ofgem

Making a positive difference
for energy consumers

Access to half-hourly electricity data for settlement purposes: a Data Protection Impact Assessment

Jenny Banks and Kieron McGlinchey

Contents

Executive Summary

A Data Protection Impact Assessment (DPIA) is a tool to help organisations find the most effective ways of complying with data protection obligations and meet individuals' expectations of privacy. In the UK, the Data Protection Act 2018 and General Data Protection Regulations (GDPR) are the cornerstones of data privacy legislation. They replaced the Data Protection Act 1998 on May 25 2018. We have reflected this legislative change in this DPIA. DPIAs are a key element of a 'privacy by design' approach - one that builds in privacy and data protection compliance from the outset.

Half-Hourly Settlement

In July 2017, we launched our Electricity Settlement Reform Significant Code Review (SCR). Since then, the Smart Meters Act 2018 has passed through parliament. This Act grants Ofgem additional powers with regards to market-wide Half-Hourly Settlement (HHS). We will continue under the SCR process until we make our decision, informed by our economic impact assessment as part of the market-wide HHS Business Case, on if, when and how to implement market-wide HHS. At that point, we will enact the powers granted to us in the Smart Meters Act, through which we will implement an enduring process to enable market-wide HHS for domestic and smaller non-domestic consumers.[1]

Smart and advanced meters can record a customer's consumption during each half hour period, enabling HHS. They also record how much electricity a consumer exports to the grid on a half-hourly (HH) basis.[2]

Settlement is the reconciliation of suppliers' contractual purchases of electricity against their customers' actual usage. At present, for domestic and smaller non-domestic consumers it is usually based on periodical meter reads, with in-day differences estimated using profiles[3] of consumption. HHS does this using actual half-hourly data, removing the need for estimates. HHS will expose suppliers to the true cost of their customers' usage and incentivise them to take steps to help their customers move their consumption to times of the day when electricity is cheaper to generate and transport, eg by offering smart tariffs and other innovative products. This will build on the platform provided by smart metering and enable a smarter, more flexible energy system that lowers bills, reduces carbon emissions, and enhances security of supply.

In order to settle consumers HH, data relating to individual consumers' electricity consumption in each half hour period of the day is required. The current Data Access and Privacy Framework (DAPF)[4] governing supplier access to smart and advanced meter data requires suppliers to obtain opt in consent from customers to access HH data from domestic smart and advanced meters. Given the anticipated system and consumer

[1] https://www.ofgem.gov.uk/system/files/docs/2017/07/electricity_settlement_reform_significant_code_review_launch_statement.pdf

[2] This DPIA is primarily focused on consumption data. However, use of export data for settlement is in scope and is covered specifically in chapter 7 below.

[3] Also known as load shaping or load profiling, this is the process where a consumption pattern (or shape) based on an average of users' consumption is applied to a long-term meter reading to estimate more granular consumption (eg HH) of a consumer, eg when the actual HH data for a particular period(s) is not available

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

benefits of HHS,[5] we are reviewing the rules on access to HH data to establish whether to amend the conditions of access to HH data specifically for settlement purposes.

As part of the HHS project, we are developing a new Target Operating Model[6] (TOM) for settlement. The TOM will outline the changes needed to settlement arrangements and supporting institutions to deliver market-wide HHS, including transitional arrangements. The TOM will need to accommodate Ofgem's decision on access to HH data for settlement and its implications in terms of any consumers whose HH data would not be available for settlement.

Options under consideration

As part of our review of the access to HH data arrangements for settlement purposes for domestic and microbusiness customers, we are considering three core options:

1. **Opt-in:** Access to HH electricity consumption data for settlement purposes is subject to existing data access rules, giving domestic consumers the choice to opt-in (the status quo for domestic consumers)

2. **Opt-out**: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only, unless the consumer opts out (HH data for microbusinesses is currently collected on an opt-out basis)

3. **Mandatory**: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only

We are considering two additional 'enhanced privacy' options which would both result in all smart or advanced metered consumers being half-hourly settled. These options would provide additional privacy to consumers:

4a. **Anonymisation**: consumers can choose to have their data retrieved, processed and aggregated by a centralised body, rather than by suppliers and their agents, with HH data anonymised after settlement processes are complete. All consumers would be settled using their HH data under this option. [7]

4b. **Hidden Identity**: HH electricity consumption data is retrieved by a new 'pseudonymisation service'. They replace the information[8] which can be used to identify an individual with a new unique identifier – obscuring their identity, as the data can no longer be attributed to individual consumers without a key. This pseudonymised[9] data is

[5] https://www.ofgem.gov.uk/system/files/docs/2018/02/market_wide_HHs_strategic_outline_case_february_2018.pdf

[6] https://www.elexon.co.uk/wp-content/uploads/2018/04/DWG-Consultation-Skeleton-TOMs-30April2018.pdf

[7] Providing they have a smart or advanced meter installed

[8] A device identifier which can be linked to an MPAN (Metering Point Administration Number).

[9] Pseudonymisation is the process of distinguishing individuals in a dataset by using a unique identifier that does not reveal their 'real world' identity

then processed for settlement purposes by the usual parties responsible for settlement. All consumers would be settled using their HH data under this option.[10]

Each option carries implications for how much HH data is available for settlement purposes and how data will flow and to what parties. The decision therefore has direct implications for both the costs and benefits of market-wide HHS. Flows of data will also be impacted by the work to design a new TOM for HHS and the question of whether or not to centralise the functions currently performed by supplier agents.

We are also considering whether any additional regulatory clarity may be needed with respect to the legal basis for processing HH export data from smart or advanced meters.

Assessment of Risks

We have identified and evaluated a number of risks arising or related to access to HH data for settlement purposes. Each risk has been evaluated after taking into account existing legal frameworks and proposed mitigations. This evaluation will be taken into account in reaching a final decision on access to HH data for settlement. Our current evaluation of risks is set out below with evaluation split between:

- anticipated severity of a risk
- anticipated likelihood of risk occurring

Overall evaluation of risk

	Access to HH electricity consumption data option	**Severity [11]**	**Likelihood[12]**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH data	Opt in	Moderate	Unlikely	Medium
	Opt out	Moderate	Unlikely	Medium
	Mandatory	Moderate	Unlikely	Medium
	Anonymisation	Moderate	Unlikely	Medium
	Hidden Identity	Moderate	Rare	Low
Privacy Risks: Suppliers, agents or other parties misuse HH data	Opt in	Minor	Possible	Medium
	Opt out	Minor	Possible	Medium
	Mandatory	Moderate	Possible	Medium
	Anonymisation	Moderate	Unlikely	Medium
	Hidden Identity	Moderate	Unlikely	Medium
Risk to market-wide HHS benefit realisation	Opt in	Major	Likely	High
	Opt out	Moderate	Likely	Medium
	Mandatory	Moderate	Possible	Medium

[10] Providing they have a smart or advanced meter installed

[11] Risk severity is ranked on a five-point scale: insignificant, minor, moderate, major, catastrophic

[12] Risk likelihood is also ranked on a five-point scale: rare, unlikely, possible, likely, almost certain

	Anonymisation	Moderate	Possible/likely[13]	Medium
	Hidden Identity	Minor[14]	Possible/likely[15]	Medium

Evaluation of export data risks

	Severity	**Likelihood**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH export data	Minor	Rare	Low
Privacy Risks: Suppliers, agents or other parties misuse export HH data	Minor	Rare	Low

Next steps

This is a draft DPIA. We would welcome comments from stakeholders on our approach and assessment of risks associated with the introduction of market-wide HHS and the decision on access to half-hourly electricity consumption data for settlement. Alongside this DPIA, we have published a consultation on access to HH electricity consumption data for settlement purposes. The DPIA should be read in conjunction with this consultation. We plan to carefully consider all evidence and views we receive in response to this consultation. We are working towards publishing a decision by the end of 2018.

[13] At this stage, we are not able to be more specific than "possible/likely" because of the current uncertainty of the costs and timeframes of implementing and operating an anonymisation or hidden identity solution

[14] Severity here is minor, but with potential for significant costs and/or delay

[15] At this stage, we are not able to be more specific than "possible/likely" because of the current uncertainty of the costs and timeframes of implementing and operating an anonymisation or hidden identity solution.

1. Introduction and scope

Background and context

1.1 Energy suppliers purchase electricity based on their forecasts of customer consumption. The differences in each half-hour between the volumes of energy purchased by suppliers and the volumes their customers are deemed to have used are identified, reconciled and paid for through the settlement system.

1.2 Domestic and small non-domestic consumers have traditionally been settled non-half-hourly (NHH) against an estimated profile of their consumption. Profile Classes[16] provide estimates as to when consumption has occurred for individual consumers. This is necessary because smaller electricity consumers have, until recently, not had meters that are capable of recording half-hourly (HH) electricity consumption.

1.3 Profile classes are currently divided so that domestic customers fall into classes 1-2, while profile classes 3-4 comprise smaller non-domestic consumers, a significant proportion of which are microbusinesses.[17] Smart and advanced meters,[18] which can record actual consumption in each HH period, are currently being offered to Profile Class 1-4 customers. The installation of smart and advanced meters will enable these customers to be settled based on actual HH consumption, rather than using estimated consumption profiles.

1.4 HH electricity consumption data[19] from domestic consumers is considered to be personal data where it is combined with certain information, eg the Meter Point Administration Number (MPAN), which enables it to be linked back to a specific household. Only certain parties can link this.[20] We are also considering the sensitivity of HH export data and whether any regulatory clarity is needed on access to HH export data from smart and advanced meters. We refer to the specific risks relating to export in chapter 7.

1.5 The Data Access and Privacy Framework (DAPF), enacted through the Standard Conditions of Electricity Supply Licence, Distribution Standard

[16] Profile classes are calculated using a sample of customers that are representative of the population. More information about Profile Classes can be found on ELEXON's website: https://www.elexon.co.uk/knowledgebase/profile-classes/

[17] The definition of a microbusiness customer is set out in condition 7A of the Standard Conditions of Electricity Supply Licence.

[18] In some cases, some non-domestic customers are having advanced meters installed rather than smart meters.

[19] By consumption data, we refer to half-hourly import data, henceforth referred to as "HH data"; however, less granular data can also be personal data in some circumstances. Where we discuss export data, we specify this. We note that we consider export data also to be personal data, where it relates to a natural person.

[20] Distribution network operator (DNOs), suppliers and their agents, and some authorised third party intermediaries can use information from the ECOES industry database to see the address associated with an MPAN.

Licence Conditions and the Smart Energy Code, governs access to energy consumption data from domestic and microbusiness consumers.[21] Ofgem extended the DAPF in 2015 to apply the provisions to all remote access meters.

1.6 Where non-domestic consumers are concerned, only HH data from those classified as 'microbusinesses'[22] is treated by the Standard Conditions of Electricity Supply Licence as being sufficiently similar to domestic consumption data as to warrant specific controls on data access.[23] The consumption data of larger non-domestic consumers is not within scope of this DPIA because it is not considered to be personal data.

1.7 Settling customers HH requires HH data on electricity consumption to be retrieved from smart or advanced meters, validated, processed and passed to the body responsible for administering the settlement system.

1.8 As we have set out previously,[24] potential use of consumption data for calculating transmission and distribution network charging by suppliers and their appointed agents is within the scope of the work underway to develop a Settlement Target Operating Model (TOM). If network charging proposals currently being developed by Ofgem require changes necessitating a further DPIA or an update to this one (eg access to additional types of personal data or requirement for additional parties to handle individual consumers' HH consumption data beyond what is considered in the attached DPIA) this would be subject to further consultation.

Overview of Settlement Reform

1.9 In July 2017, we launched the Electricity Settlement Reform Significant Code Review (SCR) to design, assess and implement market-wide HHS.[25] We intend to make our final decision on if, when and how to introduce market-wide HHS in the second half of 2019. Our business case, based on the Treasury's Five Case Model[26] and which incorporates a cost-benefit analysis, will support our final decision on market-wide HHS. As part of our Business Case work, we are conducting an economic assessment (an Impact Assessment) to weigh up the

[21] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486352/DAPF_Consultation_Response.pdf

[22] This is defined in the Standard Conditions of Electricity Supply Licence (7A.14) as "a Non-Domestic Consumer: (a) which is a "relevant consumer" (in respect of premises other than domestic premises) for the purposes in article 2(1) of The Gas and Electricity Regulated Providers (Redress Scheme) Order 2008" or "(b) which has an annual consumption of not more than 100,000 kWh".

[23] For microbusinesses, these controls are on an opt out basis for HH data access for settlement purposes, see https://www.gov.uk/government/consultations/smart-meter-data-access-and-privacy

[24] In Appendences 1D and 1B of our HHS SCR Launch Statement, see https://www.ofgem.gov.uk/publications-and-updates/electricity-settlement-reform-significant-code-review-launch-statement-revised-timetable-and-request-applications-membership-target-operating-model-design-working-group

[25] https://www.ofgem.gov.uk/system/files/docs/2017/07/electricity_settlement_reform_significant_code_review_launch_statement.pdf

[26] The Five Case Model is a methodology for producing business cases for spending proposals. See here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/469317/green_book_guidance_public_sector_business_cases_2015_update.pdf

expected current and future costs and benefits of a decision on market-wide HHS.

1.10 Alongside the Business Case and our access to HH data for settlement purposes work, our other workstreams, as part of the market-wide HHS project, include designing the TOM and our work on supplier agent functions.

Benefits of market-wide HHS

1.11 The move to market-wide HHS forms part of a wider set of reforms looking to facilitate the energy system transition and to improve the outcomes that consumers can achieve from the retail market. Market-wide HHS has a critical role to play by acting as an enabler for flexibility and facilitating new and innovative business models. A smarter, more flexible energy system could have significant benefits, with estimated savings of £17-40bn by 2050.[27, 28]

1.12 HHS will expose suppliers to the true cost of their customers' usage and therefore incentivise them to take steps to encourage their customers to move their consumption (and/or export) to times of the day when electricity is cheaper (or more expensive in the case of export). Suppliers may do this, for example, by offering time of use or other types of smart tariffs.

1.13 This is expected to enable a smarter, more flexible energy system that lowers bills, reduces carbon emissions and enhances security of supply. For example, price signals to incentivise consumers to use electricity when it is cheap and abundant and to reduce consumption when supply or networks are constrained are expected to lead to reduced requirement for network reinforcements and expensive additional generation capacity.

1.14 HHS should therefore enable more efficient use of existing network and generation infrastructure, including of less flexible sources of generation such as nuclear and some renewables. All consumers are expected to benefit from lower system costs because of HHS, not just those who engage with the new opportunities it provides.

1.15 Innovations and technological advances such as smart appliances,[29] electric vehicles with smart charging,[30] and batteries should enhance consumers' ability to adapt their consumption in response to price signals. HHS will incentivise the development and adoption of these new technologies, and enable significant benefits over time if, as expected, the cost of these technologies falls and they become more accessible to more consumers.

---

[27] These benefits are broader than HHS, however HHS will be a key enabler in achieving them, as noted in the joint Ofgem-Government Smart Systems and Flexibility Plan (July 2017): https://www.ofgem.gov.uk/system/files/docs/2017/07/upgrading_our_energy_system_-_smart_systems_and_flexibility_plan.pdf

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/568982/An_analysis_of_electricity_flexibility_for_Great_Britain.pdf

[29] https://www.gov.uk/government/consultations/proposals-regarding-setting-standards-for-smart-appliances

[30] The Automated and Electric Vehicles Bill 2017 seeks to improve the consumer experience of EVs by allowing the Government to require the installation of charge points at motorway service areas and large fuel retailers and to require a set of common technical and operational standards for public charge points, ensuring they are convenient to access and work seamlessly right across the UK

1.16 We have considered the impacts of our decision on access to HH data for settlement on the expected benefits of market-wide HHS in the consultation published alongside this DPIA. We focus on privacy risks in this DPIA but have also briefly reflected the key risks of not realising benefits in the risk assessment section. We have more thoroughly reflected proportionality of the different access to HH data for settlement options in the consultation.

The regulatory framework governing access to data from smart and advanced meters

1.17 The first provisions of the Data Access and Privacy Framework (DAPF), governing access to smart and advanced metering energy consumption data, was placed into regulation in 2013, and subsequently extended by Ofgem in 2015 to apply the provisions to all remote access meters.[31] Under the rules set out in this framework, HH data can only be accessed by suppliers or third parties where consumers have given their consent ('opt in').[32] HH data for microbusiness consumers is available to suppliers on an opt out basis.

