique identifiers would cause the data to be "immediately disposed of".

[8] While technically feasible, it could compromise security provisions

The pseudonymisation options were progressed as one option, as the options considered were not thought to affect the overall strawmen or assessment, but rather were variants that could be considered during the detailed design of the arrangements.

2.3 Data processing and data quality

It was recognised that both technically feasible enhanced privacy options involve processing of personal data. The only settlement option for customers that does not involve some form of increased data processing is to be settled on RRs using demand profiles (i.e. using the data that is already available to suppliers for regulated purposes when a customer opts out of sharing their data).

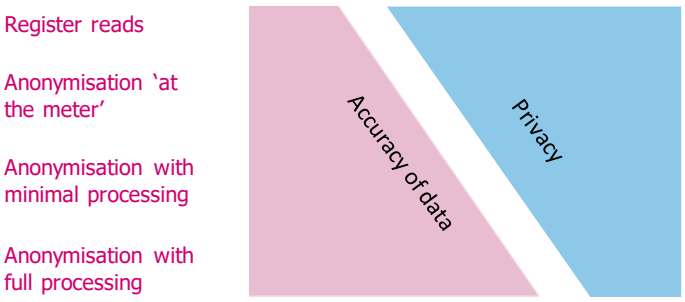
It appears that settlement functions would not be adversely affected by pseudonymisation, as existing validation processes should be unaffected – pseudonymised identifiers could act in a similar way to MPANs in the current arrangements so should not impact on the ability for data to be validated under the existing settlement functions (see Section 2.4.2).

However, for anonymisation, how and when data is anonymised could affect the scope to validate the customer data, and therefore data quality. There is a spectrum of notional options on how much data is processed before anonymisation, with a broad trade-off between data accuracy and the extent to which personal data is being processed. The degree to which data is validated will affect how accurate the data used in settlement is.

We considered a range of options:

- **Anonymisation at the meter** – whereby service requests would pull HH data from meters without any Globally Unique Identifiers (GUIDs) so that personal data is never processed.
- **Anonymisation part way through data processing with minimal validation** – whereby HH data is retrieved by a data processor checked for completeness but not validated in any other way before being sent to another party for submission to settlement.

Figure 2 - Data validation and processing high-level trade-offs



- **Anonymisation part way through data processing with full validation and aggregation** – whereby HH data is retrieved by a data processor and subject to full data validation before being aggregated and sent to another party for settlement.
- **Anonymisation following complete data processing** – whereby HH data is retrieved by a data processor, subject to full data validation before being aggregated and submitted into settlement by the party processing the data (rather than being passed to another party to carry out this step).

These options differ depending on how much the data is validated, with anonymisation at the meter representing one extreme because (if technically feasible) the party receiving the anonymised service requests would not know:

- Which meters' data it had received (as this relies on having GUIDs attached to the data); or
- Any information that could be used to validate (or provide estimates for missing/incorrect) data.

However, anonymisation at the meter is not considered technically feasible. This is the only option that would allow anonymisation before data is processed. Therefore, all remaining options that we considered involved some level of data validation before anonymisation.

We considered the range of methods for data validation currently used, and whether these could be reduced (on the assumption that limiting the extent of data processing would be positive from a consumer privacy perspective).

Existing validation processes for the HHDC are set out in BSCP502. These activities include:

- Checking the MPANs expected were received;
- Checking Maximum Permissible Energy; and
- Checking data isn't corrupt.

In addition to data validation, the HHDC currently carries out data estimation where data is missing, corrupted or deemed invalid. Data estimation is carried out using actual historical data where possible.

One option discussed was whether a new anonymisation function would check only that it had received all the meters' data that it had expected before aggregating the data. However, this option was not considered workable, as removing validation activities would lead to lower data quality compared to existing settlement arrangements (i.e. using RRs and historic data to estimate). Further, these validation processes are not seen as particularly onerous, over and above the minimum possible processing for HHS in the first place. It was generally felt that any notional privacy benefit of lower levels of data validation is likely to be out-weighed by the cost of lower data quality, and therefore should not be considered.

The strawman that we set out in this document therefore assumes that the new function carries out all the data validation and data estimation processes that the HHDC currently carries out. We understand through discussions with ELEXON that this would avoid loss of data quality.

We note that there is an inherent tension between anonymisation and allowing suppliers visibility of data being submitted into settlement, as by definition anonymisation is irreversible; allowing suppliers to have sight of this data for any reason undermines consumers' anonymity. If anonymisation were to be taken forward, careful consideration would need to be given to whether and how anonymised settlement data could be queried, and the level of information that could be made available to suppliers (e.g. for forecasting).

2.4 Overview of processes

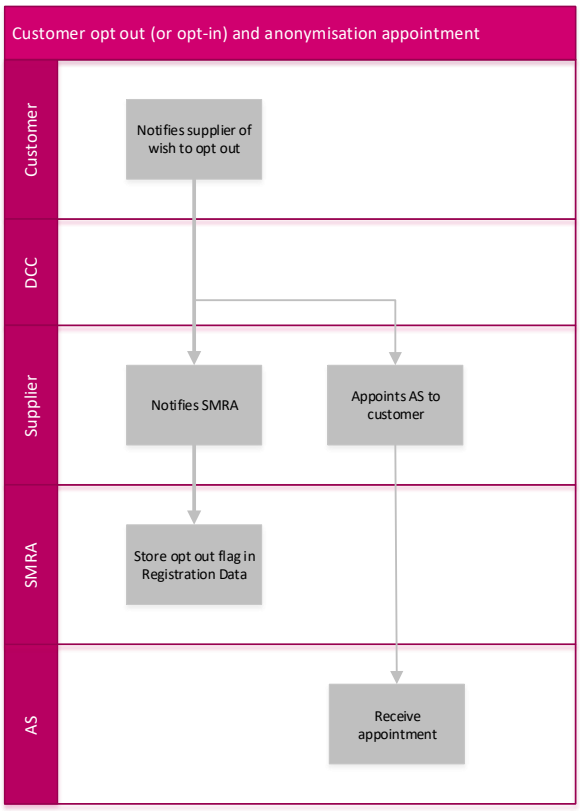
Given remaining uncertainty on which of the TOMs will be adopted, we describe these potential new functions as services – the anonymisation service (AS) and pseudonymisation service (PS) – rather than organisations. This approach allows either enhanced privacy strawman to be considered against each of the TOMs.

As we set out later in the document, we assume that anonymisation would only apply in instances where consumers have opted out of 'mainstream' HHS (or opted into an anonymisation service).