1.18 The DAPF, along with the relevant data protection legislation outlined below sets out the basis upon which suppliers can access consumers' data from smart and advanced meters and the choices consumers have in relation to this access.[33] The aspects of the framework that are relevant to the conditions for access to HH data from smart meters and advanced meters are set out in Standard Condition 47 of the Standard Conditions of Electricity Supply Licence.[34]

1.19 Given that consumers currently have to make an active decision to opt in to share their HH data for settlement purposes, retaining the current licence conditions covering access to HH data for settlement from smart and advanced meters presents the risk that many consumers are not HH settled. In the Government response to the consultation on the DAPF, Government noted that there "are also expected to be wider developments in the energy market (such as on settlement)" that "might have implications for smart metering data access and privacy. The Government is therefore clear that the framework should be kept under review in order that it can take account of any relevant developments". Ofgem is therefore reviewing the rules on access to HH data from smart and advanced meters to consider whether any changes should be made to enable access to HH data for settlement purposes, and if so, what the appropriate privacy safeguards should be. We are publishing a consultation document alongside this DPIA.[35]

Personal data

[31] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486352/DAPF_Consultation_Response.pdf

[32] Suppliers are also able to access this data where they have an approved trial

[33] This only applies to domestic and microbusiness consumers' data only

[34] Ofgem standard conditions of electricity supply licence, see: https://epr.ofgem.gov.uk/Content/Documents/Electricity%20Supply%20Standard%20Licence%20Conditions%20Consolidated%20-%20Current%20Version.pdf

[35] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

1.20 When HH data is retrieved from a smart and advanced meter, it comes with information that can be used by some parties to determine the identity of an individual consumer. Specifically, this data is supplied with a device ID that can be linked with an MPAN. An MPAN is required for data to be processed for settlement. As the potential exists to identify a consumer from a particular set of consumption data with the MPAN attached, Ofgem's approach is to treat this data as personal. It is worth highlighting however, that only authorised parties, such as DNOs, certain third party intermediaries, suppliers, and supplier agents are able to map MPANs to individual addresses.[36]

1.21 Given that we are treating HH electricity import (also known as consumption) and export data as personal data, data protection legislation is relevant. Two particularly relevant pieces of legislation are:

- The UK Data Protection Act (DPA) 2018;[37] and
- The EU General Data Protection Regulation (GDPR),[38] as discussed below

General Data Protection Regulation

1.22 The GDPR has applied since 25 May 2018, two years after its entry into force in May 2016. The decision on access to HH data for settlement is being assessed against the requirements of the GDPR and the DPA 2018.

1.23 The GDPR makes a number of changes to the UK's existing data protection regime and puts in place more stringent obligations in relation to personal data processing than applied under the original DPA 1998. Compliance with this legislation is overseen by the Information Commissioner's Office (ICO), which was set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Key changes which the GDPR introduces that may be relevant to access to HH data from smart and advanced meters for settlement purposes include:

- An entity processing personal data under the instruction of another organisation will be directly liable under the GDPR for failure to meet certain obligations. Under the GDPR, the obligations are more extensive than before and include direct liability for data processors.
- Where processing is based on consent, such consent must be 'freely given, informed, specific and unambiguous'. Such consents will have to be unbundled, allowing individuals the choice of giving or not giving separate consents for non-essential purposes. Consent that is reliant on opt out default arrangements is no longer valid under GDPR;
- That organisations are required to disclose to the relevant regulatory authorities within 72 hours any breaches that are likely to result in a risk of adversely affecting individuals' rights and freedoms;

[36] Distribution network operator (DNOs), suppliers and their agents, and some authorised third party intermediaries can use information from the ECOES industry database to see the address associated with an MPAN.

[37] This repealed and replaced the Data Protection Act 1998, and was given Royal Assent on May 23rd 2018 see: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted/data.htm

[38] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- That organisations are required to disclose to the affected individuals without undue delay any breaches likely to result in a *high* risk of adversely affecting individuals' rights and freedoms; and
- That fines of up to €20m or 4% of annual worldwide turnover can be levied against non-compliant organisations for serious breaches.
- Individuals will have new rights. These include a right to 'data portability' and a 'right to be forgotten'. Respectively, these rights will give individuals, under some circumstances, the right to be provided with their data in a reusable, electronic format (or to have this data "ported" directly to another organisation) and to delete and destroy data on request.
- Reinforcement of the existing data protection principles, such as fairness and transparency, data minimisation, accuracy and security, as well as a new principle of accountability, which requires organisations to be able to demonstrate their compliance.

1.24 Ofgem will consider the implications of the GDPR when assessing the merits of the access to HH data options.

Purpose and rationale for undertaking a Data Protection Impact Assessment

1.25 In summer 2014, the provisional findings of the CMA's energy market investigation found that the absence of a firm plan for moving to HHS for domestic electricity consumers represented an adverse effect on competition. In its final report, published in summer 2016,[39] the CMA recommended that DECC (now BEIS) "*consider removing any potential barrier for suppliers to collect consumption data with greater granularity than daily in the context of the review of the Data Access and Privacy Framework*" (DAPF).[40]

1.26 Ofgem launched an SCR in July 2017 with the aim of introducing market-wide HHS for consumers in profile classes 1-4.[41] As such, we are reviewing the choices that consumers have with respect to the sharing of their HH data for settlement purposes. This process will therefore potentially result in changes to both the use of HH data and an individual's control over that data for settlement purposes.

1.27 Given these possible changes, Ofgem has decided to undertake this Data Protection Impact Assessment (DPIA). This is in line with best practice guidance from the ICO. Ofgem is taking a privacy by design approach[42] to considering the changes to data access and utilisation. The ICO recommends the use of DPIAs as integral to this. For more information on what a DPIA entails, see Appendix 1.

[39] https://www.gov.uk/cma-cases/energy-market-investigation#remedies-implementation
[40] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf
[41] https://www.ofgem.gov.uk/system/files/docs/2017/07/electricity_settlement_reform_significant_code_review_launch_statement.pdf
[42] A privacy by design approach promotes privacy and data protection compliance from the start of a project. See https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

1.28 Specifically, Ofgem has identified the following potential changes which are relevant in our decision to undertake a DPIA:

- Most domestic and profile class 3-4 electricity consumers are presently settled non-HH. Moving to market-wide HHS will mean that HH data from smart and advanced meters is used for settlement at a far larger scale than is currently the case;[43]
- Depending on the option chosen, HH data from smart and advanced meters could be taken and used for settlement purposes including calculation of network charges, which includes load shaping,[44] without consumers having a choice over whether or not to provide consent;[45] and
- Depending on Ofgem's decision on whether or not to centralise functions currently performed by supplier-appointed agents and the design of the Target Operating Model (see section two), HH data would potentially be retrieved and processed by parties that do not currently have access to this information.

1.29 This DPIA is being undertaken in order to draw together evidence to inform and support Ofgem's decision on access to HH data from smart and advanced meters for settlement purposes and the mitigations that may be developed to address any risks identified.

1.30 The preparation of this DPIA has been an iterative process that has been informed by the ICO's best practice guidance and comments at key points. We welcome and will consider comments from all stakeholders, and will update the DPIA accordingly in light of further evidence received in response to our consultation on access to HH data.

[43] Currently suppliers can choose to settle consumers HH under elective HHS, however, at present, the vast majority have not chosen to do so

[44] Also known as load profiling, this is the process where a consumption pattern (or shape) is applied to a long-term meter reading to estimate more granular consumption (eg HH) of a consumer, for example' when the actual HH data for a particular period(s) is not available

[45] Access to data for any purpose outside of settlement including billing and marketing would remain subject to the Data Access and Privacy Framework, which stipulates that suppliers must obtain opt in consent to use HH data for these purposes.

2. Approach to Half-Hourly Settlement and options under consideration

Progress so far

2.1 The Information Commissioner's Office highlighted in its response to our 2015 consultation on the way forward for HHS that *"Consumption data collected from a smart meter is personal data when linked to the particular Meter Point Administration Number (MPAN) relating to a domestic premises or sole trader".*[46]

2.2 The ICO also stated, "*We strongly advise that any move towards half-hourly settlement does not take place until the issue of how it will interact with the* [Data Access and Privacy Framework (DAPF)] *has been fully considered. We would also strongly recommend that the possibility of anonymising or aggregating half-hourly consumption data for settlement purposes is fully explored to establish the extent to which this would be compatible with half-hourly settlement. Only once other more privacy friendly alternatives have been ruled out should any changes to the DAPF be considered. To address these issues we suggest that a privacy impact assessment (PIA) be undertaken".*[47]

2.3 Ofgem is taking a privacy by design approach to considering access to half-hourly (HH) electricity consumption data for settlement. We communicated to stakeholders in September 2017[48] that we are considering access to HH electricity consumption data[49] for settlement purposes only.[50, 51] As we set out in Appendices 1D and 1B our SCR Launch Statement for HHS, use of data for calculating transmission and distribution network charges by suppliers and their appointed agents is within the scope of the work underway to develop a Settlement Target Operating Model (TOM). If network charging proposals currently being developed by Ofgem require changes necessitating a further DPIA or an update to this one (eg access to additional types of personal data

[46] We also note that the ICO responded to our 2016 consultation, "Mandatory Half-Hourly Settlement: aims and timetable for reform", see here: https://www.ofgem.gov.uk/system/files/docs/2017/01/information_commissioners_office_consultation_response.pdf

[47] https://www.ofgem.gov.uk/system/files/docs/2016/03/information_commissioner_response_-_dec_15_open_letter.pdf

[48] https://www.ofgem.gov.uk/system/files/docs/2017/09/project_objectives_and_assessment_options_for_the_market-wide_half-hourly_settlement_business_case.pdf

[49] Henceforth referred to as "HH data". Where we discuss export data, we specify this.

[50] The BSC definition is that settlement means the determination and settlement of amounts payable in respect of Trading Charges (including Reconciliation Charges) in accordance with the Code (including where the context admits Volume Allocation); https://www.elexon.co.uk/wp-content/uploads/2018/02/Section_X_1_v80.0.pdf

[51] Through the consultation accompanying this document, we are also considering whether licensed parties should have access to *aggregated* HH data – and therefore not personal data – for forecasting purposes, to protect consumers from the additional forecasting costs HHS would otherwise introduce.

or requirement for additional parties to handle individual consumers' HH consumption data beyond what is considered in the attached DPIA) this would be subject to further consultation.

2.4 Suppliers and other parties wishing to access HH data for activities not included under the definition of settlement will still be required to follow the provisions of the DAPF and any relevant wider legislation when seeking to retrieve data for non-settlement purposes. BEIS has committed to concluding a review of the Data Access and Privacy Framework by the end of 2018.

2.5 Our assessment of feasible options will take into account the implications of access to HH data choices on the realisation of the intended benefits of HHS, including facilitating flexibility in the energy system.

2.6 Ofgem published a voluntary request for information in October 2017 to gather information on the ways in which suppliers communicate with consumers when seeking to access HH data, how consent preferences are recorded, storage of HH data and uses of HH data. The information gathered has been used in drafting this DPIA.

2.7 We contracted Baringa Partners to provide analysis including assessing whether and how anonymisation or pseudonymisation techniques can be applied to HH data in settlement. Anonymisation is defined under GDPR as "data rendered anonymous in such a manner that the data subject is not or no longer identifiable",[52] while pseudonymisation is defined in the ICO's anonymisation Code of Practice as "the process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity".[53] We have published Baringa's assessment alongside this DPIA.

2.8 We have engaged with stakeholders to gather views on the options set out for settlement and to explain the parameters and key factors in our evaluation process. Given the significance of our decision on access to HH data for consumers, we have regularly engaged with Citizens Advice. We have also engaged with suppliers, supplier agents, other consumer groups and BEIS. Specific engagement points have included:

- Settlement Reform Stakeholder workshop
- Independent Suppliers' Forum
- Settlement Reform Stakeholder teleconferences
- Bilaterals with stakeholders
- Presentations to and discussions with the HHS Design Working Group[54] and Design Advisory Board[55]
- Ofgem Consumer Panel and a broader consumer survey

Options being considered on access to half-hourly electricity consumption data for settlement

[52] GDPR, Legislative acts (26)
[53] https://ico.org.uk/media/1061/anonymisation-code.pdf
[54] https://www.elexon.co.uk/group/design-working-group/
[55] https://www.ofgem.gov.uk/gas/retail-market/forums-seminars-and-working-groups/design-advisory-board-market-wide-half-hourly-settlement

2.9 Ofgem published a document[56] in September 2017 outlining the project objectives and assessment options under consideration for the market-wide HHS business case. We have slightly amended the enhanced privacy options (with 'hidden identity' formerly referred to as pseudonymisation) options under consideration since publishing this document.

2.10 The options we are considering are now as follows:

1. **Opt in**: Access to HH electricity consumption data for settlement purposes is subject to existing data access rules, giving domestic consumers the choice to opt-in (the status quo for domestic consumers)

2. **Opt out**: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only, unless the consumer opts out (HH data for microbusinesses is currently collected on an opt-out basis)

3. **Mandatory**: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only

2.11 Since publishing the original options, Ofgem has also worked with Baringa to consider whether pseudonymisation or anonymisation could be combined with any of options 1-3 above. In practice, most combinations of pseudonymisation or anonymisation with opt in or opt out have been ruled out as they were not expected to offer significant benefits in comparison to the additional anticipated costs or complexity.[57]

2.12 We are now referring to these options as 'enhanced privacy' options, and, for reasons of accuracy and clarity, we are now referring to pseudonymisation as 'hidden identity'. These options are as follows:

4a. **Anonymisation**: consumers can choose to have their data retrieved, processed and aggregated by a centralised body, rather than by suppliers and their agents, with HH data anonymised after settlement processes are complete. All consumers would be settled using their HH data under this option. [58]

4b. **Hidden Identity**: Hidden Identity: HH electricity consumption data is retrieved by a new 'pseudonymisation service'. They replace the information[59] which can be used to identify an individual with a new unique identifier – obscuring their identity, as the data can no longer be attributed to individual consumers without a key. This pseudonymised data is then processed for settlement purposes by the usual parties responsible for settlement. All consumers would be settled using their HH data under this option. [60]

[56] https://www.ofgem.gov.uk/system/files/docs/2017/09/project_objectives_and_assessment_options_for_the_market-wide_half-hourly_settlement_business_case.pdf

[57] This can can be found in Baringa's evaluation https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[58] Providing they have a smart or advanced meter installed

[59] A device identifier which can be linked to an MPAN (Metering Point Administration Number).

[60] Providing they have a smart or advanced meter installed

Proportionality

2.13 We have taken a number of steps to ensure that any change to rules on access to HH data for settlement are proportionate when weighed against the anticipated benefits. As discussed above, this includes investigating 'enhanced privacy' options as part of a privacy by design approach.

2.14 We have restricted the amount of processing in the scope of the access to HH data for settlement decision to settlement purposes only.[61] In paragraphs 2.20-2.22 below, we detail why we are minded to treat existing smart and advanced metered consumers differently to consumers who had a smart or advanced meter installed prior to any regulatory or code changes.

2.15 We have also considered the risks to consumers of sharing and not sharing this data. In chapter 8, we discuss the various safeguards already in place and protecting the rights of individuals. It is our view that the existing safeguards provide suitable protection to the privacy rights of consumers under all access to HH data options under consideration.

2.16 Market-wide HHS will expose suppliers to the true cost of supplying their customers in any half-hour period, putting incentives on them to help their customers shift their consumption to times when electricity is cheaper to generate or transport. HHS is thus expected to lead to a more sustainable and affordable energy system, driven by consumers responding to the incentives offered by their suppliers to better manage their energy consumption. The scale of benefits that can be achieved through market-wide HHS will depend (in part) on the rules under which suppliers access their consumers' HH data, as suppliers will not be exposed to the true cost of supply for those customers that do not provide their HH data for settlement purposes.

2.17 Without the demand shift and reduction associated with wider supplier exposure to the costs of supply, decarbonising the GB energy system, integrating EVs and maintaining the networks will be considerably more expensive.[62] Therefore, without HHS or where few consumers opt to share HH data, societal harm emerges in the form of a financial and environmental loss[63] relative to a counterfactual scenario with market-wide HHS and sufficient numbers of consumers sharing their HH data for settlement purposes. The additional costs to the energy system without HHS would subsequently be passed to consumers.

2.18 Ofgem requests information annually from all larger electricity suppliers (those with more than 250,000 customers), through the Smart Metering annual Request for Information (RfI), on the proportion of domestic consumers opting in to share their HH data with their supplier. On the basis of current opt in rates, it appears likely that a potentially significant proportion of consumers would not be settled using their actual HH data if Ofgem decided to retain the requirement to obtain opt in consent to access data.

2.19 Suppliers may opt to introduce HHS and new products through elective HHS, but, without exposing suppliers to the cost of supply of most of their customers in each half-hour period, we are unlikely to see these products

[61] As stated above, we have previously set out that use of data for calculating transmission and distribution network charging by suppliers and their appointed agents, is within the scope of this work.

[62] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/568982/An_analysis_of_electricity_flexibility_for_Great_Britain.pdf

[63] Market-wide HHS is likely to lead to a less carbon intense electricity generation system

develop to an extent that will bring significant system-level benefits. Moreover, without requiring all suppliers to settle their customers on a HH basis, suppliers may either never use elective HHS or cherry-pick certain customers through elective HHS to help manage their requirements in the competitive market, leaving remaining customers unable to access and realise direct HHS benefits.

Existing smart and advanced metered customers

2.20 We have previously noted[64] in communications with stakeholders that we will need to consider further any bespoke rules that may be necessary for consumers who had a smart or advanced meter installed prior to any regulatory or code changes. This customer group will have accepted a smart or advanced meter on different terms[65] to those whose smart or advanced meters were installed after any changes relating to data access.

2.21 In the interests of fairness, we are keen to avoid requiring retrospective changes to the terms of consumers' contracts. As such, our proposal is that the point at which a consumer made a choice to change electricity supply contract, they would then be subject to the new regulatory framework. Such a change would take place following either a switch to a new supplier or an explicit choice to take up a different tariff with their existing supplier.

2.22 Our current proposal, outlined in the consultation document,[66] is that a consumer who had accepted a smart or advanced meter prior to any regulatory or code changes on access to HH data for settlement would be subject to the new regulatory framework only after they made an active choice to change their electricity contract. Suppliers would be required to make their customers aware of the terms of the new contract and clearly present any choices that the customer has about sharing their HH data.

Microbusiness customers

2.23 As highlighted above, supplier access to HH data for settlement from microbusiness customers is currently on an opt out basis. We intend to rule out option one above (opt in) for microbusiness customers on the basis that this would introduce a layer of privacy that was not considered appropriate or necessary when the original framework was established.[67] Moreover, this would be likely to lower the proportion of HH data available from this consumer group and therefore the percentage that could be HH settled.