2.4.1 Anonymisation strawman – overview of processes

To facilitate the opt-out process[9], information about which customers opt-out would be held by the Supplier Meter Registration Agent (SMRA) as an 'opt out' flag in the SVA Metering System Registration Data. It is expected that the supplier (or other party depending on the regulatory arrangements) would receive the opt-out notification from the consumer and communicate this to the SMRA[10].

Figure 3 - Consumer opt in and anonymisation appointment



When a consumer opts out, responsibility for the processing of its data would pass from the competitive party responsible for data retrieval and/or processing to the party responsible for anonymisation. In effect, the AS would be appointed to opted-out MPANs as supplier agents are now – effectively similar to the Change of Agent (CoA) process set out in BSCP514.

Once appointed, the AS would have responsibility for retrieving the HH for 'opted out' customers. It would do this by submitting a service request to the DCC and receiving service responses for those customers' data. To facilitate this, it would likely need to be a new DCC User (noting this would require SEC changes) and have the appropriate security certificates that support smart meter encryption.

Before aggregation the data would be subject to the validation and estimated processes currently performed by the Data Collector role. It is expected that the data for these consumers would be processed in the same way that the data processor currently does. Therefore, the party responsible for anonymising the data would have access to all the customer registration data required to process the data.

The AS would submit the aggregated data to settlement on behalf of each supplier with opted out customers. We considered an option where the AS handed off the aggregated data to the supplier's agent responsible for data processing, but this was ruled out as it was seen as an unnecessary data transfer.

[9] This term is used as short-hand. It could be that it is more accurate to describe the activity as opting into the anonymisation service.

[10] For the avoidance of doubt, we refer here to registration in the BSC context to refer to functions carried out by the SMRA, noting that the definition of this term might change in future in light of the proposed new Retail Energy Code and changes to switching arrangements.

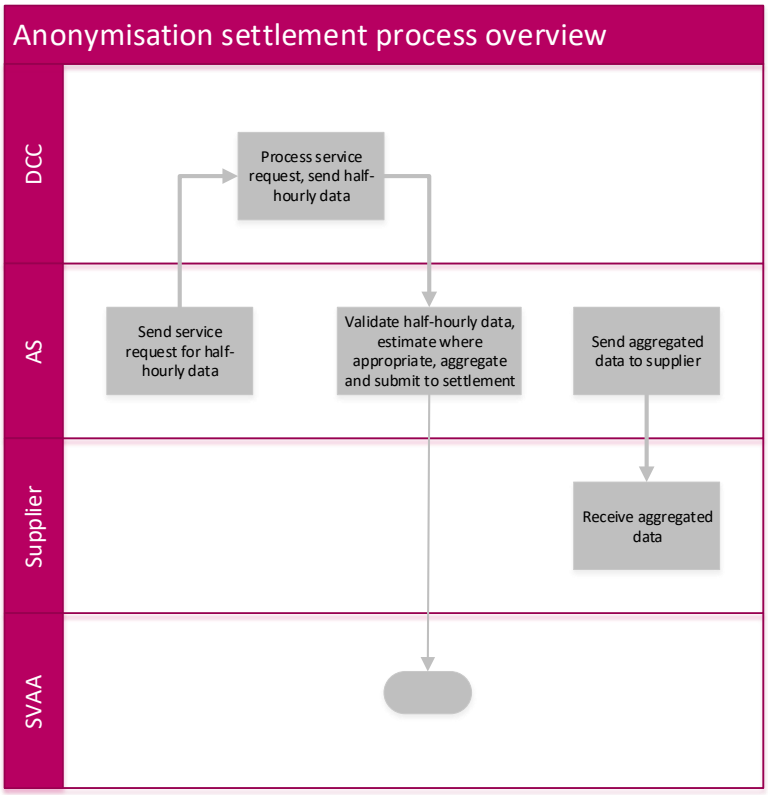
The AS would also send a report to the supplier (or other party as appropriate) with the aggregated consumer data for each GSP group area for forecasting/proposition pricing purposes. Further consideration will be needed to ascertain the most appropriate level of aggregation for this data.

Impact of centralisation of settlement functions

It is recognised that this model effectively represents centralisation of settlement functions for a (potentially significant) subset of customers, and this is a policy decision for Ofgem. We note that customers will need to be able to move fluidly between the two sets of arrangements (e.g. on Change of Tenancy or when they change their opt-out status).

Further, it is suggested that if all settlement functions, or data retrieval and data processing settlement functions were centralised in such a way that suppliers (or their agents) do not retrieve the HH data, it is assumed that there would not be an additional benefit of having separate settlement functions for opted out customers.

Figure 4 - Anonymisation settlement functions



The AS therefore appears appropriate where it is applied to a subset of customers only, and that this would occur to facilitate competition for other settlement functions.

If only data aggregation settlement functions are centralised it is anticipated that a stand-alone body would be still required.

Query process

Suppliers would likely have concerns if they are unable to dispute data being submitted on their behalf into settlement, especially for periods of high imbalance prices.

Consideration would need to be given for arrangements to allow suppliers to query anonymised settlement data. It is likely that the query window would need to relatively short to ensure that consumer data was not being held for longer than needed, but it would likely need to be long enough

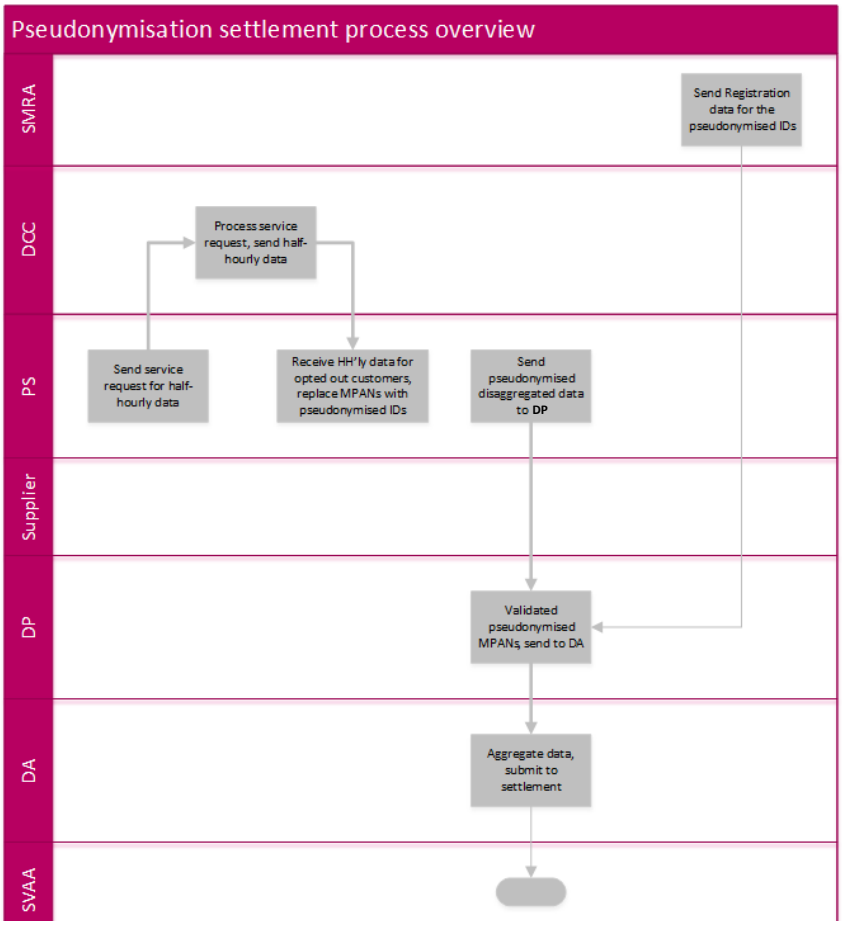
to allow suppliers to have sight of 30 day register reads. The effect of any errors could be smeared across all suppliers, as with the GSP Group correction factor now[11].

However, we note that there would be mechanisms in place to ensure that data is accurate – data validation and estimation processes, 30 day register reads to compare against – and it seems unlikely that the error arising from the anonymisation function would be greater than those that currently exist due to the use of demand profiles.

2.4.2 Pseudonymisation strawman – overview of processes

Under this model, an additional process would be introduced to replace consumers' Meter Point Administration Numbers (MPANs). These additional processes would be delivered by a new function, the PS[12].

Figure 5 - Pseudonymisation settlement overview



Pseudonymisation could be applied to all customer – or customers who opt into the service to provide enhanced privacy. When an additional opt in process was required, this would be similar to the process set out in 2.4.1.

The PS would request HH data via a service request to the DCC. HH data would be sent via the DCC to the PS, accompanied (as normal) by the unique device number, which is then be mapped to the correct MPAN. This function would be responsible for replacing consumers' MPANs with Pseudonymised IDs[13]. The PS would then pass this Pseudonymised data onto the data processor for processing.

[11] The GSP Group Correction factor is used to smear the effect of any errors that arise due to the use of profiles to allocate Non Half Hourly (NHH) metered volumes to a particular settlement period, as well as a number of other sources of data inaccuracy such as errors and theft.

[12] This service could be performed by one or multiple parties.

[13] We note that generating the pseudonymised MPANs could alternatively be the role of the SMRA.

Central to this option is a data map that would map MPANs to Pseudonymised IDs. This would need to be held by two parties – the PS and the Supplier Meter Registration Agent (SMRA). These parties would need to ensure that the data map is aligned and refreshed regularly (integrity and security of this dataset is therefore central to settlement).

It is not expected that the PS would need to carry out significant validation processes beyond checking it had received the data it expected. Where missing data are identified or suspected as a result of this process, a notification would be sent to the relevant supplier for investigation, and to data processor so that it the data can be estimated.

Once the PS had replaced the MPANs with pseudonymised IDs, it would provide the data to the party responsible for data processing.

The data processer would be appointed on the basis of pseudonymised IDs by the PS. It would have access to a limited sub set of Metering System Registration Data for the pseudonymised IDs, to allow it to complete its validation and aggregation activities. This party will receive the required MDD through the normal channels, as now but with pseudonymised IDs instead of MPANs.

Only the SMRA and the PS would have access to the full set of pseudonymised MPANs.

It is anticipated that pseudonymised IDs would be refreshed upon change of supplier. This may require daily updating of pseudonymised MPANs[14].

As for anonymisation, if this option were to be progressed, careful consideration would be needed as to the level of information that can be provided to suppliers (e.g. on Change of Supplier) for forecasting/proposition pricing purposes.

Design options ruled out

Another option that was under consideration was for the MPAN-Pseudonymisation role to remain relatively light and limited to storing the map MPANs and pseudonymised IDs. Under this option data retrieval would continue to be competitive, and it would be the role of the competitive DR to replace the MPAN with a pseudonymised ID. The pseudonymised data would then be sent to the competitive DA role, which would un-pseudonymise the data.

This option was ruled out on the basis that it would not deliver adequate privacy benefits compared to models where data retrieval and pseudonymisation are carried out as part of the same function.

2.5 Enhanced Privacy points for evaluation

Impact on data accuracy

We do not anticipate material errors to be associated with either technically feasible enhanced privacy option, as both would allow data validation. However, it is recognised that new processes and/or additional complexity could introduce some additional scope for error, compared to the status quo.

[14] We note that discussions at the DAB suggest that sub-daily supplier changes (e.g. to support P2P trading) may be necessary, if this is the case, then further consideration on when the ID is changed would be needed.

Effectiveness of privacy protection

Both enhanced privacy options risk not being effective in a number of circumstances, for example if:

- A supplier has a small number of customers in a particular GSP group;
- A supplier has taken on a new customer; or
- A supplier is alerted to a meter error.

Under anonymisation, this may occur because a supplier only has one or a small number of customers of a particular type on a particular GSP group, so aggregation is not effective.

Under pseudonymisation the risk is higher as the pseudonymised IDs would allow parties to identify individuals by cross-referencing with the fuller data set (i.e. it would potentially be able to determine an individual customer in practice by looking at start dates for supplier agents and other data). A possible mitigation against this would be to aggregate the pseudonymised data, and allow suppliers to validate packages of data, with disaggregated data provided to suppliers by exception, or not at all.

Interactions with TOMs

Decisions on both the TOMs and access to data (which are wider than the decision on whether or not to introduce enhanced privacy) will have implications for how these functions would be governed and operate. For example, it is assumed that both the AS and PS roles would need to be performed by a stand-alone party that is not active in the competitive market if Data Retrieval and Data Processing settlement functions remain competitive.

Impact on market roles

We assume that both feasible enhanced privacy services would need to be performed by central bodies in a world where other settlement functions remain competitive, on the basis that it would not be appropriate for competitive parties to perform the enhanced privacy roles as the intention of this intervention would be to prevent personal data being shared with suppliers or their agents. These would therefore preclude services being offered for the settlement functions of these customers.

For anonymisation this means that all settlement functions are effectively centralised for these customers, as we anticipate that this party would need to take on all settlement functions for these customers. As such, competition for the settlement processes for these customers is precluded. We therefore suggest that it is not appropriate to apply anonymisation to participating customers under Legal Obligation, or non-participating customers under opt in.