2.24 Ofgem is therefore considering all remaining access to HH data for settlement options for microbusiness consumers. We outline in our consultation that we are most likely to align access to HH data for microbusiness customers with a) other larger businesses or b) domestic consumers (if we do not retain opt in for this group). We are also considering retaining existing the opt out arrangement for this group.

---

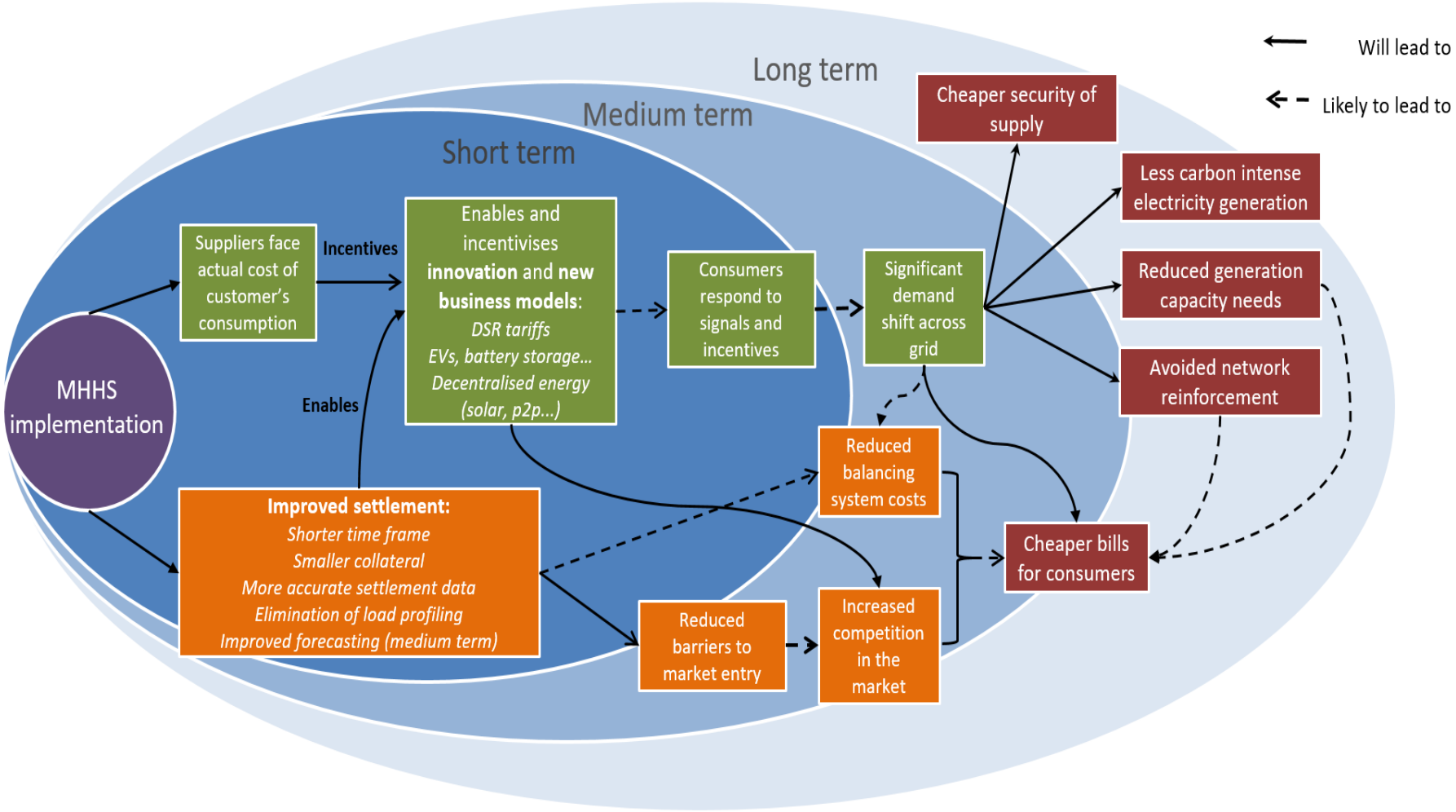
[64] https://www.ofgem.gov.uk/system/files/docs/2017/09/project_objectives_and_assessment_options_for_the_market-wide_half-hourly_settlement_business_case.pdf

[65] ie where sharing HH data for settlement was based on opt in consent

[66] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[67] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

Figure One: Benefits of HHS



2.25 It is important to note that currently, only consumption data from those classified as 'microbusinesses'[68] is treated by the Standard Conditions of Electricity Supply Licence as being sufficiently similar to domestic consumption data as to warrant specific controls on access. The consumption data of larger, non-domestic consumers is not within scope of this DPIA because consumption data for these organisations' is not considered to be personal data.

Access to data for settlement of export

2.26 Smart and advanced meters also record HH export data although this is recorded under a separate Meter Point Administration Number (MPAN). This data is a record of quantity of electricity fed back to the grid, eg from a solar panel. As set out in our TOM design principles, we have considered this in the development of the HHS TOM.[69] We are seeking views, via the consultation accompanying this DPIA, on the extent to which this data, because it reveals less about a consumer, is likely to be less of a concern than HH import (ie electricity consumption) data and whether more regulatory clarity is needed on the processing of data for export.

2.27 Some consumers are exporting to the grid without HH settled export data, creating a less accurate settlement system. Settling HH export data would correct this and strengthen the incentives placed on suppliers.

Timeframes for Ofgem's HHS project

2.28 This DPIA is focused on the decision on access to HH data for settlement purposes. The decision on access to HH data for settlement is critical in order to enable progression of the project as a whole. Specifically, clarity on the approach on access to HH data will enable:

- Progression of the second stage of the Design Working Group's settlement target operating model (TOM) detailed design work; and

- More clarity on the expected scale of benefits arising from HHS (given that levels of access to data will limit the proportion of customers who can be HH settled on the basis of their actual consumption)

2.29 ELEXON has published a planned timeframe for progressing the Design Working Group's[70] (DWG) TOM work that sets out the intention to progress the second phase of TOM design work from April 2018 – March 2019.[71] This incorporates an assumption that a final decision on access to HH data for

[68] This is defined in the Standard Conditions of Electricity Supply Licence (7A.14) as "a Non-Domestic Consumer: (a) which is a "relevant consumer" (in respect of premises other than domestic premises) for the purposes in article 2(1) of The Gas and Electricity Regulated Providers (Redress Scheme) Order 2008" or "(b) which has an annual consumption of not more than 100,000 kWh".

[69] https://www.ofgem.gov.uk/system/files/docs/2018/01/appendix_2_proposed_governance_arrangements_for_the_development_of_the_target_operating_model.pdf

[70] https://www.elexon.co.uk/group/design-working-group/

[71] https://www.elexon.co.uk/wp-content/uploads/2017/09/Design-Authority-DWG-Market-Wide-HHS-forward-planning-document.pdf

settlement is made by the end of 2018. We expect to make our decision on if, when and how to implement market-wide HHS[72] in the second half of 2019.

[72] Where HH data is available for settlement purposes

3. Options being considered to facilitate access to half-hourly electricity consumption data for settlement purposes

3.1 As set out in paragraph 2.9, we confirmed in September 2017 that we are considering the following access to half-hourly (HH) electricity consumption data for settlement options:

1. **Opt in**: Access to HH electricity consumption data for settlement purposes is subject to existing data access rules, giving domestic consumers the choice to opt-in (the status quo for domestic consumers)
2. **Opt out**: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only, unless the consumer opts out (HH data for microbusinesses is currently collected on an opt out basis)
3. **Mandatory**: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only

3.2 As outlined in the previous section, we are also considering two 'enhanced privacy' options. These options are as follows:

4a. **Anonymisation**: consumers can choose to have their data retrieved, processed and aggregated by a centralised body, rather than by suppliers and their agents, with HH data anonymised after settlement processes are complete. All consumers would be settled using their HH data under this option. [73]

4b. **Hidden Identity**: Hidden Identity: HH electricity consumption data is retrieved by a new 'pseudonymisation service'. They replace the information[74] which can be used to identify an individual with a new unique identifier – obscuring their identity, as the data can no longer be attributed to individual consumers without a key. This pseudonymised data is then processed for settlement purposes by the usual parties responsible for settlement. All consumers would be settled using their HH data under this option. [75]

3.3 Sections 2-4 of the GDPR confer a number of rights on consumers and requirements on data controllers and processors relating to:

- Information and access to personal data (section 2);
- Rectification and erasure (section 3); and

[73] Providing they have a smart or advanced meter installed
[74] A device identifier which can be linked to an MPAN (Metering Point Administration Number).
[75] Providing they have a smart or advanced meter installed

- Right to object and automated individual decision-making (section 4).

3.4 We are mindful that, whichever option is chosen, data controllers will need to be able to comply with these requirements, where relevant. Once we have confirmed which data option we have selected, we intend to publish an updated DPIA.

Option 1, Opt in: Access to HH electricity consumption data for settlement purposes is subject to existing data access rules, giving domestic consumers the choice to opt-in (the status quo)

3.5 HH data from domestic consumers will only be accessed on an opt in basis by suppliers (or where relevant, other authorised third parties). As such, the grounds for lawful processing under opt in is consent.[76]

3.6 With the exception of a small minority of suppliers that have chosen to take advantage of elective HHS,[77] suppliers are not currently using smart meter HH data for settlement purposes. Some suppliers do however, seek consent to access their smart or advanced metered customers' HH data for other purposes, for example providing those consumers with their HH data online. The proportion of customers who provide consent to share this data varies significantly by supplier.

3.7 Retaining opt in consent to access HH data for settlement purposes would therefore enable suppliers to HH settle some but not all customers on the basis of their HH data.

Option 2, Opt out: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only, unless the consumer opts out (HH data for microbusinesses is currently collected on an opt out basis)

3.8 Under this option, energy suppliers (or other licensed parties) would be under a legal obligation to process HH data for settlement purposes, unless the customer has opted out.[78] This would not affect the rules governing suppliers' access to HH data for other purposes.

3.9 This option would continue to provide consumers with the choice of whether or not to share their HH data for settlement purposes. However, it would be likely to increase the proportion of consumers who were HH settled using their HH data compared to option 1, as sharing such data would become a default rather than requiring action on the part of the consumer.

3.10 Article 6(1)(c) of the GDPR – legal obligation – provides an appropriate and sufficient ground for lawful processing by the licensed party, where obtaining consent is not feasible and proportionate. The licence conditions set by the

[76] Article 6(1)(a) of the GDPR

[77] Ofgem worked with industry to deliver a number of code changes that were completed in June 2016, which remove barriers for suppliers wishing to settle their profile 1-4 customers on a HH basis.

[78] Article 6(1)(c) of the GDPR

Gas and Electricity Markets Authority (GEMA) create a legal obligation. Breaches of any code obligations would also constitute a breach of licence conditions.[79] However, the Data Controller would need to be a licensee in its own right for this provision to be relied upon.

Option 3, Mandatory: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only

3.11 Under this option, energy suppliers (or other licensed parties) would be under a legal obligation to process HH data for settlement purposes.[80, 81]

3.12 While consumers would not have a choice over sharing this data, suppliers would not be allowed to use HH data for other purposes,[82] such as marketing and billing without the consumer's consent, in line with the DAPF.[83] This option would mean that all customers with a smart or advanced meter would be settled using their HH data.

Anonymisation

3.13 Recital 26 of the preamble to the GDPR describes anonymisation as "data rendered anonymous in such a manner that the data subject is not or no longer identifiable". Where data is considered to be truly anonymised, it is no longer classified as personal data. A useful test, as recommended by the ICO, to determine whether data is truly anonymised or not is the following: data should not be considered anonymised if a reasonably competent 'motivated intruder', who is willing to employ investigative techniques but not break the law, is likely to identify an individual from it.[84]

3.14 Where HH data from smart meters is concerned, the party retrieving data from the smart meter will receive HH data with information attached, such as a device ID, that enable the meter and therefore the associated household to be identified by a certain industry parties who have access to the relevant database.[85] It is not possible to draw data from smart meters in a pre-anonymised format due to the functioning of and security protocols associated with Data Communications Company's (DCC) systems.[86] Therefore, it would be necessary to undertake anonymisation post-data retrieval. This is similarly the case for advanced meters, which do not have functionality to

[79] Under Standard Conditions of Electricity Supply Licence 11.1 and 11.2
[80] Article 6(1)(c) of the GDPR
[81] We could select this option for domestic consumers, microbusiness consumers or both groups.
[82] We have previously stated that, for data already collected for settlement, we consider network charging as part of this work. We also note that we are requesting evidence in relation to forecasting as part of the consultation accompanying this DPIA
[83] Access to HH energy consumption data is provided on an opt in basis for domestic consumers and on an opt out basis for microbusiness consumers.
[84] https://ico.org.uk/media/1061/anonymisation-code.pdf
[85] Distribution network operator (DNOs), suppliers and their agents, and some authorised third party intermediaries can use information from the ECOES industry database to see the address associated with an MPAN.
[86] DCC provides the network for HH data retrieval

provide data in a pre-anonymised format. This potentially reduces the overall attractiveness of anonymisation because the data would, at the point of retrieval, still be considered to be personal data. We have therefore ruled out this form of anonymisation.

3.15 Following analysis by Baringa and discussions with stakeholders, Ofgem's view is that anonymisation would have to take place after data had been validated and processed to ensure that data met minimum required levels of accuracy and integrity. Baringa's report concluded, "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".[87]

3.16 Baringa's report concludes that, if a model were to be pursued which incorporated anonymisation, it would need to be undertaken by a centralised body rather than individual suppliers or their agents. This is based on the following principles:

- A degree of anonymisation can be achieved through separation (and centralisation) of settlement functions for a subset of customers

- 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 suppliers.

3.17 Ofgem originally discussed the use of anonymisation combined only with option 3. However, following Baringa's analysis, we have now concluded that true anonymisation of settlement data would not be proportionate. Baringa's anonymisation model requires HH data to be processed by a central body where consumers opt for enhanced privacy. Therefore, this option is best represented as a hybrid of options 2 and 3: there is a legal obligation to process HH data for settlement, but consumers do have a choice to opt out of supplier and supplier agent processing of their data in favour of processing by a centralised body.

Hidden Identity (formerly 'Pseudonymisation')

3.18 Article 4(5) of the GDPR defines pseudonymisation as "the 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." Pseudonymisation is described by the ICO as carrying a "greater privacy risk [than anonymisation] but not necessarily an insurmountable one".[88] It would however, provide more privacy for consumers than option 3.

3.19 Where settlement is concerned, pseudonymisation of data would mean that a designated party[89] would be responsible for replacing information supplied with HH data that could be used to identify an individual household (for

[87] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[88] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

[89] If we decide to pursue this option, we would need to address governance and design issues, including how the designated party would be appointed

example the MPAN), with a unique identifier known only to the party responsible for pseudonymisation and the supplier meter registration agent (SMRA).[90] All other parties handling the consumption data for settlement purposes would receive only the pseudonymised data with personal identifiers removed.

3.20 Ofgem originally discussed the use of hidden identity combined only with option 3 (there is a legal obligation on the party responsible for settlement to process HH electricity consumption data[91] for settlement purposes only). Theoretically, hidden identity could be combined with any of the options under consideration, but in practice, we think that pseudonymising would be most beneficial if it enabled all consumers with a smart or advanced meter to be HH settled (therefore combined with option 3 above).[92] This conclusion was reached based on the following reasons:

- Hidden identity would be most beneficial for consumers who have a concern about their data being processed for settlement purposes.
- Pseudonymising data for customers who opt in to sharing would introduce a layer of privacy that was not considered appropriate or necessary when the original DAPF was established.[93]
- Pseudonymising data for customers who have not opted out of sharing data seems unlikely to have a large impact on opt out rates (because of the difficulty of explaining the technicalities simply to consumers), and would not be necessary for those who are content for their HH data to be used for settlement purposes.

3.21 If we decide to proceed with hidden identity, we will need to consider which of the following models is most beneficial from a consumer privacy and from a system efficiency perspective:

- HH data from all consumers is pseudonymised regardless of their preferences about sharing HH data
- HH data is only pseudonymised where consumers indicate that they would prefer their identity is hidden/pseudonymised

3.22 HH data would be retrieved from smart meters for settlement purposes and subsequently pseudonymised for some or all consumers.

3.23 A potential downside of hidden identity is that if data was pseudonymised regardless of data sharing preferences, suppliers and other parties would not be able to use the pseudonymised data for purposes other than settlement even if they had the right consent from the customer. HH data would therefore potentially need to be retrieved and validated separately by the supplier if consent had to be obtained to retrieve data for billing or marketing purposes.

[90] This is the model proposed in the report prepared for Ofgem by Baringa. We would need to consider design in more detail if we decide to proceed with the hidden identity option.
[91] Henceforth referred to as "HH data". Where we discuss export data, we specify this.
[92] More detail can be found in Baringa's report https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes
[93] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

3.24 If this option were to be pursued, Ofgem would need to consider whether this should be applied only to domestic consumers or also extended to microbusiness consumers.

4. Flows of Information in Settlement

To properly assess the risks associated with policy change, Data Protection Impact Assessment (DPIA) best practice recommends organisations map out how and where data flows. We are only considering data flows relevant to domestic and microbusiness consumers.