The pseudonymisation service, on the other hand, is likely to be lighter than the anonymisation service, and could exist alongside competitive settlement arrangements for data processes and aggregation (although as designed it would require centralisation of data retrieval functions).

3 How the access to data and Enhanced Privacy options could combine

3.1 Introduction

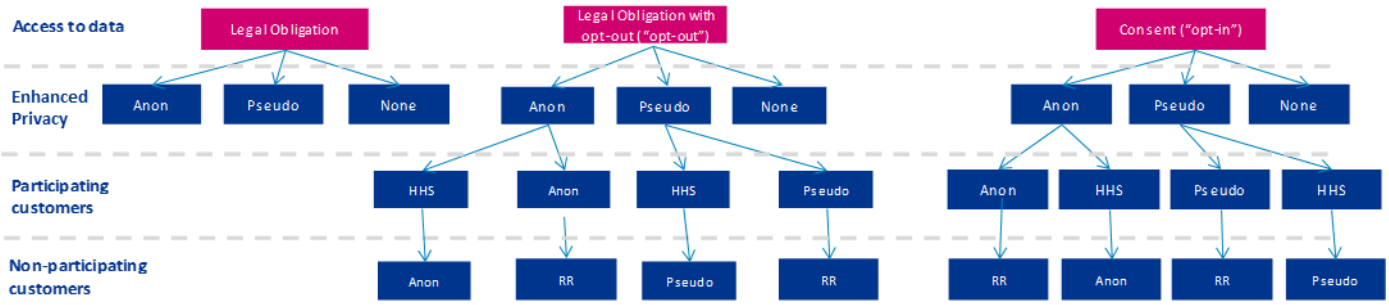
In this section, we consider the full list of possible access to data and enhanced privacy combinations, before setting out which of these we believe are most feasible following an initial assessment.

Under the notional long list of options, anonymisation or pseudonymisation could be applied to:

- All customers;
- No customers;
- Only 'participating' customers that do not opt-out, or that do opt in (with the remaining 'non-participating' customers settled with RRs and profiles); or
- Only for 'non-participating' customers that have opted out, or have not opted-in (with participating customers allowing their HH data to be used in settlement without any addition of enhanced privacy measures).

There are therefore a number of possible access to data and enhanced privacy combinations (see Figure 6). This list was reduced following the elimination of options that were illogical, or were otherwise unfavourable.

Figure 6 - All possible access to data and enhanced privacy options



3.2 Short list of access to data and Enhanced Privacy options

We developed a short list of options from all possible combinations following feedback received from workshops and discussions with Ofgem and ELEXON. We developed a number of 'design principles' to support this assessment:

- It was assumed that additional enhanced privacy would not act as an incentive for consumers to opt in or not to opt out of HHS[15] (but it is recognised that enhanced privacy could shift the balance

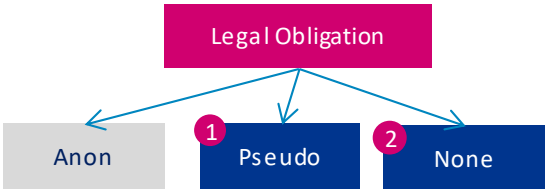
[15] However, we note that this is an assumption, and Ofgem will be carrying out consumer research to inform whether anonymisation and pseudonymisation would affect consumer participation.

of a decision in favour of protecting the rights and freedoms of consumers with regards to the privacy and security). It was noted that consumers who would prefer not to share their Half-Hourly data may choose not to accept a smart meter.

- It was recognised that a degree of personal data processing is required under all technically feasible enhanced privacy options.
- It was assumed that anonymisation and pseudonymisation would not be implemented together.
- Neither feasible enhanced privacy option is expected to have any material impact on data quality (when compared to HHS without enhanced privacy) as existing data validation processes should be unaffected (although some small errors from additional complexity are assumed).
- Both feasible enhanced privacy options would need to be performed by central bodies, even if other settlement functions remain competitive. For anonymisation this means that these functions are effectively centralised for opted out customers but could remain competitive for customers that do not opt out. Options where anonymisation is applied to participating customers under Legal Obligation, or non-participating customers under opt in, are excluded.
- Specific settlement arrangements for customers with existing smart meters covered by the existing regulatory regime (as described in Section 1.2) would not be worthwhile, especially as this customer group is expected to decline over time – although it was recognised that there could be different access to data options for customers covered by the existing regime (e.g. opt in for existing customers and opt-out for new customers)[16].

3.3 Enhanced Privacy Options under Legal Obligation

Figure 7 - Legal obligation and enhanced privacy



There are two options considered possible under Legal Obligation (with no opt out) access to data arrangements – one with pseudonymisation applied to the data of all consumers, and one with no additional enhanced privacy.

Under these options all consumers would have their data processed for HHS.

Anonymisation was excluded as this would effectively represent full centralisation of settlement functions for all (rather than just a sub-set) consumers. However, we note that a policy decision to centralise all settlement functions could be seen to achieve some of the same high level outcomes for all customers.

Legal Obligation with pseudonymisation for all customers has the advantage in that it could be seen to mitigate privacy concerns of having data processed on a mandatory basis.

[16] It was recognised that there could be different arrangements for customers covered by the existing regulatory regime, but this assessment focuses on the arrangements for customers with any new regulatory regime that GEMA introduces.

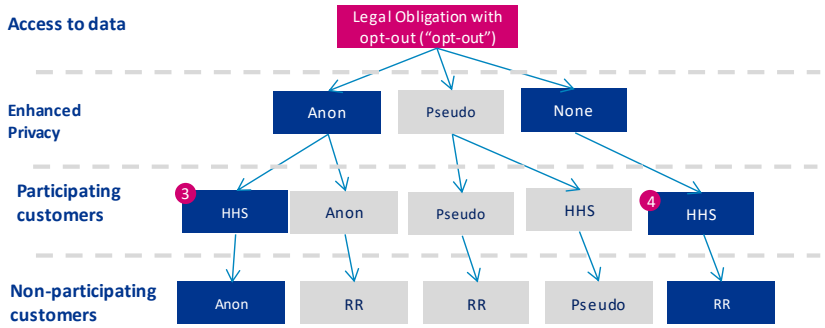
An additional option could allow pseudonymisation to be offered as a service that customers could opt into for enhanced privacy. This is not presented as an additional option, but rather as legal obligation, with an additional enhanced privacy service that customers could opt for.

3.4 Enhanced Privacy Options under Opt-out

There are two possible options under the Opt-out data access arrangements – one where consumers who opt out have their data anonymised, and another where there is no additional enhanced privacy.

Where there is no enhanced privacy, consumers who opt out are settled on the basis of RRs.