4.1 In both the current and proposed half-hourly settlement (HHS) arrangements, there are four main procedures applied to half-hourly (HH) data:

- Retrieval: The process of accessing and retrieving consumption data (import) and export from meters
- Load shaping: Also known as load profiling, this is the process where a consumption pattern (or shape) is applied to a long-term meter reading to estimate more granular consumption (eg HH) of a consumer, for example when the actual HH data for a particular period(s) is not available;
- Processing: Validating and estimating consumption data, providing data to relevant parties, exception[94] reporting, and estimation; and
- Aggregation: Where settlement period data is aggregated for use in settlement.

4.2 Those parties with access to HH data during the settlement process in the existing system and those potentially having access in a future system are:[95]

- Supplier: A party which holds a supply licence and is responsible for import or export for a given Meter Point Administration Number (MPAN);
- Supplier agents: Under certain circumstances, they perform some or all of the activities listed in 4.1, above, including reading meters, validation, processing and aggregating consumption data, fixing problems with meters and estimating as required. Some suppliers use in-house supplier agents (also known as integrated supplier agents);
- Central agent[96]: Potentially replaces supplier agents and carries out settlement function/s for the whole market, eg processing and aggregation; and
- ELEXON: Receives aggregated meter volume data by supplier by Grid Supply Point (GSP) Group[97] and other elements, eg consumption component class, applying correction and calculating Balancing Mechanism Unit volumes

[94] Issues which occur that limit the accuracy of settlement data on either a transitory or permanent basis
[95] The responsibilities included here are a summary and not a comprehensive list of those held by these parties
[96] The involvement of a centralised body in this process – besides DCC – is dependent upon the outcome of our work on whether or not to centralise functions currently performed by supplier agents
[97] A distribution network region, as defined under the BSC

4.3 We have mapped out data journeys for the existing and future settlement systems below.

Use of HH data in the current system

4.4 In summer 2017, we concluded our work on elective HHS, allowing those suppliers wanting to HH settle their customers to do so cost-effectively.[98]

4.5 HH data processed for Elective HHS is currently retrieved from smart meters through an authorised third party before being passed to suppliers or, where appropriate, their agents for processing then aggregation, ahead of submission to central settlement systems.

4.6 HH data retrieved for the purposes of elective HHS is then processed and aggregated for submission to central settlement systems.

Variables and decisions affecting future data journeys

4.7 In the context of settlement, a number of variables and future decisions will determine how data moves around the future settlement system. These variables and future decisions are described in this section.

4.8 The meter type from which the data originates, whether smart[99] or advanced,[100] dictates how data is retrieved, as described at paragraph 4.5 in respect of smart meters, and by supplier agents in respect of advanced meters. Settlement arrangements for each meter type will differ by TOM, as shown in figure 2.

4.9 The decision on the access to HH electricity consumption data[101] options will determine whether anonymisation or hidden identity are used to further protect consumers' data. Incorporating one of these privacy by design solutions would add steps to the settlement process.

4.10 Consumers can therefore fall into a number of different potential categories:

- Those with smart meters settled using HH data
- Those with smart meters settled using register reads[102]
- Those with advanced meters settled using HH data
- Those with advanced meters settled using register reads
- Those with traditional meters settled using register reads

[98] Provided they have the necessary consents from their customers to access their HH data

[99] Smart meters are being offered to all domestic consumers in GB by the end of 2020. Suppliers are also required to offer smart meters to small non-domestic (profile class 3 and 4) consumers. This is subject to certain exceptions, which allows for an advanced meter to be installed instead of a smart meter (see Standard Conditions of Electricity Supply Licence for further details).

[100] Advanced meters are those with remote read and HH consumption recording capability. Some but not all non-domestic customers with profile class 3-4 sites will have advanced meters, in accordance with the exceptions in the Standard Conditions of Electricity Supply Licence.

[101] Henceforth referred to as "HH data". Where we discuss export data, we specify this.

[102] Register Readings are the meter readings obtained from meter's tariff registers. This could be the cumulative register or the meter's time of use registers.

4.11 For those consumers settled using register reads, HH data will not be retrieved from their smart/advanced/traditional meter for settlement purposes. We do not therefore consider this group further in this section because we do not anticipate that there would be any privacy impacts for this group resulting from market-wide HHS. Nevertheless, the size of this NHH settled group does impact the HHS benefits that can be achieved and the costs of administrating the settlement system, so it does come into consideration in our decision on access to HH data.

4.12 As part of the HHS project, we are gathering evidence and working with stakeholders to decide whether functions currently performed by supplier agents should be centralised or not. The CMA's Energy Market Investigation recommended that we should consider the cost-effectiveness of alternative designs, such as a centralised entity. The outcome of this decision will determine whether competitive agents, a centralised body or several centralised bodies will be responsible for processing and aggregating HH data.[103]

4.13 Market-wide HHS is a step-change relative to previous arrangements, as well as an enabler of new business models. ELEXON is chairing a Design Working Group that has developed five skeleton TOM designs; ELEXON has consulted on these TOM designs.[104] Ofgem will make the final decision on which of the skeleton TOMs to take forward. The implications of the selected TOM on HH data flows is shown in figure 2 and described below. The minimum criteria we set for TOM designs require that, among other things, they do not preclude any of the access to HH data options.[105]

4.14 The economic case for market-wide HHS, which is being evaluated through the market-wide HHS Business Case, will be affected by the proportion of customers' HH data that is available.

Data flows under TOMs A-E for smart and advanced meters

4.15 Movement of data between different parties in the settlement system differs for smart and advanced meters across all five TOMs, as shown in figure 2. Similarly, different parties have access to HH data for settlement at different stages. This varies across TOMs. This also varies across suppliers, for example, some currently choose to sub-contract certain settlement activities to supplier agents while others do this using in-house agents (also known as integrated supplier agents).

4.16 Retrieval and processing for advanced meters are separate services to retrieval and processing for smart and traditional meters in every TOM, with advanced meter aggregation services separated from smart and non-smart in TOMs B and C. Aggregation either takes place cross-market (TOMs A, D, and E) or alongside retrieval and processing (TOMs B and C). In all cases, aggregated data is passed on to ELEXON, for Supplier Volume Allocation.

[103] If Ofgem decides to offer anonymisation for some customers it may be that a central body processes HH data for this group while other consumers' data is processed by a competitive agent

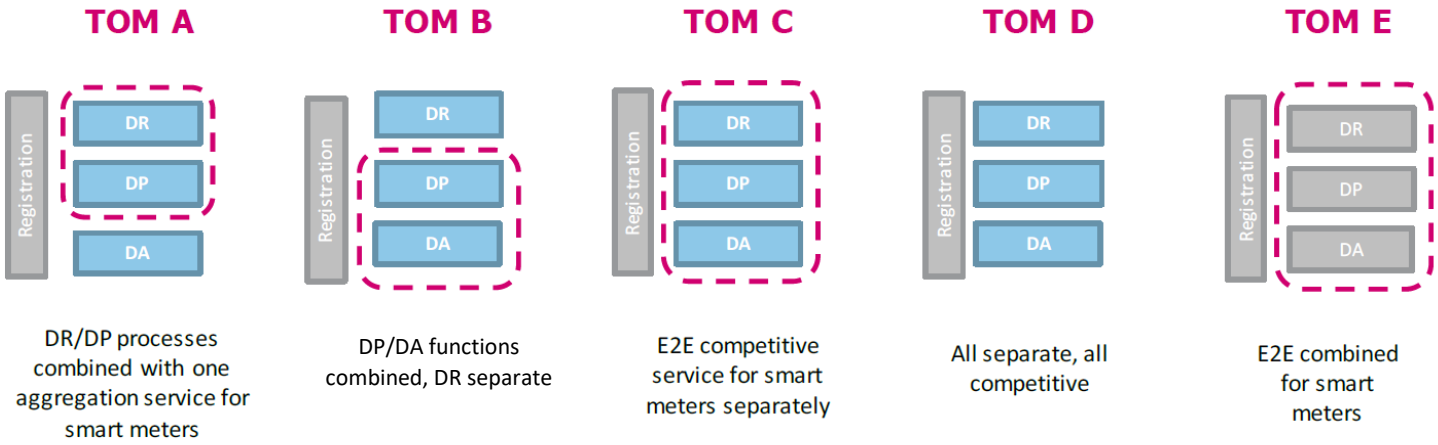
[104] This consultation has closed. The consultation can be found here: https://www.elexon.co.uk/wp-content/uploads/2018/03/DWG_Draft_TOMs_for_Evaluation_v1.0.pdf; published responses can be found here: https://www.elexon.co.uk/wp-content/uploads/2018/03/DWG_Draft_TOMs_for_Evaluation_v1.0.pdf

[105] https://www.ofgem.gov.uk/system/files/docs/2018/01/appendix_2_proposed_governance_arrangements_for_the_development_of_the_target_operating_model.pdf

4.17 Figure 2 does not include NHH data, the route for which is the same across all TOMs, but differs to the existing NHH process. For consumers with smart or advanced meters who have not chosen to share their HH data, or where this data cannot be accessed, eg due to communication software issues, NHH data is retrieved in the same way as HH data from these meters. For NHH data from traditional meters, this is retrieved by a meter reading service which passes register reads, depending on the TOM, to a Retrieval and Processing service (TOM A and E), Processing and Aggregation Service (TOM B), Retrieval, Processing and Aggregation Service (TOM C), or a Processing Service (TOM D). Wherever processing occurs in the TOMs below, the load shaping occurs alongside this.

4.18 If we decide to integrate enhanced privacy solutions, ie anonymisation or hidden identity/pseudonymisation, a designated party would be tasked with anonymising or pseudonymising consumers' HH data. In the case of anonymisation, following analysis by Baringa and discussions with stakeholders, Ofgem's view is that this party would be likely to carry out all settlement functions for consumers participating in anonymisation and submit data to ELEXON.[106]

Figure Two, overview of TOMs A-E for smart metered consumers



Transmitting, storing and deleting HH data as part of the settlement process

4.19 Transmission of HH data from smart meter to data retriever[107], via the DCC takes place through user systems purpose-built for communicating with DCC's systems. The user systems have to be compatible with the certificates issued by the Smart Metering Key Infrastructure,[108] and therefore securely transmit data from smart meters to DCC Users.

[106] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[107] The data retriever must be a DCC user

[108] https://www.smartdcc.co.uk/implementation/design-and-assurance/key-infrastructures/smart-metering-key-infrastructure/

4.20 Transmission of HH data between organisations party to the Balancing and Settlement Code (BSC) is governed by the BSC. This transmission has to take place across a BSC Panel-approved data network.[109] The Data Transfer Catalogue,[110] which forms part of the governance arrangements of the Master Registration Agreement[111], also determines, in part, data transfer practices.

4.21 The settlement timetable currently lasts for 28 months, including dispute runs. If the current timetable were retained, it would be likely to be necessary to retain individualised HH data for this time-period in case it is needed for dispute runs. One of the aims of settlement reform is to significantly shorten the settlement timetable.[112]

4.22 The length of time suppliers, which at present predominantly use HH data for non-settlement related purposes, retain HH data (collected with the consumer's opt in consent) varies significantly. A number of suppliers have highlighted that they are reviewing or have reviewed their current data storage policies in light of the GDPR. The GDPR states, "Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".[113] It is therefore important that consumers' HH data, for whatever purpose it is retrieved, is only retained for as long as it is strictly necessary to do so.

4.23 We anticipate that all suppliers will want to review how they handle personal data to satisfy themselves that they are compliant with the GDPR and the new Data Protection Act.

4.24 Storage and deletion of settlement-relevant data in the future settlement system will have to conform to relevant sections of the SEC, where this data has been retrieved through the DCC, as well as GDPR requirements. In addition to principle e) above, notable requirements include GDPR article 13, 2.(a), which requires that data controllers provide data subjects with "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period".

4.25 It is likely that suppliers will need to store data for the duration of the settlement timeframe. As stated before, we expect one of the benefits of market-wide HHS will be to significantly reduce the length of the settlement timeframe.

4.26 A number of best practice codes and certifications are relevant to this area, including the ICO's Data Sharing Code of Practice. Some suppliers are also ISO27001 certified. This certification specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation.[114]

---

[109] https://www.elexon.co.uk/wp-content/uploads/2011/10/section_o_v3.0.pdf

[110] https://dtc.mrasco.com/Default.aspx

[111] The Master Registration Agreement provides a governance mechanism to manage the processes established between electricity suppliers and distribution companies to enable electricity suppliers to transfer customers

[112] https://www.ofgem.gov.uk/system/files/docs/2017/07/electricity_settlement_reform_significant_code_review_launch_statement.pdf

[113] Article 5, principle e)

[114] https://www.iso.org/standard/54534.html

5. Privacy and related risks

In this chapter, we consider privacy risks affected by the change to market-wide Half-Hourly Settlement (HHS), regardless of the access to half-hourly (HH) electricity consumption data option we choose to pursue, as well as the likelihood and potential harm of these risks.

Chapter 6 considers privacy and security risks in relation to our access to HH data electricity consumption for settlement purposes options. Chapter 8 provides a more detailed assessment of the extent to which privacy risks are mitigated in the access to HH electricity consumption data[115] options under consideration

In coming to a decision on access to HH data for settlement, we will consider the proportionality of each privacy option in the context of the costs that it may incur and the extent to which we would expect benefits to be realised. We discuss this in chapter 2, paragraphs 2.13-2.19, chapter 9, and in the consultation accompanying this DPIA.[116]

Risk 1: Security Risks: Unauthorised parties access and use, amend or delete HH data

Risk overview

5.1 Robust security provisions are in place in relation to smart metering. However, as with all systems, there are risks. Here we consider the risk that unauthorised parties could potentially access and use, amend or delete HH data while it is being moved between parties (data-in-transit) or while it is being held by a supplier or agent that has obtained the data legitimately (data-at-rest). Given that some suppliers already access HH data from smart and advanced meters for specific purposes, this risk already exists. However, market-wide HHS is likely to significantly increase the volume of HH data being retrieved from smart and advanced meters and the number of parties that process this data.[117]

5.2 Security of HH data is subject to a number of regulatory controls that are set out more fully in the existing mitigation section below.

5.3 The level of risk is likely to depend on the quality of the data controller or processor's security systems. Obvious areas for consideration include:

- How data is stored – for example, is it stored with name and/or

[115] Henceforth referred to as "HH data". Where we discuss export data, we specify this.

[116] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[117] The volume of data and number of parties processing will depend on the final access to data decision, the TOM design, the decision on whether or not to centralise functions currently performed by supplier agents and the number of parties currently handling HH data on a supplier's behalf.

address data attached or with a unique identifier such as an MPAN?[118]
- How is internal access to data controlled?
- Where data is stored
- How data is protected
- How data is moved

5.4 There are a number of types of risk to security of information. These are:

- **External threat** – Risk that data could be maliciously obtained (eg by a hacker) or accidentally lost[119] then used, amended or deleted

- **Insider threat** – An individual who has legitimate access to HH data could maliciously or accidentally amend or delete HH data. Alternatively, an individual working for an organisation that holds HH data but who does not personally have permission to access HH data could gain access to the data, for example through phishing or obtaining a password.[120]

5.5 Our belief is that HH data is likely to be of limited use to those looking to exploit or otherwise financially gain from its misuse when compared to other types of personal data. Data covering a reasonable period of time would reveal general information about a household's normal consumption pattern which could, for example, provide information on patterns of behaviour.

5.6 This data could potentially be obtained and used to target unwanted marketing. Commercially, HH data is likely to be most useful to companies operating in the energy sector. For example, to identify consumers with certain profiles. However, such companies will normally have more conventional means to access this data via the DCC. This would be unauthorised access to data if it was retrieved without a legal basis for doing so, but would not constitute a security breach of DCC's systems because the misuse came from a party that could legitimately access DCC systems.

5.7 For non-energy related marketing purposes, we think that the value of HH data is likely to be significantly lower than other types of personal data such as social media profiles or medical records that can reveal far more detailed and sensitive information about an individual. This view is supported by evidence from a recent Ofgem consumer survey, where 96% of consumers ranked electricity consumption data outside of their top three most sensitive forms of personal data of the nine categories considered, while 49% of consumers placed it in their bottom three.[121] Other forms of personal data considered included medical records, location data and financial records.

5.8 There may potentially be a risk that HH data, where it belongs to a high profile individual, could be used to gain some insight into their lifestyle. However, the gain to a malicious party from doing this may be relatively

[118] As previously highlighted, an MPAN is personal data because it is possible to link an MPAN to an address. However, restrictions on access to databases that enable identification of an address from an MPAN mean that storing data with an MPAN rather than an address would provide some protection.
[119] For example, where an employee accidentally leaves a data storage device in a public place
[120] This risk overlaps with data misuse risks discussed in the next section. Insider amending or deleting of data are covered in the security section. Insider misuse of data is covered in the security section if such misuse is unrelated to the organisation and its interests.
[121] https://www.ofgem.gov.uk/publications-and-updates/consumer-views-sharing-half-hourly-settlement-data

limited given that only general information on historic electricity consumption can be gleaned from HH data.

External Threat – Risk that data could be maliciously amended or deleted

5.9 It is possible that HH data could be targeted in order to damage or disrupt the settlement system itself. For example, an unauthorised party could seek to delete or manipulate data to undermine the accuracy of information in the settlement system. This could be done at scale or to target one specific individual. If data was amended or deleted it could be re-retrieved from the meter[122] as long as the data controller/processor was able to detect that the security breach had occurred or if the data failed validation.

5.10 If the objective of such an intrusion was to increase the bill of a particular individual then it could theoretically be possible to do this. However, this appears to be a relatively difficult and obscure method of causing harm to an individual. If the objective was broader system disruption then such harm could probably be rectified by re-retrieving the data or using profile data to fill gaps. In both scenarios, the effort needed to gain access to the data may be disproportionate to the harm that could be caused. There are likely to be more straightforward and obvious ways of causing harm to either an individual or the system.