Figure 8 – Options for Legal Obligation with opt out



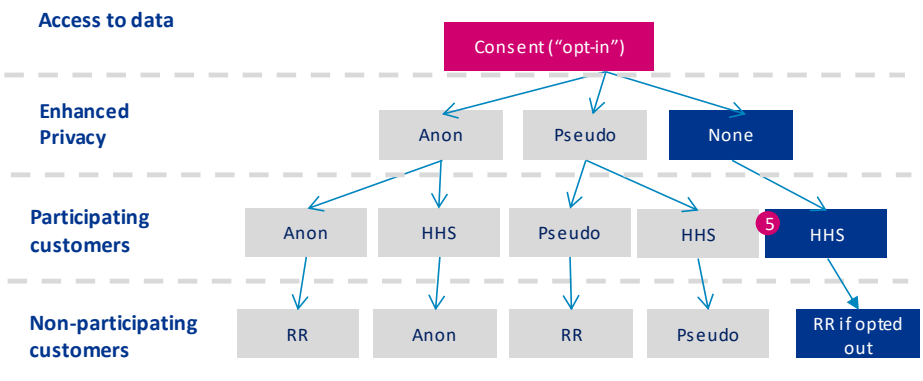
Options with enhanced privacy for participating (non-opted out) customers were ruled out on the assumption that these would not affect opt out rates, and lead to greater cost with limited/no benefit for customers are willing to share their HH data.

We have not presented opt-out with pseudonymisation for consumers that do opt-out. This was ruled out as it could be seen as misleading, and not in the spirit of GDPR (unlike opt out and anonymisation). However, it is recognised that a pseudonymisation service could be offered as an additional, optional service alongside legal obligation.

3.5 Enhanced Privacy Options under Consent

Both enhanced privacy options were ruled out where customers have not consented to opt in.

Figure 9 - Opt-in options



Pseudonymisation was ruled out on the basis that it would be strengthening status quo (for existing smart metered customers), without being likely to be increase opt in rates (given the complexity of explaining HHS and pseudonymisation to customers), and anonymisation was ruled on the assumption that if opt in rates were low, anonymising

customers that do not opt in would result in *de facto* centralisation for the majority of customers, and this the subject of a separate policy decision.

In addition, enhanced privacy is not expected to bring any additional benefit in terms of proportion of consumers' data used to carry out settlement.

This left one option under the Consent access to data arrangements, namely customers either opt into HHS, or else continue to be settled using consumer profiles and RR reads.

3.6 Possible options and evaluation

In summary, this leaves five possible access to data/enhanced privacy combination options as shown in Table 2 below.

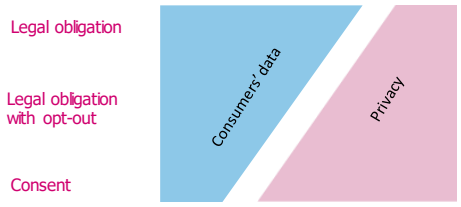
Table 2 – Possible access to data and enhanced privacy combination options

	Participating group[17]	Non-participating group[18]
Legal Obligation	No enhanced privacy	-
Legal Obligation	Pseudonymisation	-
Opt-out	No enhanced privacy	Anonymisation
Opt-out	No enhanced privacy	Settled on register reads
Opt-in	No enhanced privacy	Settled on register reads

Privacy and efficiency trade-offs

The key benefit of HHS is to enable the transition to a smarter, more flexible energy system. However, we note that there is a trade-off between the number of consumers that have their data processed for HHS (which helps drive the realisation of smart meter benefits for GB as a whole, through improving the efficiency of the electricity settlement) and the level of control that consumers have of their data.

Figure 10 - Privacy and data accuracy trade-offs



From a market efficiency perspective, the two Legal Obligation options are preferable in terms of maximising the amount of HH data used in settlement.

However, we note that GEMA's decision will need to balance the protection of consumers' privacy on the one hand, with the proportion of consumers' data being HHS and the benefits which this would deliver to consumers, on the other.

[17] i.e. all customers, customers that do not opt out, or customers that opt in depending on the access to data arrangements

[18] i.e. customers that opt out or do not opt in depending on the access to data arrangements

Opt-out rates are a known unknown. Further work and potentially learning from experience, would therefore be required to determine the differences between the Legal Obligation and Opt-out options from this perspective.

Proportionality of enhanced privacy interventions

The proportion of consumers that would be subject to anonymisation (determined by non-participation rates), will affect the acceptability of costs associated with implementing and then running the anonymisation processes.

While it is assumed that using consumers' anonymised data in settlement is better (from a data accuracy perspective) compared to using RRs and profiles, it is also noted that arrangements for consumer profiles already exist. Therefore if opt-out rates were assumed to be low, then the existing (or potentially a similar but different set of) profiling arrangements could remain appropriate for these low volumes of customers, while the additional cost of a separate anonymisation service may be warranted if non-participation rates were higher.

Recovering the costs of enhanced privacy

There is a question about how the costs of an anonymisation service are recovered – i.e. whether these costs are paid by the consumers that use the service (therefore creating a disincentive to opt-out) or whether they are smeared across all consumers. We note that this is a policy decision for Ofgem.

Unintended consequences of demand profiles

We note that there could be unintended consequences of continuing to use demand profiles and these should be considered when Ofgem is making a policy decision on access to data. For example, it is possible that customers could strategically opt out of HHS to avoid higher energy or network prices (e.g. in a world with time of use network tariffs).

This risk could in part be mitigated by ensuring that demand profiles are refreshed regularly, and that the data used to determine the demand profile are based on the aggregate/average consumption pattern of the opted out group, rather than the wider population. We note that consumers will be able to choose which tariff to accept, and that there are no current plans to mandate time-of-use tariffs. We also note that the proposed access to data options are for settlement purposes only.

4 Target Operating Models (TOMs)

4.1 Introduction

The Design Working Group (DWG) has developed skeleton Target Operating Models (TOMs) for HHS settlement. The TOMs reflect different market function configurations for each of the settlement processes. Ofgem will make a decision about which TOM to implement for HHS, and whether any of the settlement functions should be centralised.

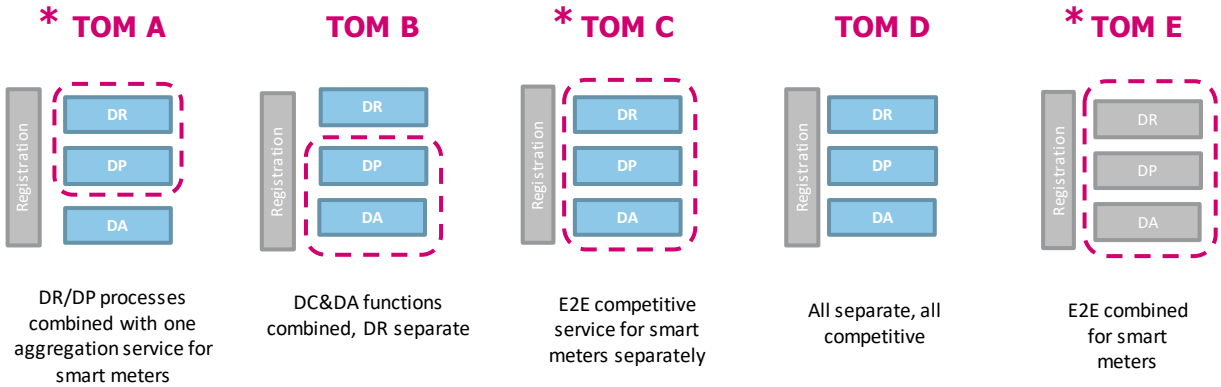
In this section, we do not detail all aspects of the TOMs, but highlight the key elements that are relevant for our evaluation of data access and enhanced privacy options.

4.2 Overview of TOMs

The TOMs were developed by mapping all the services that cover the end-to-end settlement process. Below is a simple representation of the key services relevant for our evaluation. These are:

- **Data retrieval (DR)** – accessing and retrieving energy usage data (import and export) from meters and associated technical details.
- **Data processing (DP)** – validating and estimating meter data, converting RRs to Settlement period (SP) data, providing data to relevant parties and exception reporting.
- **Data Aggregation (DA)** – responsible for receiving and aggregating Settlement Period data for use in settlement, network charging and other purposes (e.g. flexibility).
- **Registration** – registrar for all Metering Systems (and other related registration information) in Supplier Volume Allocation (SVA); a service currently undertaken by the Licensed Distribution System Operators.

Figure 11 - High-level overview of relevant aspects of the TOMs (for DCC enrolled smart meters)



In addition, Ofgem will make a decision about whether any of these functions are centralised. There may be more than one different configuration of centralised and competitive functions for each of the high-level TOMs.

4.3 Assumptions about centralisation of the TOMs

Given the uncertainty of the exact nature of settlement processes/functions, we make some simplifying assumptions to aid our evaluation – under a scenario where there was a decision to centralise some or all settlement functions – we assume:

- Under TOM A, DA functions would be centralised while the DR and DP functions would remain competitive.
- Under TOM B, DR functions could be centralised.
- TOM C and TOM E are effectively the same for the evaluation, because the key difference between these two TOMs is the treatment of advanced meters, which is out of scope. We therefore focus on TOM C for our evaluation.

4.4 Evaluation criteria

Our evaluation was informed through workshops and discussions with Ofgem and ELEXON, and with our privacy and security subject matter experts. In some cases, the evaluation was finely balanced, and ultimately may depend on the details of implementation.

There were a number of evaluation criteria that we agreed with Ofgem to aid our evaluation.

Table 3 - Evaluation criteria

Criterion	Description
Impact on consumer privacy	▲ Data privacy is defined as the appropriate use of data ▲ Our evaluation of privacy risks relates to incentives on parties processing data to misuse that data. The current elective arrangements HH data can flow from the meter to the supplier for validation. There is an open question as to whether the enduring arrangements will allow HH data to flow to suppliers. ▲ Models that have centralisation of settlement are assumed to perform better from a privacy perspective, as centralised parties that are not active in the competitive market are less likely to have an incentive to misuse consumers' personal data (however, this impact could be undermined if there is a decision to allow suppliers to receive HH data). ▲ Models with enhanced privacy are assumed to lead to greater privacy protections as they would prevent personally identifiable data from flowing to supplier agents or suppliers.
Impact on data security	▲ Data security refers to the confidentiality, availability, and integrity of data ▲ We reflect the extent to which options impact data security ▲ In particular, we considered the security trade-offs of a single body acting as a 'single point of failure' as a result of a data breach, compared to multiple bodies responsible for data processing. On balance, we assess a single body to provide greater security protection, compared to multiple market players.
Implications for accuracy of data settlement	▲ Data accuracy will be affected by the extent to which data can be validated and the number and nature of data transfers
Extent to which the option facilitates delivery of the benefits arising from HHS	▲ The arrangements should be coherent and excessive complexity should be avoided ▲ The arrangements should also support the changing nature of the electricity market ▲ Arrangements should also contribute to the smart meter roll out more generally by instilling (and not undermining) consumer confidence

Cost implications	▲ Cost implications, considering the impact of new roles and/or new organisations, as well as implications for other market players ▲ The relative cost of enhanced privacy/TOM options will be affected by the consent arrangements (i.e. the relative cost of new interventions will be higher if they only apply to a certain proportion of consumers)

In addition to these criteria, Ofgem will have consideration of distributional impacts – whether the effects of the proposals may be experienced differently by different groups or individuals, or may have differing effects across a variety of circumstances. As there are no obvious differences in distributional impacts between the different TOMs and access to data options (particularly at this high-level evaluation stage), we do not explicitly consider it in our assessment.

4.5 TOM evaluation

Our evaluation of the TOMs was from one particular lens – access to data and enhanced privacy. It does not consider wider costs or impacts of HHS or the TOMs.

At this high level, we could not identify any differences in terms of benefits of HHS or cost implications of the TOMs from the lens of our assessment. However, we note that a wider assessment of these factors could conclude different weightings.

Figure 12 - Evaluation criteria

Evaluation criteria
Strongly positive: +2
Positive: +1
Neutral / similar to the status quo: 0
Negative: -1
Strongly negative: -2

TOMs with no centralisation

Privacy

Options where there is more division between the roles perform worse on the assumption that there is the potential for a greater number of different commercial organisations to be involved in data processing.

- ▲ TOM D scores negatively and TOM C scores positively on this basis

Security

Options with greater data transfers compared to the status quo are assumed to perform worse, and those with less data transfers better.

- ▲ TOM D scores negatively and TOM C scores positively on this basis

Accuracy

We identified no areas for areas of likely impact on data accuracy compared to the status quo.

TOMs with centralisation

Figure 13 - TOMs with no centralisation

Criterion	A	B	C	D
Privacy	0	0	+1	-1
Security	0	0	+1	-1
Accuracy	0	0	0	0
Benefits of HHS	0	0	0	0
Cost	0	0	0	0

Figure 14 - TOMs with centralisation

Criterion	A	B	C
Privacy	0	0	+2
Security	+1	0	+2
Accuracy	+1	+1	+2
Benefits of HHS	0	0	0
Cost	0	0	0

Privacy

Options without competitive parties processing personal data perform better

- TOM C with centralisation performs best on this basis, but without other changes both TOM A and TOM B could have competitive parties processing personal data.