Internal Threat – Risk that data could be maliciously amended or deleted[123]

5.11 Individuals working for a supplier or supplier agent could potentially amend or delete data in order to deliberately cause harm to settlement systems or to consumers' interests. This data could potentially be transferred to external parties with malicious intent or by accident. Such individuals may not have permission to access the data and may have gained access for example by obtaining a colleague's password or due to negligence.

5.12 As with other risks described above, there may be limited incentives for individuals to do this in practice. If an external party had a strong reason to obtain the data then they could potentially bribe an employee to cooperate. However, it is doubtful whether the value of the data is high enough to warrant an external party going to such lengths and whether an employee would wish to risk their career by participating in such an activity.

Legal Requirements

5.13 Parties who handle HH data are subject to a number of legal requirements that relate to security. The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures be used.[124]

[122] Data is stored on smart meters for 13 months so data over 13 months old would not be able to be re-retrieved.

[123] Internal misuse of data is covered in the privacy risk section below

[124] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/

5.14 In practice, Ofgem expects that parties that handle HH data will take steps to ensure that they have assessed risks and put in place appropriate security measures. Appropriate measures, which may in some cases be legal requirements, can include some or all of the following:

- Carrying out a Data Protection Impact Assessment (DPIA)[125]
- Carrying out a threat assessment
- Achieving compliance with the 'Cyber Essentials' or ideally 'Cyber Essentials Plus[126]' security standards
- Considering whether to carry out independent 'penetration testing' to a standard recommended by the National Cyber Security Centre[127].
- Putting in place a vulnerability management programme to continuously monitor and respond to vulnerabilities
- Considering whether achieving ISO27001 certification would be appropriate

5.15 The ICO advises "organisations must do a DPIA for certain types of processing, or any other processing that is likely to result in a high risk to individuals".[128] The Article 29 Working Party includes representatives from the data protection authorities of EU member states. It has set out nine criteria that may be associated with high risk processing. These include "data processed on a large scale" and "innovative use or applying new technological or organisational solutions".[129]

5.16 Alongside the GDPR[130], several other legal frameworks place requirements on parties involved in settlement where data and system security are concerned. The following all place minimum security system requirements on relevant parties to protect against unauthorised access to data and security breach more generally:

- Network and Information Security Directive (2016);[131]
- Smart Energy Code (SEC);[132]
- Standard Conditions of Electricity Supply Licence;[133] and
- Balancing and Settlement Code (BSC).[134]

5.17 Moreover, SEC Users, which includes suppliers, are required to put in place and maintain arrangements in accordance with Good Industry Practice in regards to the energy consumer to which the data relates (I1.5 of the SEC).

---

[125] This is a GDPR requirement under certain circumstances

[126] Cyber essentials plus involves on premises testing and is therefore more thorough than the basic cyber essentials standard.

[127] https://www.ncsc.gov.uk/scheme/penetration-testing

[128] https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf

[129] https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf

[130] Under Article 32, Recital 1.(b), amongst others

[131] See: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[132] Section G3.3(c). See: https://smartenergycodecompany.co.uk/download/4676

[133] Conditions 46 and 46A are relevant to this end, with the former stating, among other things, that licensees "must take such steps and do such things as are within its power to provide that the Supplier End-to-End System is at all times secure"

[134] See Section O3.4.2, which states "Each Party […] shall take all reasonable steps to prevent unauthorised access to a Communication or Communications Medium"

5.18 These requirements cover varying portions of the settlement process, with some notable overlap. Moreover, they apply to a range of parties in the process. We are content that there are no gaps in the parties covered. Moreover, in combination, these frameworks serve to significantly reduce the risk of security breaches and unauthorised access to data.

5.19 Some of these frameworks also put in place monitoring and reporting requirements:

- Under SEC,[135] all DCC Users, including suppliers, are required to "maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the DCC and each such User to demonstrate that it is complying with its respective obligations under Sections I1.2 to I1.5 and I1.7".
- All parties to the BSC are required[136] to notify the BSC Code Operator and relevant BSC Agent if they become aware of a breach of security in relation to a Communication.[137]
- GDPR requires[138] that data controllers shall, without undue delay, notify relevant supervisory authorities in the event of personal data breaches that are likely to result in risk to the rights and freedoms of individuals.
- GDPR requires[139] data controllers to carry out an assessment of the envisaged processing operations on the protection of personal data, and particularly when using technologies and where the processing is likely to result in a high risk of infringing the rights and freedoms of a natural person or persons.

5.20 Non-compliance with the SEC can mean, for licensed parties, breach of licence. The Gas and Electricity Markets Authority (GEMA) may impose financial penalties of up to 10% of a licensee's turnover, make consumer redress orders and issue provisional/final orders, where appropriate, for breaches of relevant conditions and requirements under the Gas Act 1986 and the Electricity Act 1989.[140]

5.21 If an organisation is found to be non-compliant with the GDPR, the ICO can levy fines of up to €10m (or 2% of total worldwide annual turnover[141]) or €20m (or 4% of total worldwide annual turnover[142]) depending on which provision/s has/have been infringed.

5.22 The Network and Information Systems directive requires member states to ensure that operators of essential services, including in the energy sector, take appropriate measures to manage security risks to their network.[143] Penalties associated with this directive are to be laid down by EU member states in provisions adopted as a result of this directive. Government has consulted on a proposed penalty regime and issued a formal response to

[135] Section I1.8
[136] Under section O3.4.3
[137] A Communication, under the BSC, includes half-hourly consumption data
[138] Under Article 33, Recital 1.
[139] Under Article 35, Recital 1.
[140] https://www.ofgem.gov.uk/sites/default/files/docs/2014/11/financial_penalties_and_consumer_redress_policy_statement_6_november_2014.pdf
[141] Whichever is higher
[142] Again, whichever is higher
[143] Article 14, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

this, outlining its intentions ahead of implementation.[144]

5.23 As described above, existing legal frameworks require parties handling personal data to have robust security measures in place. The size of the security risk will vary slightly depending on the access to HH data option that Ofgem chooses. We assess the level of risk associated with each access to HH data option in chapter 6 below.

Overall assessment of risk

5.24 We consider that the relevant factors in assessing security risks to HH data are:[145]

a) the ease with which a party could potentially maliciously obtain, amend or delete HH data;
b) the extent of harm which could be caused; and
c) strength of incentives to do so.

5.25 Alongside actual harm to consumers, a security breach could potentially undermine consumers' confidence that their HH data is secure. This could have a knock-on effect on willingness to accept a smart meter or share HH data for any purpose.

5.26 While it would be possible to cause some harm by obtaining, amending or deleting HH data, in comparison to other types of personal data we think that the potential harm to individuals or the system would be fairly limited in comparison to the likely effort required to access the data. This effort would be likely to include not only obtaining the HH data, but also identifying with which address a particular MPAN is associated, unless HH data was stored with addresses and names already with it.

5.27 As we have set out above, there are a number of robust requirements on parties handling HH data to maintain minimum standards of security. This is particularly the case since the GDPR came into force in May 2018.

[144] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf

[145] We explain our risk assessment methodology at the beginning of chapter 6.

Risk 2: Suppliers, agents or other parties misuse HH data

5.28 There is a risk that suppliers or other parties with access to HH data will:

a) Retrieve data for which they do not have lawful basis for processing or
b) Retrieve data that they do have lawful basis to process (eg for settlement) but use it for purposes for which they do not have lawful basis to process (eg marketing)

5.29 If they choose not to comply with licence conditions and data protection legislation, suppliers could already technically access their customer's HH data from smart or advanced meters without appropriate consent. However, in doing so they would risk significant penalties and reputational risk.

5.30 HHS will place new requirements on suppliers to settle consumers HH. We anticipate that incentives to misuse data will rise as a result of HHS.

5.31 Once HHS is introduced, suppliers will face differentiated costs for consumers depending on their electricity consumption at different times of day.

5.32 Any change to the rules on access to HH data resulting from Ofgem's policy decision will be applicable to settlement only.[146] Suppliers will therefore still be required to obtain opt in consent from their customers in order to use data for other purposes, such as billing[147] and marketing, in line with the DAPF.

5.33 Specifically, activities for which the supplier would need separate consent would include using an individual's HH data:

- to compare costs incurred in supplying electricity to a property with payments for electricity (this falls under billing) and therefore assess the level of profit or loss linked with that customer;
- to make price-related (or other) decisions about consumers;
- to market specific tariffs based on a customer's consumption pattern; and
- to design new time of use type products.[148]

5.34 If we decide to implement market-wide HHS, suppliers will have a financial incentive to encourage their customers to allow their HH data to be used for some or all of the purposes described above. For example, to identify which customers are more or less expensive to serve and to offer tariffs accordingly.

5.35 While many consumers could benefit from tariffs tailored to their consumption pattern, for example if they had low peak consumption, others could lose out if a supplier identified that they were a high cost customer and responded by offering them a significantly higher priced tariff.

[146] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486352/DAPF_Consultation_Response.pdf

[147] Using HH consumption data and all other relevant information to calculate and prepare a bill or statement of account to a customer of account and the collection and use of information relating to the consumption of electricity.

[148] However, suppliers would be able to use aggregated data for this purpose

5.36 HHS will therefore potentially[149] mean that suppliers legitimately retrieve some or all of their customers' HH data but for a sub-section of these customers, are only allowed to use it for settlement purposes.

5.37 There are other risks that are increased by the introduction of HHS. For example, the incentive for suppliers to use HH data for marketing or billing without authorisation will likely be greater if consumers' data is on the supplier's system rather than just on the meter.

Categories of misuse

5.38 Misuse of HH data could occur for one of two reasons:

- A deliberate decision by a company or their employee/s to retrieve and use data for purposes they do not have grounds to lawfully process;[150] or
- Ignorance of the regulatory framework.

Deliberate misuse of data

5.39 In this case, a company or individual/s within a company would make a decision to misuse data in full knowledge of the fact that they were in breach of the regulatory framework.

5.40 A number of energy suppliers have told us that companies would be very unlikely to deliberately misuse data given the potentially very large financial penalties for doing so[151] and the associated reputational risk.

5.41 Individuals working for an organisation could potentially identify a benefit to themselves or their team, for example to meet or exceed targets or increase profits, by using HH data for purposes for which they do not have consent. The risk of individuals within a company misusing data may be higher than a company level decision to do so, however, the ICO does have powers to fine individuals in breach of data protection laws.[152] We also note that in some situations, a court might choose to hold an employer liable for the actions of an employee.

Ignorance of regulatory framework

5.42 Staff working for a company, driven by the incentives described above, may use HH data for certain purposes without realising that by doing so they are in breach of the regulatory framework.

5.43 Employers have a duty to ensure that staff who have an opportunity to

[149] If the target operating model chosen requires suppliers to retrieve data rather than data going direct to central or supplier agents.

[150] This is similar to the internal threat risk described under the security risk section of this DPIA. However, this risk is classified as a privacy and not a security threat because it is carried out by an internal party in the interest of the company rather than by an internal party against the interests of the company, as is the case where security risks are concerned.

[151] See paragraphs 5.20-5.22

[152] Under sections 161-166 of the Data Protection Bill. See https://services.parliament.uk/bills/2017-19/dataprotection.html. See also https://ico.org.uk/action-weve-taken/enforcement/

handle personal data are informed about legal requirements relevant to handling that data. Such a breach would indicate that the organisation was not complying with obligations where data handling was concerned.[153]

5.44 This type of breach could also indicate that the organisation did not have robust procedures to control internal access to data and therefore limit opportunities for misuse and/or security breaches.[154]

Legal Requirements and Risk Mitigation

5.45 The GDPR contains several provisions aimed at preventing data misuse by data controllers and data processers. The following legal requirements place requirements on those handling personal data.

- Principle b) states that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". Breach of the basic principles of the GDPR can carry a fine of up to €20m or 4% of group annual global turnover.

- Parties are required, under GDPR article 33, to notify the ICO of data breaches where it is likely to result in a risk to the rights and freedoms of individuals. Breach of article 33 can carry a fine of up to €10m or 2% of group annual global turnover.

- Suppliers and other parties handling HH data will be required under the GDPR to appoint a Data Protection Officer (DPO) where their core activities require large scale, regular and systematic monitoring of individuals.[155] The DPO will have a number of responsibilities which include "*monitor[ing] compliance with the GDPR and other data protection laws, and with data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits".* The DPO must be independent, adequately resourced and report to the highest management level, advising on data protection obligations.[156]

5.46 The requirements for supplier access to data under the Data Access and Privacy Framework was implemented through the Standard Conditions of Electricity Supply Licence. This requires that suppliers obtain (opt in) consent from consumers in order to use their HH data for marketing purposes. Breach of these rules could represent breach of the SLCs, for which we would consider whether to take action against that supplier.[157]

5.47 If a SEC party is found to be misusing personal data, they could potentially be in default of the SEC, ie non-compliance. The SEC Panel is required to notify DCC, the Party and Ofgem when a Party is found to be in default of the SEC. The SEC Panel can take a number of additional actions against parties

[153] See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
[154] https://www.cyberessentials.ncsc.gov.uk/advice/
[155] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
[156] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/
[157] https://www.ofgem.gov.uk/system/files/docs/2017/10/enforcement_guidelines_october_2017.pdf

in this situation, such as requiring the party to put a remedial action plan in place, suspending its rights under SEC,[158] or expelling them from the SEC.[159]

5.48 We also note the monitoring and reporting requirements listed under 5.19, above, and the sanctions associated with contravention of these frameworks.

5.49 Ofgem currently requires some suppliers to provide information relating to the installation of smart meters. The focus of information requested from suppliers may change as the smart meter rollout nears completion. As part of any potential change, we would need to consider how to continue to monitor supplier communications in relation to processing HH data and supplier behaviour where approaches to gaining consent to access and use HH data from smart and advanced meters is concerned. On the basis of such an evaluation, we may choose to conduct additional compliance monitoring to supplement or replace existing measures.

5.50 The ICO's Data Sharing Code of Practice[160] is a collection of good practice recommendations that data controllers can adopt to reduce the likelihood of this risk occurring.

Overall assessment of risk

5.51 It would be relatively easy for a supplier or other party with access to HH data to use the data for purposes for which they, either deliberately or through negligence, did not have grounds for lawful processing.

5.52 However, suppliers are required to adhere to licence conditions and other relevant regulatory frameworks, in particular the GDPR, and such misuse of data could be a clear breach of both regulatory frameworks. Financial consequences of breaching such rules could be significant and therefore act as a strong deterrent. In addition, any supplier found to have deliberately misused data would be likely to suffer significant damage to its reputation. This damage could negatively impact levels of trust in suppliers more generally.

5.53 Assessing this risk is challenging because the severity would depend on the scale of any breach – considering factors including but not limited to the number of customers affected and the harm, or potential harm, they suffer or are exposed to. Where a breach is detected, we will consider enforcement action based on the criteria set out in our enforcement guidelines.[161]

5.54 The decision on whether or not to centralise functions currently performed by supplier agents may impact on the assessment of risks above. Suppliers may have less temptation or opportunity to misuse data or accidentally misuse data if HH data is retrieved and processed by another party, eg a central body, and therefore suppliers only retrieve and handle such data if they have opt in consent to do so.

5.55 However, a similar level of mitigation could potentially be achieved if the current supplier agent model is retained and data went directly to agents rather than via suppliers. This would depend on the extent of ring-fencing

[158] Specifically, those under section M8.5 of the SEC, and one or more rights under section M8.6

[159] In accordance with Section M8.10

[160] https://ico.org.uk/media/1068/data_sharing_code_of_practice.pdf

[161] https://www.ofgem.gov.uk/system/files/docs/2017/10/enforcement_guidelines_october_2017.pdf

among suppliers and agents, particularly where in-house agents are concerned.

6. Privacy risks of specific access to half-hourly electricity consumption data options

In this section, we evaluate the level of risk that we think is likely to be associated with each basic policy option under consideration. We then consider, drawing on evidence from Baringa's report,[162] the extent to which enhanced privacy options could mitigate risks. Finally, we consider how privacy implications of different options can be weighed up against broader evaluation criteria. These include cost implications and the extent to which the intended benefits of HHS would be realised under each option.

Consumers' attitudes

6.1 Research on consumers' attitudes towards sharing half-hourly (HH) data with DNOs for network planning and management purposes[163] suggested that consumers can generally be split into four groups where attitudes towards sharing data are concerned:

- **Happy to share** – relaxed about public sharing of own information in most cases
- **Quid pro quo** – comfortable sharing their data where personal value to them of doing so is clear
- **Depends who's asking** – comfortable sharing their data where value of doing so is clear (whether this is of benefit to them or others)
- **Big brother** (smallest group) – reticent towards any sharing of their data

6.2 This research, by Ipsos MORI, indicated that some consumers would be less willing to share their data with suppliers than with DNOs, particularly if they felt that this information could be used for differential pricing.

6.3 Alongside this DPIA, we have published two pieces of research[164,165] that we commissioned to inform our decision on access to HH electricity consumption data[166] for settlement purposes. The first of these is a nationally representative survey of circa 1,467 consumers. The second is a report on the findings of the third wave of Ofgem's 2018 Consumer Panel. The Consumer Panel is a series of focus groups held in different locations across GB.