Security

On balance, a central (and regulated) body is likely to lead to greater security benefits than leaving security to all market participants under de-centralised models. With de-centralised models there is a risk that market participants will have differing levels of security, and incentives to innovate or reduce costs in a competitive market could undermine security standards.

- TOM C with centralisation performs best on this basis, and TOM A performs positively because the party that would hold the full customer dataset would be centralised.

Accuracy

It is assumed that there are benefits of a single, central body for data accuracy because of the lower number of data transfers, and the benefits of a single system / set of protocols for processing data. On the other hand, however, we note that it has been argued that competitive pressures should create incentives for high quality service more generally.

- On balance we note that TOM C with centralisation is assumed to have greater benefits for data accuracy as there are lower number of possible handoffs (although we recognise this argument is finely balanced) and as it could lead to additional benefits in terms of standardisation of data
- TOM A and TOM B are assumed to lead to improvements in accuracy as some parts of the settlement functions are centralised.

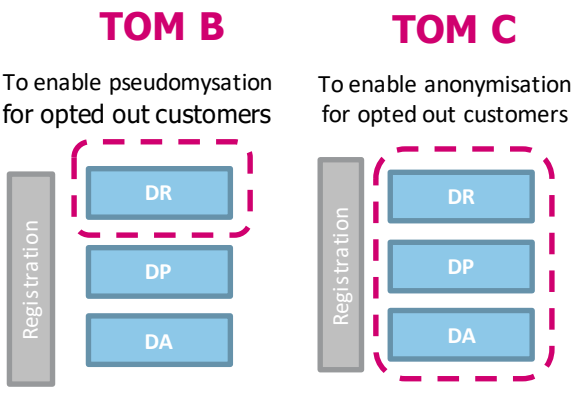
4.6 Compatibility with enhanced privacy and preferred TOMs

The TOMs will affect the effectiveness and coherence of the enhanced privacy options:

- It would appear that TOM B would be most suitable to achieve effective pseudonymisation (with centralisation of data retrieval functions, while allowing competition for the other settlement processes).
- It would appear that TOM C would be most suitable to achieve anonymisation for non-participating (or opted out) customers, as there would be less difference in the approach taken for anonymised and non-anonymised customers.

Therefore we suggest under options with enhanced privacy that TOM C and TOM B would appear most suitable.

Figure 15 - TOM and enhanced privacy compatibility



Under options with no centralisation of settlement functions, and no enhanced privacy, it would appear that TOM C performs best.

5 Drawing the assessments together

We have assessed a number of combinations of enhanced privacy, TOM and access to data arrangements (as described in Sections 2 to 4) and present six possible preferred options that combine these dimensions (Figure 16).

On the basis of our assessment, it appears that it is necessary to centralise part of the settlement processes for all customers, or all settlement processes for some customers:

- To achieve effective **pseudonymisation** it would be sensible that the data retrieval processes were centralised, in order to achieve effective privacy protections.
- To achieve effective **anonymisation**, all settlement arranges would effectively be centralised for a subset of customers.

We also note that many of the privacy benefits of (the technically viable approach to) anonymisation could be achieved by full centralisation of settlement functions, so we do not consider additional enhanced privacy to deliver significant value if all settlement functions were to be centralised. We assume any centralised party would have stringent data management techniques and security practices to protect consumers' data.

We then assessed the coherence of the enhanced privacy options with the access to data options, ruling out the following options:

- Anonymisation for all customers since this would drive a requirement for full centralisation of settlement regardless of other policy considerations;
- Adding enhanced privacy for participating (i.e. opted in or not opted out) customers since this would add unnecessary complexity which is deemed unnecessary; and
- Pseudonymisation for non-participating customers since pseudonymised data is still personal data (unlike fully anonymised data), and this would not be in the spirit of GDPR[19].

This resulted in five remaining combined access to data/enhanced privacy options:

Table 4 - Access to data and enhanced privacy options in scope

	Participating Customers [20]	Non-participating customers[21]
Legal Obligation	No enhanced privacy	-
Legal Obligation	Pseudonymisation	-
Opt out	No enhanced privacy	Anonymisation
Opt out	No enhanced privacy	Settled on register reads
Opt in	No enhanced privacy	Settled on register reads

[19] We note, however, that an additional pseudonymisation service could be offered alongside legal obligation, as an additional 'opt in' service.
[20] i.e. all customers, customers that do not opt out, or customers that opt in depending on the access to data arrangements
[21] i.e. customers that opt out or do not opt in depending on the access to data arrangements

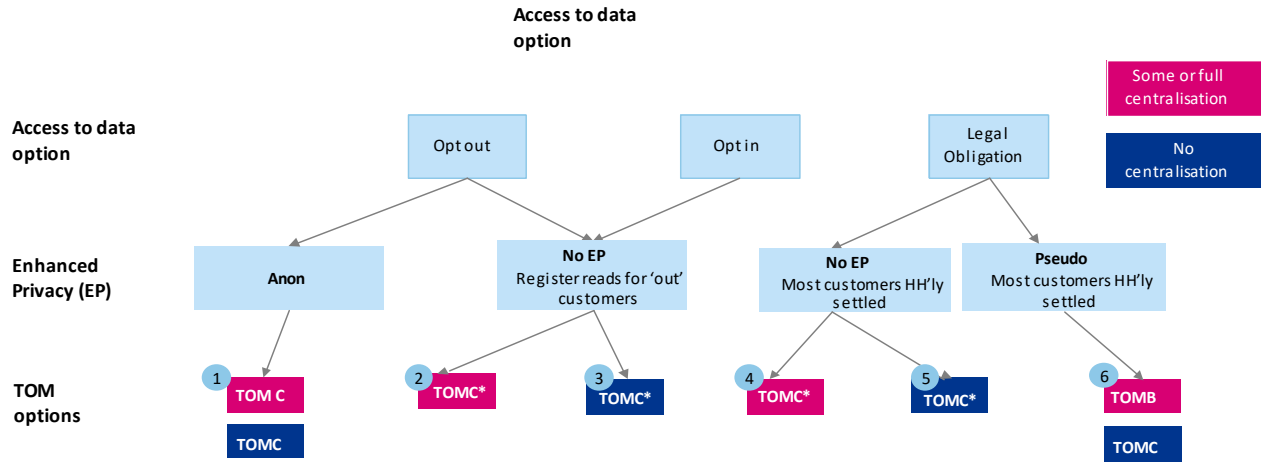
We also considered the coherence of the TOMs with the enhanced privacy strawmen. On this basis it would appear that:

- TOM B would be most obvious option to achieve effective pseudonymisation (as part of the DR function), while allowing the potential for competition for the other settlement (DP and DA) processes.
- TOM C[22] would be most suitable to achieve anonymisation for non-participating (or opted out) customers, as there would be less difference in the approach taken for anonymised and non-anonymised customers.