[162] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[163] http://www.energynetworks.org/assets/files/Ipsos%20MORI%20Report%20DNO%20Use%20of%20HH%20Data%20-%20FINAL%2016-03-17.pdf

[164] https://www.ofgem.gov.uk/publications-and-updates/ofgem-consumer-first-panel-year-9-wave-3-half-hourly-settlement

[165] https://www.ofgem.gov.uk/publications-and-updates/consumer-views-sharing-half-hourly-settlement-data

[166] Henceforth referred to as "HH data". Where we discuss export data, we specify this.

6.4 A standout finding from the survey is that 65% of consumers would be willing to share their HH data for settlement purposes, a further 19% were neutral (neither willing or unwilling to share), while 16% preferred not to share their HH for settlement. We also asked consumers whether or not they trusted Ofgem (61% said they did), their energy supplier (58%), a central body appointed to process HH data from all consumers for settlement (53%), supplier agents (39%), and third parties that the consumer had given permission to access their data (34%).

6.5 A majority of the consumers that took part in Ofgem's 2018 Consumer Panel research were happy to share their HH data for settlement purposes and saw this as beneficial for the supplier, for wider society, and potentially for themselves. When presented with options 1-3 that we are considering for access to HH data,[167] the majority of participants perceived opting-out to be the best option as consumers were thought to be unlikely to act on any message required to opt in or out. More generally, a small minority would be unlikely to wish to share their HH data in any circumstances.

Assessing risks

6.6 In this DPIA, we have assessed the severity and likelihood of a number of risks in relation to processing HH data for settlement. The severity and likelihood are each ascribed on a 1-5 scale, from 1 being least severe or likely to 5 being most severe or likely. This is shown in the table below:

Likelihood rating	Severity rating	Scale
Rare	Insignificant	1
Unlikely	Minor	2
Possible	Moderate	3
Likely	Major	4
Near certain	Catastrophic	5

6.7 The likelihood and severity rating are multiplied by one another to give an overall rating. The ranges for these are as follows:

Low 1-4
Medium 5-14
High 15-25

6.8 The GDPR requires risks in DPIAs to be considered in terms of both likelihood and severity. The ICO defines a high risk in the context of a DPIA as a high threshold of "any significant physical, material or non-material harm to individuals" where "harm is more likely, or because the potential harm is more severe, or a combination of the two".[168]

6.9 The meanings of the terms we have used for the risk likelihood are self-evident. For severity, we have taken the terms to mean the following:

Severity	Definition for security	Definition for risk to

[167] We did not discuss the enhanced privacy options with panel members because of the inherent complexity of these options and as Panel Members had been given a lot of new information to process in relation to the settlement system and the HHS project

[168] https://www.ofgem.gov.uk/sites/default/files/docs/2009/04/risk-management-at-ofgem_0.pdf

rating	and privacy risks	benefits realisation
Insignificant	Limited impact on a small number of consumers if the risk occurs	Little to no impact on the realisation of HHS benefits
Minor		A small impact on the realisation of HHS benefits
Moderate	If the risk occurs, there would be moderate impact on a significant minority of consumers; or limited impact on most consumers; or significant impact on a small number of customers	A large minority of the benefits of HHS are not realised
Major		A majority of the expected benefits of HHS are not realised
Catastrophic	Significant impact on most consumers if the risk occurs	Few of the expected benefits of HHS are realised

Option 1, Opt in: Access to HH electricity consumption data for settlement purposes is subject to existing data access rules, giving domestic consumers the choice to opt in (the status quo for domestic consumers) – Assessment of Risk

6.10 The party responsible for settlement would be required to retrieve and process HH data for settlement only where consumers provide opt in consent to share their HH data for settlement. Under this option, customers who did want to share their HH data for settlement would have to make a proactive choice to opt in.

Security Risks: Unauthorised parties access and use, amend or delete HH data

6.11 Where suppliers or other parties in the settlement process are handling HH data, despite robust security provisions in place for smart metering, a residual security risk will remain. As discussed above, this should be significantly mitigated by the numerous legal requirements on parties handling HH data.

6.12 If Ofgem decides to maintain the requirement to obtain domestic consumers' opt in consent to access HH data for settlement then it is likely that there will be a lower volume of HH data being retrieved from meters than would be the case if a legal obligation were introduced. This would reduce potential harm (ie the severity) caused by a security breach but not the likelihood.

Suppliers, agents or other parties misuse HH data

6.13 Ofgem requests information annually from all larger electricity suppliers (those with more than 250,000 customers), through the Smart Metering Annual Request for Information (RFI), on the proportion of domestic consumers opting in to share their HH electricity consumption data with their supplier. This data provides us with a general indication of consumers' willingness to share their HH electricity consumption data. Suppliers are taking different approaches to communicating options and seeking consent, and not all are proactively asking their customers to share HH electricity

consumption data.

6.14 Among suppliers that proactively ask their customers if they can access their HH data, opt-in rates opt-in rates are highly variable. Although in some cases they can be as high as 80%, we do not think this is a reliable predictor. Those who have already had a smart meter installed are comparatively early adopters of smart meters. This group may have a different attitude towards sharing their data than consumers who have a smart meter installed at a later date. Information provided to Ofgem by suppliers generally indicates that while variance could be explained by difference in consumer base, more important factors in determining whether or not people are willing to share their data are: the approach taken to obtaining consent; explaining how data will be used; services offered to customers; and potential benefits in return for their data.[169]

6.15 The majority of suppliers do not currently HH settle profile class 1-4 customers. The RFI data does not therefore provide insight on willingness to share data for settlement purposes specifically or the extent to which consumers who are willing to share their data for one purpose are more (or less) likely to share their data for other purposes. We have however conducted consumer research to inform our access to HH data decision, which does indicate willingness to share data for settlement purposes, as noted in paragraph 6.4.

6.16 If Ofgem decides to retain the requirement for domestic consumers to opt in to sharing HH data for settlement, consumers would then fall into one of four broad categories:

- Share data for HHS and also for other purposes (eg billing, marketing)
- Do not share HH data for settlement but choose to share data for other purposes (eg billing, marketing)
- Share data for HHS but choose not to share data for other purposes (eg billing, marketing)
- Do not share HH data for any purpose

6.17 In section 5.28-5.55, we examined the incentives on suppliers or other parties to misuse HH data. In practice, a supplier's incentives to do so would depend on consumers' data sharing choices, whilst the magnitude of the risk would depend partially on the number of consumers in a particular category, with those categories discussed in relation to each access to data option below.

Consumers share data for HHS and also for other purposes (billing, marketing)

6.18 There is limited incentive on suppliers to misuse data in this case because they would already have consent to use HH data for marketing and/or billing purposes. This is potentially a relatively large group as those who choose to proactively opt in to sharing HH data for settlement would likely be the consumer group who are more confident about sharing data generally and therefore may be more willing to share it for other purposes.

Consumers do not share HH data for settlement but choose to share data for other purposes (billing, marketing)

[169] Ofgem expects that all parties seeking consent to access HH data do so in a manner which complies with the GDPR and standard conditions of electricity supply licence.

6.19 Suppliers would have an incentive to encourage some customers in this group with low peak consumption to be HH settled as this would enable them to reduce their settlement bill.[170] Our view is that the strength of incentives to misuse data would not be very strong in this case, as suppliers would understand the profiles on which such a customer was settled and be confident of margins made on that particular customer. Sharing data for billing and marketing but not settlement appears relatively unlikely because research suggests that consumers view sharing data for marketing and billing to be higher risk than sharing data for settlement.[171] Moreover, for some products, suppliers would likely require participating consumers to share data for settlement and billing. We would therefore expect this group to be relatively small.

Consumers share HH data for HHS but choose not to share data for other purposes (billing, marketing)

6.20 This is the scenario in which suppliers would have the strongest incentive to misuse data as these customers would be HH settled but suppliers would not be able to use HH data to reflect consumption patterns in tariff offers to the consumer. We expect that this group will be a smaller proportion of consumers if Ofgem chooses to maintain the current requirement for consumers to opt in to sharing HH data than if Ofgem chooses to move to a legal obligation to share HH data for settlement purposes with or without the option to opt out. The reason for this is that opting in to sharing data requires a proactive choice and therefore we think that if consumers proactively agree to share data for one purpose, they are more likely to share it for other purposes, and vice versa.

Consumers do not share HH data for any purpose

6.21 Customers in this group would not be HH settled. Suppliers would therefore not have legal grounds to process their HH data for any purpose. In the absence of any particularly strong incentives on suppliers to wish to settle such customers HH, there is little or no increase in suppliers' incentive to misuse data compared to today's market. Moreover, suppliers would be able to understand the costs of supplying customers in this category without needing to view HH data because those costs would be determined by the profile.

Opt In: Access to HH electricity consumption data for settlement purposes is subject to existing data access rules, giving domestic consumers the choice to opt in (the status quo for domestic consumers) – Overall assessment of risks

6.22 The likelihood of a data security breach occurring is similar across all three basic access to HH data options.[172] The volume of data and therefore the potential severity of such a breach is potentially relatively the lowest if access to HH data is on an opt in basis.

6.23 The incentives to misuse data depend on a customer's data sharing choices.

[170] We note that suppliers may have an incentive to encourage some consumers, eg those with high peak consumption, in this category to remain NHH settled, as this will reduce settlement costs for the supplier. We do not consider this to be a privacy risk, however, we asked for views on this risk through question three in our consultation accompanying this DPIA

[171] https://www.ofgem.gov.uk/publications-and-updates/consumer-views-sharing-half-hourly-settlement-data

[172] Those being opt in, opt out and mandatory.

Suppliers have the highest incentive to misuse data where a customer is settled HH but has chosen not to share their data for billing or marketing purposes. If customer data was used for billing or marketing without consent, consumers with higher peak demand could be offered more expensive electricity tariffs as a result. There are however, strong deterrents, primarily reputational and potentially financial risks to deter parties from misusing data. The magnitude of the risk would depend on the number of consumers whose data had been misused, the nature of the misuse, for example what the supplier did with the data and the resulting impact on consumers.

	Severity	**Likelihood**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH data	Moderate	Unlikely	Medium
Privacy Risks: Suppliers, agents or other parties misuse HH data	Minor	Possible	Medium

Option 2, Opt out: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only, unless the consumer opts out (HH data for microbusinesses is currently collected on an opt out basis) - Assessment of risk

6.24 The party responsible for settlement would be legally obliged to retrieve and process HH data for settlement. Under this option, customers who did not wish to share their HH data for settlement would have to make a proactive choice to opt out.

Security Risks: Unauthorised parties access and use, amend or delete HH data

6.25 We anticipate that if we choose option 2, a larger proportion of customers' HH data will be retrieved from smart and advanced meters relative to option 1. Therefore, the potential harm caused by a security breach would rise relative to opt in. The likelihood could potentially be higher because of the incremental benefit of being able to access a larger volume of data.

Suppliers, agents or other parties misuse HH data

6.26 The four data access categories outlined above are relevant for this option. However, because the default access to HH data choice is to share data for settlement purposes, we expect that the number of consumers who share data for HHS but not for billing or marketing purposes would be larger. The incentives and risks associated with each group remain the same as those described under opt in but we expect that the size of each group would change significantly and therefore impact the severity of risks.

Group	**Anticipated change in size compared to option 1 (status quo for domestic consumers)**
Consumers share data for HHS and also for other purposes (billing, marketing)	No change or larger
Consumers do not share HH data for settlement but choose to share data for other purposes (billing,	Slightly smaller

marketing)	
Consumers share data for HHS but choose not to share data for other purposes (billing, marketing)	Significantly larger
Consumers do not share data for any non-regulated purpose	Significantly smaller

Opt out: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only, unless the consumer opts out (HH data for microbusinesses is currently collected on an opt out basis) - Overall assessment of risks

6.27 If Ofgem decides to move to opt out access to HH data for settlement, we consider that security and privacy risks will be slightly higher than for an opt in arrangement. This is primarily because we expect that more customers will share HH data for settlement but choose not to share data for other purposes. This is the group where there is the highest incentive for suppliers to misuse data.

6.28 However, we have not amended our assessment of the likelihood or severity of a security risk relative to opt in because we do not think that the incremental change to this risk resulting from more consumers sharing HH data for settlement purposes is enough to move to the next category.

	Severity	**Likelihood**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH data	Moderate	Unlikely	Medium
Privacy Risks: Suppliers, agents or other parties misuse HH data	Minor	Possible	Medium

Option 3, Mandatory: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only - Assessment of risk

6.29 The party responsible for settlement would be legally obliged to retrieve and process HH data for settlement.

Security Risks: Unauthorised parties access and use, amend or delete HH data

6.30 HH data will be retrieved for settlement from all smart and advanced meters. Therefore, the potential harm caused by a security breach would be somewhat higher than under options 1 or 2, although not sufficient to move to the next category. The likelihood could potentially be higher because of the incremental benefit of being able to access a larger volume of data, although again not sufficient to move to the next category.

Privacy Risks: Suppliers, agents or other parties misuse HH data

6.31 Only two of the data access categories described above are relevant to this option.

6.32 Consumers who are most reluctant to share their HH data would be required to do so for settlement purposes under option 3. This group would be unlikely to choose to share such data for other purposes. Some consumers who would be willing to share their data for settlement purposes would

choose not to share HH data for other purposes.

6.33 We anticipate that the proportion of consumers HH settled and also sharing data for other purposes would be significantly higher relative to opt in and potentially higher relative to opt out. A significant factor in this will be the strength of incentives offered by suppliers to encourage customers to share their HH data for other purposes.

Group	**Anticipated change in size from opt in/out**
Consumers are HH settled and choose to share data for other purposes (billing, marketing)	Potentially larger
Consumers are HH settled and choose not to share data for other purposes (billing, marketing)	Significantly larger

Mandatory: There is a legal obligation on the party responsible for settlement to process HH electricity consumption data for settlement purposes only – Overall assessment of risk

6.34 If Ofgem decides to place a legal obligation on suppliers to HH settle customers we anticipate that privacy risks will be higher relative to opt in and somewhat higher relative to opt out – enough to put the privacy risk into a higher category of severity. The reason for this is that the proportion of customers HH settled but choosing not to share data for other purposes would be largest under option 3. The incentive to misuse data is therefore largest in this case. The volume of HH data being processed is also largest in this case.

	Severity	**Likelihood**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH data	Moderate	Unlikely	Medium
Privacy Risks: Suppliers, agents or other parties misuse HH data	Moderate	Possible	Medium

7. Privacy and security risks of access to half-hourly export data

7.1 We set out in our Significant Code Review Launch statement documentation that we are considering settlement of export in the development of the Half-Hourly Settlement (HHS) target operating model (TOM).[173] We are seeking views, via the consultation accompanying this Data Protection Impact Assessment (DPIA), on whether any regulatory clarity is needed on the legal basis for access to half-hourly (HH) export data from smart and advanced meters. We are also seeking views on whether, given our analysis suggests that HH export data reveals less about a consumer, HH export data is likely to be of less concern to consumers than HH electricity consumption data.

7.2 There is no specific reference to export data in the Data Access and Privacy Framework. However, we consider that HH export data is personal data given that it can be linked to an MPAN which can in turn be linked to a specific customer's account. Therefore, HH export data is covered by data protection regulation. Nevertheless, we think that export data does not reveal as much about a consumer as their consumption data and is therefore less likely to be of concern to consumers. This is because export data is less indicative of when consumers are home and usually more indicative of local weather conditions. Similarly, varying rates of export may also be accounted for by the presence of a storage device, making it more difficult to determine a consumer's lifestyle habits from their HH export data alone. We have categorised the risk posed to consumers of processing their HH export data in this chapter (see table below).[174]

7.3 In our HHS TOM design principles,[175] we said we would consider settlement of export during the development of the TOM and that specifically:

- "At a minimum, improvements to the process for settlement of export should provide solutions for elective take-up;
- Any settlement arrangements including export should facilitate accurate measurement and allocation of electricity volumes;
- The solutions to the settlement of import and export should align in the long term to realise the full benefits of settlement reform. This will improve the accuracy of balancing at distribution network level into the mid-2020s to support increased uptake of micro-generation; and
- The enduring settlement arrangements for export should facilitate the implementation of future policy on small-scale low-carbon generation."

Benefits of settling export HH

7.4 A large number of sites with distributed generation (primarily solar PV) that

[173] https://www.ofgem.gov.uk/system/files/docs/2018/01/appendix_2_proposed_governance_arrangements_for_the_development_of_the_target_operating_model.pdf

[174] Whenever we refer to "HH data" in this document, we are referring to import (ie consumption) data unless otherwise specified

[175] https://www.ofgem.gov.uk/system/files/docs/2018/01/appendix_2_proposed_governance_arrangements_for_the_development_of_the_target_operating_model.pdf

are exporting to the grid are not currently HH settled, making the settlement system less accurate than it otherwise would be. This is also known as 'spill'. This spill distorts the accuracy of NHH profiles. The costs of this spill, which can occasionally be negative, ie payments, are shared across all electricity suppliers based on their share of consumption in each distribution region. Settling export HH would remove these costs and increase the accuracy of the settlement system.[176]

7.5 We would expect settling HH export to have similar benefits as settlement of HH electricity consumption. For example, costs would no longer be socialised across suppliers but allocated to the correct parties that in turn would have an incentive to reward consumers for exporting at times that are beneficial for the system.

Risks associated with the collection of HH export data

7.6 HH export data provides information about the volume of electricity that is exported from a particular premises. This is the amount generated[177] that has been fed back to the grid. Where microgeneration is concerned, the primary driver of export volumes is weather conditions, which do not reveal information about individuals. However, given that any consumption of electricity generated in a premises will reduce the amount of electricity exported, it could in theory be possible, if the party processing such data had access to localised weather data and/or output from similar exporters nearby, to use HH export data to provide an indication of whether a premises was occupied (or at least whether it was consuming any electricity at the time).

Security Risks: Unauthorised parties access and use, amend or delete HH export data

7.7 We anticipate that the potential harm to consumers from unauthorised access of their HH export data is likely to be very limited because HH export data tells very little about a consumer. GDPR rules on data handling would apply to export data. Given the limited incentives to unlawfully access, use or amend export data and the difficulty parties would have in obtaining this data, our view is that the likelihood of this risk occurring is very low.

7.8 To identify an individual consumer from export data, a malicious party would have to access the export data and then identify the address to which it related. We would anticipate that parties handling such data would, given legislative requirements to store data securely,[178] store it without specific addresses attached. Therefore access to information enabling MPANs or other unique identifiers to be mapped to specific addresses would be required to match export data to HH specific consumers. This information is held in a separate data-base with restricted access.

	Severity[179]	**Likelihood[180]**	**Overall Assessment of Risk**

[176] ELEXON, through the BSC Panel's Settlement Reform Advisory Group, have also investigated the benefits of settling export, see: https://www.elexon.co.uk/wp-content/uploads/2015/10/27_249_13A_SRAG_Report_PUBLIC2.pdf

[177] Or potentially generated at or supplied to the premises then stored using a battery for later export

[178] Article 5, 1 (f), of GDPR

[179] Risk severity is ranked on a five point scale: insignificant, minor, moderate, major, catastrophic

[180] Risk likelihood is also ranked on a five point scale: rare, unlikely, possible, likely, almost certain

Security Risks: Unauthorised parties access and use, amend or delete HH export data	Minor	Rare	Low

Privacy Risks: Suppliers, agents or other parties misuse HH export data

7.9 As described above, in most instances, it will be difficult to determine the habits of consumers based on their HH export data, given that for those with solar panels or storage for example, export is likely to take place at similar times for most consumers: during sunnier periods and at peak times respectively. This data is likely to have little value to parties outside of the energy sector, and we anticipate that the value it does have to those within this sector would be primarily for marketing purposes.

7.10 Under the rules of the FiTs scheme, suppliers are currently required to meter export already where it is practical and possible to do so.[181] If export was settled HH as well as being metered, then suppliers would have an incentive to encourage their customers to export at times of grid constraint or high peak demand.

7.11 As such, the most likely risk to these consumers is that their current supplier sends them unsolicited marketing messages. However, given that export from microgeneration is largely weather driven and predictable, a supplier's knowledge that microgeneration is present rather than access to the HH data itself, would be likely to be sufficient information for the supplier to offer tariffs to a consumer, with access to the HH export data itself a useful but not essential extra. Given the limited uses for and predictability of HH export data, we therefore think that incentives to misuse it are relatively low.

Overview

7.12 We think that security and privacy risks are less likely to occur where export data is concerned due to the limited value HH export data will have to unauthorised parties generally and relative to other forms of personal data consumers share with their suppliers, for example financial information. This is compounded by the fact far fewer consumers have a record of export data, itself restricted by the numbers of consumers with appliances like solar PV.

7.13 The GDPR potentially imposes significant penalties where both of these risks are concerned for those parties found to be in breach of the rules.

	Severity[182]	**Likelihood [183]**	**Overall Assessment of Risk**
Privacy Risks: Suppliers, agents or other parties misuse export HH data	Minor	Rare	Low

[181] Except where a FiT Order signed by the Secretary of State allows otherwise. Installation of smart meters mean it is possible to measure the export from a FIT installation and therefore triggers a requirement for the FIT generator to be paid based on metered rather than deemed export. The energy industry are working towards this and Ofgem is monitoring progress by industry in achieving compliance.

[182] Risk severity is ranked on a five point scale: insignificant, minor, moderate, major, catastrophic

[183] Risk likelihood is also ranked on a five point scale: rare, unlikely, possible, likely, almost certain

8. Mitigating the identified risks

8.1 We outlined existing regulatory requirements that apply to parties processing HH data in chapters 4 and 5, above. Our initial assessment is that this framework, particularly in light of data protection legislation which recently came into force, the GDPR, is already comprehensive.

8.2 The Information Commissioner's DPIA guidance[184] suggests a number of mitigation measures to consider. We have assessed the potential of those that are relevant to access to half-hourly (HH) electricity consumption data[185] for settlement below.

Anonymising or pseudonymising data where possible

8.3 As set out above, in addition to the three basic access to HH data options, we have also thoroughly assessed the potential for anonymisation or pseudonymisation (hidden identity) to mitigate privacy risks to consumers.

8.4 As previously described, Baringa's analysis narrowed possible applications of hidden identity or anonymisation to one potential model for each option. Specifically:

- Hidden Identity: Legal obligation to process HH data for settlement combined with pseudonymisation (MPAN replaced with unique identifier)
- Anonymisation: Legal obligation to process HH data for settlement where the data from consumers who choose to opt out of sharing their HH data for settlement is retrieved and processed by a central body and then anonymised

8.5 The rationale for narrowing down to such models alongside an evaluation of anonymisation/hidden identity options is set out in Baringa's analysis,[186] published alongside this DPIA. This includes a description of how anonymisation or hidden identity could work in practice.[187]

Option 4a: Anonymisation

8.6 Anonymisation would potentially have a higher cost implication than hidden identity on the grounds that the proposed model would require setting up a central body to retrieve, process and anonymise HH data for those customers who chose to have their data anonymised.

8.7 Baringa noted that both anonymisation and hidden identity will risk not effectively protecting privacy if:

[184] https://ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf

[185] Henceforth referred to as "HH data". Where we discuss export data, we specify this.

[186] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

[187] If we decide to proceed with either hidden identity or anonymisation then more detailed design work and stakeholder consultation will be required.

- A supplier has a small number of customers in a particular Grid Supply Point area;
- A supplier has taken on a new customer; or
- A supplier is alerted to a meter error.

Security Risks: Unauthorised parties access and use, amend or delete HH data

8.8 HH data will be retrieved for settlement from all smart and advanced meters under this option. Therefore, the potential harm caused by a security breach would be slightly higher than under options 1 or 2, although as before, not sufficient to move the risk to the next category. The likelihood could potentially be higher because of the incremental benefit of being able to access a larger volume of data, however, that would only be the case where data was obtained prior to anonymisation.

Privacy Risks: Suppliers, agents or other parties misuse HH data

8.9 Notwithstanding the risks described above, while there are privacy benefits to the anonymisation option, we note that data would be retrieved, validated and processed before anonymisation could take place. It would also potentially be retained to allow resolutions of settlement disputes by suppliers. Therefore the data would potentially, for a significant period of time, still be classified as personal data. We also note that if supplier agents rather than suppliers were responsible for retrieving and processing data, then similar privacy advantages might be achieved to those that accrue if data is processed by a designated agent for anonymised data, however, we note that some suppliers use 'in-house' agents.

8.10 Baringa notes in its report that if Ofgem decided to move from the current supplier agent model of settlement to a centralised settlement model then there may be little or no incremental benefit to introducing the anonymisation option.

8.11 As with option 3 (mandatory), we anticipate that the proportion of consumers HH settled and sharing data for other purposes would be significantly higher relative to opt in and potentially higher relative to opt out (see para 6.32 and 6.33 above). Hence, the severity of the risk with this option will be the same as for option 3 (mandatory). However, with the addition of anonymisation to the process, the likelihood of this risk occurring (compared to option 3) would be reduced for those consumers choosing to have their data settled in this way – enough to move the likelihood to a different category.

Option 4a – Anonymisation: Overall assessment of risk

8.12 We have asked stakeholders for views on both enhanced privacy options in the consultation that accompanies this DPIA. However, our current view is that, given the late stage at which anonymisation would take place, and the potential to route data away from suppliers by other means, for example requiring supplier agents to retrieve data, the costs of procuring and setting

up a single body in order to anonymise[188] the HH data, the costs of this option are likely to outweigh the privacy benefits.

	Severity[189]	Likelihood[190]	Overall Assessment of Risk
Security Risks: Unauthorised parties access and use, amend or delete HH data	Moderate	Unlikely	Medium
Privacy Risks: Suppliers, agents or other parties misuse HH data	Moderate	Unlikely	Medium

Option 4b: Hidden identity

8.13 We anticipate that hidden identity could cost less than anonymisation, because the potential pseudonymisation body would have a smaller role.

8.14 In Baringa's proposed model for hidden identity,[191] a new 'pseudonymisation service' market role would be created. This service provider would retrieve HH data and replace MPANs with a new data ID.[192] Data would then be processed by the supplier agent responsible for processing the HH data. The pseudonymisation service provider and Supplier Meter Registration Agent (SMRA)[193] would both need to hold the 'data map' to ensure that data was sent to the right parties for processing.

8.15 To enable accurate settlement, some Registration data[194] would need to accompany pseudonymised IDs in order to enable settlement parties to complete validation, processing and aggregation activities. Baringa's analysis highlights that the provision of this data, while necessary, would increase the chance that parties wishing to identify an individual address would be able to do so by cross-referencing with the fuller data set. For example, an address could potentially be identified by looking at supplier agent start dates and other data held by the supplier.[195]

Security Risks: Unauthorised parties access and use, amend or delete HH data

8.16 Whilst all consumers will be settled HH under this option, we think that the likelihood of unauthorised parties accessing this data are low. This is because the data will have been pseudonymised ahead of processing for settlement and only a limited number of parties, the pseudonymisation service and SMRAs, would have the ability to map HH data to MPANs.

[188] For the avoidance of doubt, this view is specific to the issue of anonymisation, and does not determine our wider position on whether or not to centralise functions currently performed by supplier agents
[189] Risk severity is ranked on a five point scale: insignificant, minor, moderate, major, catastrophic
[190] Risk likelihood is also ranked on a five point scale: rare, unlikely, possible, likely, almost certain
[191] If Ofgem decides to pursue hidden identity then we will do more detailed design work on it
[192] This role could also be performed by the Supplier Meter Registration Agent
[193] The SMRA role is undertaken by the relevant distribution network
[194] For example line loss factor, supplier, appointed agent. Registration in this context refers to functions currently carried out by DNOs as opposed to the role of any future new centralised switching service.
[195] Under GDPR, parties are only allowed to process personal data for purposes for which they have a legal basis and must ensure, under Article 5 of GDPR, principle (f), that they have the appropriate security measures in place to protect personal data

8.17 The severity of this risk occurring remains the same across as for option 3 (mandatory) and option 4a (anonymisation) because like these cases, data is being collected for everyone in the market and as the value of HH data to unauthorised parties remains the same.

Privacy Risks: Suppliers, agents or other parties misuse HH data

8.18 The likelihood of this risk occurring is less than option 3 (mandatory) because most parties would not have access to the 'data map' that would allow HH data to be linked to MPANs.

8.19 However, if the personal data were to be misused by an authorised party, the severity of such an occurrence would mirror that for option 3 (mandatory) due to the number of consumers HH settled.

Option 4b: Hidden Identity – Overall Assessment of risk

8.20 Overall, we assess security risks as low and privacy risks as medium under the hidden identity option. An important variable, which we are consulting on specifically in our accompanying consultation, is whether or not consumers should be able to choose to have their data pseudonymised. If they are allowed a choice, then, as for anonymisation, the nature of the privacy and security risks will slightly differ for those consumers not opting to partake in enhanced privacy.

8.21 We have asked stakeholders for views on the enhanced privacy options and specifically indicated that we may consider the hidden identity option further if evidence received in response to the consultation suggests that hidden identity could be a proportionate and practical approach.

	Severity[196]	**Likelihood [197]**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH data	Moderate	Rare	Low
Privacy Risks: Suppliers, agents or other parties misuse HH data	Moderate	Unlikely	Medium

Reducing retention periods

8.22 HH data will be collected on a more regular basis than data from traditional meters, which are often only read on a yearly or even less frequent basis.[198] One of the key objectives of the HHS project and the TOM, which is being developed, is therefore to reduce settlement timeframes. We anticipate that this will significantly reduce the period of time over which settlement data needs to be retained.

[196] Risk severity is ranked on a five point scale: insignificant, minor, moderate, major, catastrophic

[197] Risk likelihood is also ranked on a five point scale: rare, unlikely, possible, likely, almost certain

[198] SLC 21B.4 places an an all reasonable steps requirement on suppliers to obtain a meter reading for each of its customers at least once a year, excluding pre-payment metered customers

8.23 Ofgem anticipates that reducing the HH data retention period should have a small positive impact on both security and privacy risks by reducing the amount of data that is available at any point in time which can potentially be misused. However, given that recent data is likely to be of most value because of the information that it provides about a household, this will provide only limited mitigation of these risks.

Compliance and enforcement activity

8.24 Ofgem undertakes proactive and reactive compliance activities to protect customers and ensure they get a fair deal from the market. We use the intelligence we gather about suppliers to take firm but proportionate action where things are going wrong. We often publicise this activity so all suppliers can learn the appropriate lessons from our work.

8.25 In serious cases of potential non-compliance that meet our prioritisation criteria, Ofgem may decide to take enforcement action. Enforcement action includes issuing directions or orders to bring an end to a breach or remedy the harm that was caused, imposing financial penalties of up to 10% of a supplier's turnover and accepting commitments or undertakings relating to future conduct or arrangements. All our compliance and enforcement activity is intended to ensure suppliers put matters right quickly when things go wrong and to deter future non-compliance. This should boost trust and confidence in the market.

8.26 The purpose of Ofgem's broader compliance monitoring regime is to reactively and proactively determine compliance with legal obligations by relevant parties. Our subsequent actions would depend on the nature of any infringements. Such action could include fines imposed on the basis of licence breach, application for a court order to secure compliance, referral to other relevant authorities (eg ICO) or even licence revocation under exceptional circumstances.

8.27 Ofgem requests information annually from all larger electricity suppliers (those with more than 250,000 customers), through the Smart Metering Annual Request for Information (RFI), on the proportion of domestic consumers opting in to share their HH data with their supplier. While the focus of information requested from suppliers may change as the smart meter rollout nears completion, we will need to consider how to continue to monitor supplier communications and behaviour where approaches to gaining consent to access and use HH data from smart and advanced meters is concerned.

8.28 We work closely with Citizens Advice and the Energy Ombudsman to monitor complaints and issues experienced by consumers. This will continue to be an important channel for information to Ofgem to identify at an early stage if a supplier or another party is misusing data.

8.29 When Ofgem makes a decision on implementing market-wide HHS, we will need to consider what form of monitoring would be appropriate and proportionate. To this end, we are seeking views through our consultation published alongside this DPIA on the monitoring/auditing framework.

Other mitigation measures

8.30 There are a large number of measures that organisations responsible for processing data should consider in order to minimise privacy and/or security

risks. Many of these may be required or be a logical extension of the steps necessary for data controllers or processors to ensure compliance with the GDPR and other relevant legal frameworks. These include:

Mitigation	**Security Risks: Unauthorised parties access and use, amend or delete HH data**	**Privacy: Suppliers, agents or other parties misuse HH data**
Considering technological security measures	Y	Y
Training staff to ensure risks are anticipated and managed	Y	Y
Writing internal guidance or processes to avoid risks	Y	Y
Putting clear data sharing agreements into place	Y	Y

9. Risks to the realisation of the benefits of market-wide HHS

The aim of our consultation accompanying this DPIA is to set out our preliminary assessment of the access to half-hourly (HH) electricity consumption data options and invite responses to that assessment. In this chapter, we summarise our assessment of the relationship between each option and the benefits of market-wide HHS.

9.1 These risks are not privacy risks, they are an assessment of the extent to which each option supports the realisation of the benefits of market-wide HHS, and in turn, the benefits that are passed on to consumers. They are a necessary consideration as we assess the proportionality of our options.

Access to HH data options 1-3 (opt in, opt out, mandatory)

9.2 Across options 1-3, the key variable is the likely numbers of consumers HH settled. Opt in is likely to lead to the fewest number of consumers HH settled, in part because some individuals are unlikely to act against the default setting. There is scope for this proportion to vary considerably depending on prevailing public opinion over smart meters and data privacy, practicalities of engaging with consumers, wider societal attitudes towards sharing data, market conditions, and any future incentives for consumers to engage with flexibility.

9.3 Among suppliers that proactively ask their customers if they can access their HH data, opt-in rates are highly variable. Although in some cases they can be as high as 80%, we do not think this is a reliable predictor. Those who have already had a smart meter installed are comparatively early adopters of smart meters. This group may have a different attitude towards sharing their data than consumers who have a smart meter installed at a later date. Information provided to Ofgem by suppliers generally indicates that while variance could be explained by difference in consumer base, more important factors in determining whether people are willing to share their data are: the approach taken to obtain consent; explaining how data will be used; services offered to customers; and potential benefits in return for their data.[199]

9.4 We anticipate that opt out would lead to a higher proportion of consumers being HH settled than opt in. This explains the variation in severity across these two options. We have assessed the likelihood for each as likely.

9.5 In relation to the mandatory option, there is a risk that some consumers would feel so strongly that they did not wish their HH electricity consumption data to be retrieved for settlement purposes that they would choose not to accept a smart meter. They would then not be able to access the range of benefits that smart metering offers, such as accurate billing, better informed switching, and access to a wider range of tariffs, some of which could be cheaper for them. For that reason, we have rated the severity of mandatory

[199] Ofgem expects that all parties seeking consent to access HH data do so in a manner which complies with the GDPR and standard conditions of electricity supply licence.

as moderate (equal to the severity for opt out). However, we think the likelihood for this risk is one step down: possible.