In addition, our evaluation of the TOMs without centralisation or enhanced privacy concluded that TOM C appears to be the most sensible option.

Bringing together our assessment of access to data, enhanced privacy and TOMs, we present six possible preferred options.

Figure 16 - Access to data, enhanced privacy and TOM decision tree



*In the absence of enhanced privacy, we have judged TOMC to be preferable, on the assumption that it is most beneficial from the perspective of privacy and security

The relative merit of these six remaining options are driven by Ofgem's policy decisions on whether to centralise settlement functions (and to what extent), as well as the approach taken on access to data. These decisions have drivers outside the scope of our assessment (including the impact on competition and the market) but from the lens of our evaluation we note:

[22] We note that TOM E would be equally suitable in this instance (but for simplicity we just refer to TOM C)

- Options with centralisation of settlement functions would afford better privacy protections, but preclude competition for these activities (and the associated benefits, which is a dimension that we have not reflected in our assessment).
- There are varying degrees of centralisation, and we note that some form of centralisation is necessary to implement either of the enhanced privacy strawmen we have developed.
- From a market efficiency perspective, options that involve placing a Legal Obligation on suppliers (or other party as appropriate) would be the best outcome – as it would involve the largest volumes of HH data being used in settlement, and it would negate the need for additional processes to manage consumer consent and dual settlement processes to manage different customer types (e.g. opt in and non-opted in customers), which will reduce cost. Conversely, it is clear that while a consent-based access to data model would lead to lower levels of data used in settlement, it would give consumers the greater control over their data.

6 Risks and mitigations

6.1 Introduction

In this section, we highlight a number of key risks identified with the enhanced privacy strawmen for anonymisation and pseudonymisation.

6.2 Anonymisation risks and mitigations

Table 5 - Anonymisation risks and mitigations

Risk	Potential mitigation measure(s)
1. There is a risk that a proposal to anonymise data for settlement will not have industry support, or result in additional risk premiums being added to tariffs. **Suppliers will likely have concerns if data is submitted on their behalf but they cannot query/challenge it.**	Consideration should be given to whether it is appropriate to allow anonymised data to be queried, and how this can be best achieved whilst maintaining data privacy.
2. There is a risk that anonymisation would not be effective in instances where there are small amounts of customers of a particular type on a particular network. **Anonymised data will likely need to be passed to suppliers in aggregated form to support their own data validation and forecasting.**	It is noted that this is an issue with the broader access to data arrangements and should be further considered as the detailed design is developed, to ensure that this risk is minimised as far as practically possible.
3. There is a risk that a new party retrieving large amounts of consumers' data could cause capability issues for the DCC. **It has been suggested that proposals that lead to larger amounts of service requests to the DCC could cause issues for DCC's capabilities (bandwidth).**	Explore detailed implementation with DCC.
4. There is a risk that anonymisation leads to duplication in retrieving consumers' data. **As suppliers could also be retrieving data for other purposes (as appropriate, with consent) this could lead to a greater number of service requests, which could worsen any issues that DCC may have with capability.**	Explore detailed implementation with DCC.

6.3 Pseudonymisation risks and mitigations

Table 6 - Pseudonymisation risks and mitigations

Risk	Potential mitigation measure(s)
1. There is a risk that pseudonymisation is ineffective because other data items could be used to identify individuals. **Other information that would accompany the pseudonymised data – such as GSP group, DNO and supplier agent information – could be used to identify individuals**	Data could be passed to suppliers in an aggregated basis only (where there are sufficient numbers of consumers). This risk will also be reduced by ensuring that only the data items absolutely necessary for data validation are associated with the pseudonym.
2. The MPAN-Pseudonymised IDs map would act as a single point of failure for the integrity of the enhanced privacy **Central to this option is a data map that would map MPANs to Pseudonymised IDs. This would need to be held by two or more parties - the Agent responsible for pseudonymisation and the Supplier Meter Registration**	Allowing the MPAN-pseudonyms to be refreshed could improve the resilience of the overall enhanced privacy process against the risk of breach.

Agent(s) (SMRAs). It is assumed that pseudonymised IDs would change upon a change of supplier **This map could hold the information for de-pseudonymising consumers' data so its integrity is central to the enhanced privacy**	
3. There is a risk that Pseudonymisation introduces greater data errors through increased complexity **The additional pseudonymisation process would introduce additional complexity, which could lead to instances of data errors.** **As it is assumed that pseudonymisation should not otherwise affect settlement processes, it is expected that the impact of this risk is low.**	NA – low risk, to be monitored during detailed design.
4. There is a risk that pseudonymisation leads to duplication of data retrieval efforts **As suppliers could also be retrieving data for other purposes (as appropriate, with consent) this could lead to a greater number of service requests, which could worsen any issues that DCC may have with capability.**	Explore detailed implementation with DCC.

7 Conclusion

In conclusion, we consider that the decision on whether to implement enhanced privacy (and if so the best type of enhanced privacy to implement) is nuanced, and finely balanced.

There are two high-level enhanced privacy strawmen that are potentially technically viable, and either (or both) of these could be further developed and assessed as part of the detailed design of the HHS arrangements for domestic and SME customers.

We note that the assessment of the relative merits of these two strawmen is highly dependent on the decisions that Ofgem is yet to make on the approach to data access, which TOM is selected and the degree of centralisation in the settlement functions.

In addition, if the approach to data access allows consumer choice on participation, namely the option to opt in or opt out, then the proportion of non-participating customers will be a key consideration, and should the number be at the lower end of the range, then the additional costs associated with enhanced privacy may be harder to justify.

If enhanced privacy is not taken forwards, and Register Reads (RRs) are to be used for non-participating customers, then it will be important to consider further how to ensure that demand profiles continue to be fit for purpose (such that they accurately reflect the expected consumption pattern of the group of customers that they are being used for).

The further development of these strawmen, should at a minimum include consideration of:

- The data that are to be made available to suppliers (e.g. for forecasting and to enable any querying of the data used in settlement) – noting that the potential benefits of HHS may be reduced if suppliers place a significant risk premium on some tariffs because they cannot accurately predict their likely imbalance exposure;
- The risks set out in Section 6 (including developing appropriate mitigations for these); and
- How the additional cost associated with enhanced privacy should be distributed/allocated.