9.6 The benefits of market-wide HHS that are most heavily impacted by the proportion of consumers who are HH settled are those flowing from the new incentive HHS places on suppliers through new smart products being offered in the market: the system benefits. System benefits that we expect as a result of consumers responding to incentives to shift demand away from peak price periods would not be realised for consumers not sharing data. Costs of providing security of supply and adequate network infrastructure would potentially be higher, particularly if, as expected, the number of consumers with electric vehicles grows significantly over the next few decades.

Enhanced privacy

9.7 We expect that the enhanced privacy options would lead to more consumers HH settled than the status quo. This is because both enable all smart and advanced metered consumers to be HH settled. Both offer an enhanced degree of privacy relative to the status quo. Implementing one of the enhanced privacy options would however introduce some additional settlement system costs, including initial setup costs and ongoing costs of centralised functions delivering enhanced privacy protections. It may also introduce delay, as new services would need to be designed and set up. These options are discussed in detail in Baringa's report published alongside this DPIA.

Overall assessment

9.8 The overall assessment of the risks of opt in to benefit realisation is rated as high. This is a reflection of the likely trade off between consumer privacy and the realisation of the benefits of market-wide HHS. Whilst our overall assessment of the benefit realisation risk associated with opt out and mandatory is medium, the likelihood of benefits not being realised under opt out is higher, as opt out carries the risk that a significant proportion of consumers choose not to share their HH data; this risk is even greater under opt in. However, we are mindful that if sharing HH data for settlement purposes is mandated some consumers may choose not to accept a smart meter in order to not share their HH data, hence our rating of moderate.

9.9 Overall, we need to strike a proportionate balance between ensuring that consumers' privacy is safeguarded and the risk that not settling consumers HH could make the electricity system more expensive and less efficient and therefore ultimately lead to higher bills for consumers.

Assessment of the risk each option poses to the realisation of market-wide HHS benefits

	Access to HH electricity consumption data option	**Severity[200]**	**Likelihood[201]**	**Overall Assessment of Risk**
Risk to market-	Opt in	Major	Likely	High

[200] Risk severity is ranked on a five-point scale: insignificant, minor, moderate, major, catastrophic

[201] Risk likelihood is also ranked on a five-point scale: rare, unlikely, possible, likely, almost certain

wide HHS benefit realisation	Opt out	Moderate	Likely	Medium
	Mandatory	Moderate	Possible	Medium
	Anonymisation	Moderate	Possible/likely[202]	Medium
	Hidden Identity	Minor[203]	Possible/likely[204]	Medium

[202] At this stage, we are not able to be more specific than "possible/likely" because of the current uncertainty of the costs and timeframes of implementing and operating an anonymisation or hidden identity solution

[203] Severity here is minor, but with potential for significant costs and/or delay

[204] At this stage, we are not able to be more specific than "possible/likely" because of the current uncertainty of the costs and timeframes of implementing and operating an anonymisation or hidden identity solution.

10. Conclusion

10.1 We have identified two key risks that could stem from the combination of a decision to introduce market-wide HHS and a potential change of the conditions of access to HH data for settlement purposes. These risks are:

- Security Risks: Unauthorised parties access and use, amend or delete HH data
- Privacy: Suppliers, agents or other authorised parties misuse HH data

10.2 We have discussed both of these risks and considered the impact that settlement could have on the likelihood and severity of each. Our assessment includes reference to relevant existing legislation. We believe the existing regulatory framework, particularly given the introduction of the GDPR, significantly mitigates both areas of risk that we have identified.

Evaluation of risks in light of additional mitigations

10.3 We have discussed the following mitigations:

- Hidden identity
- Anonymisation
- Reducing retention periods
- Compliance monitoring

10.4 We have also highlighted that there are a significant number of mitigations that parties handling personal data will need to consider as part of ensuring their compliance with their obligations under data protection legislation.

Assessment of risk with hidden identity or anonymisation

	Access to half-hourly electricity consumption data option	**Severity[205]**	**Likelihood[206]**	**Overall Assessment of Risk**
Security Risks: Unauthorised parties access and use, amend or delete HH data	Opt in	Moderate	Unlikely	Medium
	Opt out	Moderate	Unlikely	Medium
	Mandatory	Moderate	Unlikely	Medium
	Anonymisation	Moderate	Unlikely	Medium
	Hidden Identity	Moderate	Rare	Low
Privacy Risks: Suppliers, agents or other parties misuse HH data	Opt in	Minor	Possible	Medium
	Opt out	Minor	Possible	Medium
	Mandatory	Moderate	Possible	Medium
	Anonymisation	Moderate	Unlikely	Medium
	Hidden Identity	Moderate	Unlikely	Medium

[205] Risk severity is ranked on a five point scale: insignificant, minor, moderate, major, catastrophic

[206] Risk likelihood is also ranked on a five point scale: rare, unlikely, possible, likely, almost certain

Benefits realisation risks

10.5 We have considered the impact in terms of realisation of benefits likely to result from each access to half-hourly (HH) electricity consumption data option in more detail in our consultation on access to HH data, published alongside this document.

	Access to half-hourly electricity consumption data option	**Severity**	**Likelihood**	**Overall Assessment of Risk**
Risk to market-wide HHS benefit realisation	Opt in	Major	Likely	High
	Opt out	Moderate	Likely	Medium
	Mandatory	Moderate	Possible	Medium
	Anonymisation	Moderate	Possible/likely[207]	Medium
	Hidden Identity	Minor[208]	Possible/likely[209]	Medium

Reducing retention periods

10.6 Introducing HHS should reduce the amount of time data needs to be retained for settlement purposes. This should reduce retention periods. Our assessment is that while this is a positive step it will not significantly impact on the potential severity or likelihood of risks identified relative to other potential mitigations (including those which data controllers/processors could take to mitigate such risks) because older data is likely to be significantly less useful to those who might wish to misuse it.

Overall residual risk

10.7 It is not possible to completely eliminate either of the risks identified. The regulatory framework, including requirements under the GDPR, provide significant mitigation through the requirements they place on data controllers and processors and the potential penalties for non-compliance.

10.8 If Ofgem decides to proceed with hidden identity or anonymisation then we would expect these to reduce privacy risks associated with misuse of data but not have a significant impact on risks related to the security of HH data. Most benefits associated with the anonymisation option may be achievable through opt-out, mandatory and hidden identity.

10.9 Hidden identity and anonymisation would both have time and cost implications. We will need to be convinced that the privacy benefits associated with such options would justify the cost if we decide to implement one of these measures.

10.10 We assessed privacy risks associated with misuse of data to be medium. We note that the existing legal frameworks, in particular the GDPR, allow for significant penalties for misuse of data. Compliance monitoring measures will also play a role in risk mitigation. We will keep existing compliance and

[207] At this stage, we are not able to be more specific than "possible/likely" because of the current uncertainty of the costs of implementing and operating an anonymisation or hidden identity solution

[208] Severity here is minor, but with potential for significant costs and/or delay

[209] At this stage, we are not able to be more specific than "possible/likely" because of the current uncertainty of the costs of implementing and operating an anonymisation or hidden identity solution.

monitoring measures under review.

Next Steps

10.11 We have not judged any of the privacy risks to be high and therefore we do not currently expect that the statutory requirement to consult with the ICO applies. However, we have engaged with and received feedback from the ICO since the beginning of the Settlement Reform programme and we expect to continue to do so. The preparation of this DPIA has been an iterative process that has been informed by the ICO's best practice guidance and comments at key points. We will continue to welcome advice from the ICO as we work towards our decision on market-wide HHS.

10.12 We invite comments from stakeholders on this DPIA. We will consider all comments and publish a revised DPIA when we announce our decision on access to HH data for settlement.

10.13 We have published a consultation[210] alongside this DPIA, on which we are also seeking views. We invite stakeholders to provide comment by 3rd September, 2018, as explained in the consultation.

[210] https://ofgem.gov.uk/publications-and-updates/consultation-access-half-hourly-electricity-data-settlement-purposes

Appendix 1: About DPIAs

What is a DPIA?[211]

A1.1 A DPIA is a way for parties to systematically and comprehensively analyse their processing and help them identify and minimise data protection risks.

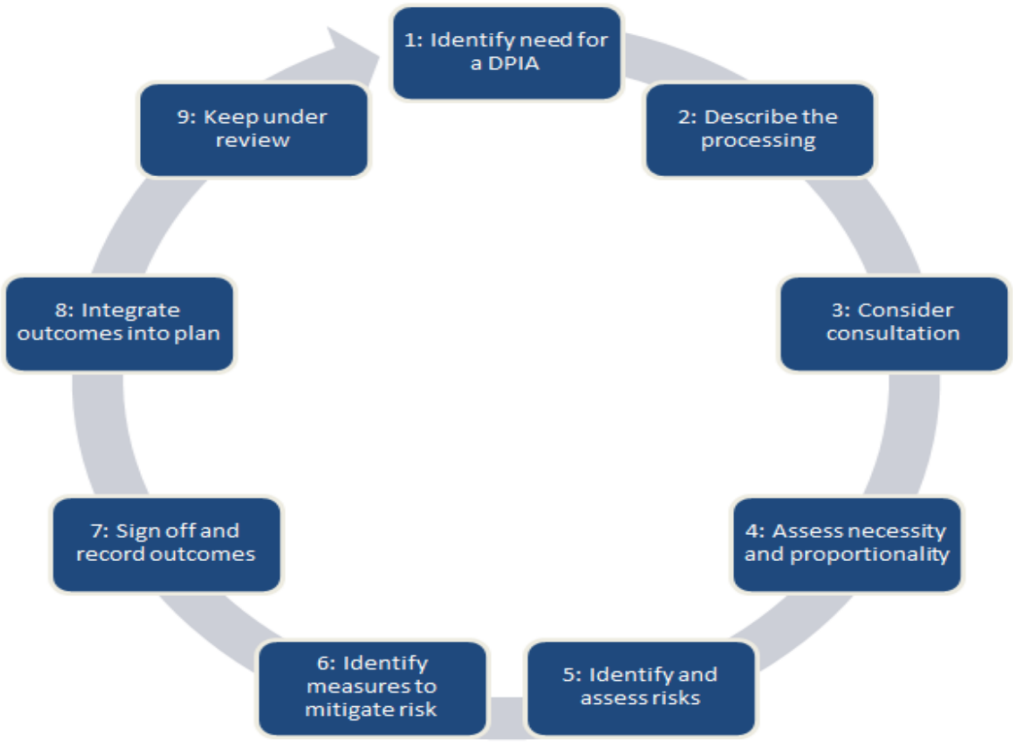
A1.2 DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

A1.3 To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A1.4 A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

The DPIA process

A1.5 A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



[211] Taken from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Appendix 2: Target Operating Models

Background

A2.1 The TOM will outline the changes to the settlement arrangements and supporting institutions needed to deliver market-wide HHS, including transitional settlement.

A2.2 The detailed design of the TOM is being undertaken by an ELEXON-led Design Working Group (DWG) comprising industry parties, consumer and government representatives. The TOM design options developed by the DWG were presented to Ofgem's HHS senior responsible owner (SRO) and accepted as suitable for ELEXON to consult on. To assist the Ofgem SRO in making this decision and future TOM decisions, an Ofgem-chaired Design Advisory Board[212] (DAB), consisting of members with expertise in energy industry, regulation and policy (GB and international), consumer issues and innovation, is providing strategic advice to Ofgem on TOM design options.

A2.3 The TOM design work consists of two main stages. In stage 1 of the design work, the DWG developed a range of high-level skeleton TOM options. We are presently at the beginning of stage 2, and Elexon has consulted with stakeholders on the high-level skeleton TOM options. In stage 2 of the design work, the DWG will undertake detailed design of the TOM options and narrow down the TOM options until a preferred TOM is identified and fully developed.

A2.4 While the development of the TOM and the decision on access to HH data for settlement options both form part of the HHS SCR, they form separate workstreams. However, the TOM must be consistent with the decision on access to HH data for settlement and other policy decisions made by Ofgem as part of this SCR. Thus, the TOM design work must ensure TOM options remain flexible[213] and do not rule out any access to HH data for settlement options being considered. This means that the preferred TOM cannot be fully developed until the decision on access to HH data for settlement is finalised.

A2.5 Additionally, the TOM design work process and the consideration of access to HH data for settlement options is iterative, as neither can be properly developed in the absence of the other. For example, this DPIA assessment has been informed by the skeleton TOM options developed by the DWG to date and, as stated above, the TOM design cannot be finalised until a decision on access to HH data for settlement is made.

TOM design work to date

A2.6 The DWG has met monthly since October 2017 and has developed five skeleton TOM options. The DWG has sought to develop the skeleton TOMs from first principles. This was done through a 'use case' approach covering all

[212] https://www.ofgem.gov.uk/gas/retail-market/forums-seminars-and-working-groups/design-advisory-board-market-wide-half-hourly-settlement

[213] This is recognised in the TOM baseline design principles agreed by the DWG. See DWG03/01 paper available at https://www.elexon.co.uk/meeting/design-working-group-3/.

'segments' in the market, classified broadly by type of meter and granularity of data that can be extracted.[214]

A2.7 The high-level steps undertaken by the DWG in the 'use case' approach were:

- Define processes required to deliver market-wide HHS and group them into high level activities;
- Identify the high level type of services required to deliver high level activities;
- Identify ways in which the identified services could be grouped for delivery by a market role. This would be done first within each segment and then done across segments.

A2.8 From this approach, five viable skeleton TOMs (A to E) mapping out how services could be grouped across all market segments to deliver MHHS was identified by the DWG.[215] The skeleton TOMs differ mainly around how data retrieval, data processing and data aggregation services are grouped for delivery. All of these skeleton TOM options can accommodate the access to HH data for settlement purposes options being considered in this DPIA.

[214] The segments are smart meters with settlement period (half-hourly) data available, smart meter without HH data available, non-smart meters without HH capability, traditional advanced HH meters and unmetered supplies.

[215] See paper DWG05/01A for more detailed information about the skeleton TOM options. Available at https://www.elexon.co.uk/meeting/design-working-group-5/.

Glossary

A

Advanced meter

As define by the Standard Conditions of Electricity Supply Licence, an advanced meter is an Electricity Meter that, either on its own or with an ancillary device, and in compliance with the requirements of any relevant Industry Code:

> (a) provides measured electricity consumption data for multiple time periods, and is able to provide such data for at least half-hourly time periods; and
>
> (b) is able to provide the licensee with remote access to such data.

Anonymisation

Anonymisation is defined under GDPR as "data rendered anonymous in such a manner that the data subject is not or no longer identifiable"

B

Balancing and Settlement Code (BSC)

The BSC contains the governance arrangements for electricity balancing and settlement in Great Britain

C

Consumption data

Also known as import data, this is a record of any granularity of the amount of electricity supplied to a given MPAN

D

Data Access and Privacy Framework

Government has developed a data access and privacy policy framework to determine the levels of access to energy consumption data from smart meters that suppliers, network operators and third parties should have. It also establishes the purposes for which data can be collected and the choices available to consumers.

Data Communications Company

The DCC is responsible for linking smart meters in homes and small businesses with energy suppliers, network operators and energy service companies.

E

Export data

This data is a record of quantity of electricity supplied – also known as export – back to the grid, eg from a solar panel

G

Grid Supply Point (GSP)

A grid supply point is a point where the transmission system connects to the distribution system

Grid Supply Point Group

A distribution network region, as defined under the BSC.

I

Import Data

Also known as consumption data, this is a record of any granularity of the amount of electricity supplied to a given MPAN

L

Load shaping

Also known as load profiling, this is the process where a consumption pattern (or shape) is applied to a long-term meter reading to estimate more granular consumption (eg HH) of a consumer, eg when the actual HH data for a particular period(s) is not available

M

Microbusinesses

This is defined in the Standard Conditions of Electricity Supply Licence (7A.14) as "a Non-Domestic Consumer: (a) which is a "relevant consumer" (in respect of premises other than domestic premises) for the purposes in article 2(1) of The Gas and Electricity Regulated Providers (Redress Scheme) Order 2008" or "(b) which has an annual consumption of not more than 100,000 kWh".

Meter Point Administration Number (MPAN)

A unique identifier allocated to a given meter point, also known as Metering System Identifier (MSID)

P

Profile class

Profile classes are calculated using a sample of customers that are representative of the population. More information about Profile Classes can be found on ELEXON's website: https://www.elexon.co.uk/knowledgebase/profile-classes/

Pseudonymisation

The process of distinguishing individuals in a dataset by using a unique identifier that does not reveal their 'real world' identity

R

Register reads

Register Readings are the Meter readings obtained from meter's tariff registers. This could be the cumulative register or the meter's time of use registers.

S

Significant Code Review (SCR)

The SCR process is designed to facilitate complex and significant changes to a range of industry codes. It provides a role for Ofgem to undertake a review of a code-based issue and play a leading role in facilitating code changes through the review process.

Settlement period

The period over which contracted and metered volumes are reconciled. This is currently defined as a period of 30 minutes.

Settlement period data

Settlement Period level data is consumption data that is the granularity of the Settlement Period this could be actual consumption data obtained directly from the Meter or consumption data derived from Register Readings or unmetered supplies that is processed to Settlement Period granularity

Smart Energy Code (SEC)

The SEC is an industry code that sets out the terms for the provision of the DCC's services and specifies other provisions to govern the end-to-end management of smart metering.

Smart meter

In the context of the smart meter rollout in Great Britain, smart meters must comply with the Smart Metering Equipment Technical Specifications (SMETS). SMETS-compliant smart meters can measure and record gas and electricity consumption on a half-hourly basis and can send readings remotely to a customer's supplier.

SMETS1 and SMETS2

Smart Metering Equipment Technical Specifications 1 and 2 refers to the first and second generation of the specification for smart meters.

SMRA

Supplier meter registration agent