RecorDER Project

Legal and Regulatory Report on the sharing and publishing of data February 2020

1. INTRODUCTION

1.1 This report is prepared on behalf of Chaddenwych Services Limited, UK Power Networks (Operations) Limited, Eastern Power Networks plc, London Power Networks plc, South Eastern Power Networks plc, SP Distribution Plc and National Grid Electricity System Operator Limited who are collaborating on an innovation project to create a shared asset register for energy asset data ("**RecorDER Project**"). This report may not be copied to, distributed to nor relied upon for any purpose by any person other than Chaddenwych Services Limited, UK Power Networks (Operations) Limited, Eastern Power Networks plc, London Power Networks plc, South Eastern Power Networks plc, SP Distribution Plc and National Grid Electricity System Operator Limited without our prior consent in writing. The contents of this report reflect the position as known to us as at 21st February 2020 and may not be relied upon or regarded as reporting at any subsequent date or time.

1.2 In this report any references to "**we**", "**our**" or "**us**" is to Pinsent Masons LLP.

1.3 The RecorDER Project, as developed by Chaddenwych Services Limited (t/a Electron), which will be a decentralised platform collating data such as the location and capacity of energy producing assets in the UK, is funded by the Network Innovation Allowance (NIA). The aim is to design and build a block-chain-based register of transmission and distribution system energy resources (assets) that could become a standard to use by ESO, DNOs and other energy sector stakeholders.

1.4 We understand that the RecorDER Project:

1.4.1 aims to create a coherent view of assets connected to the energy network by integrating existing datasets in the industry;

1.4.2 builds on the work of both The Energy Data Taskforce and ENA's Open Networks system wide resource register ("**SWRR**"); and

1.4.3 will use blockchain as an enabling technology, allowing the integration layer to be deployed and hosted by collaborating parties, removing the requirement of either a large scale infrastructure project or a central party to host the system.

1.5 More specifically the RecorDER Project will create a data coordination platform collating existing data regarding UK energy assets and covering the following aspects:

1.5.1 Creation of a database tracking the identity and relationships associated with each energy producing asset in the UK (above 1MW, so excluding most residential assets);

1.5.2 Creation of a unique ID for each asset in the UK that will be used across the datasets produced by the platform;

1.5.3 Creation of data service protocols with defined authorisation requirements and permissions for access to the data output. These protocols also store links to external datasets / databases which contain the fields set out in the protocol;

1.5.4 Access to the data will be granted in line with this protocol to users (who are proposed to include market participants (i.e. the data providers) and third parties);

1.5.5 A third party may act in an audit function where required but otherwise the register will work on the basis that each data provider (the DNO) will hold its own data.

1.6 We understand that the RecorDER Project will display a unique ID for each asset. Each of the assets will be displayed with information on its operator, with the provider of the data ultimately controlling which type of data is displayed by the RecorDER Project. For the purposes of this report we have assumed that the providers of data to the RecorDER Project will be participating Distribution Network Operators (DNOs) and the users of that data will be participating DNOs and National Grid. References in this report to *data providers* and *data users* and any similar references should be construed accordingly. It is possible that in the future the RecorDER Project may be expanded to encompass a wider group of data providers and data users.

1.7 As a result we understand that the RecorDER Project will effectively amount to a data coordination platform. The RecorDER Project and the blockchain technology used will have a facilitation role, but will not formally hold the data provided by asset operators.

1.8 The type of data which will be coordinated by the RecorDER Project will be information on specific energy assets (DERs: distributed energy resources), and we understand will include:

1.8.1 General asset data: grid supply point, plant type, point of supply, primary;

1.8.2 Connection status data (connection data, capacity);

1.8.3 Service data (distribution or transmission service, contract duration, whether any exclusivity in place);

1.8.4 Network reinforcement data (works reference, description);

1.8.5 For those assets to be connected in the future, information will include the export capacity agreed, the target date for connection, its queue position, and any other specific information on distribution and transmission reinforcement.

1.9 The problem that the RecorDER Projects seeks to address is to define, assess and pilot a blockchain-based asset register, enabling parties to use and reference a shared data set of generation and flexibility resources, which would not otherwise be possible.

1.10 We have been asked to consider a number of questions, as set out in the Legal and Regulatory Scope dated 16 August 2019 a copy of which is set out in Appendix 1 (the "**Scope**"), in relation to the sharing and publishing of data in respect of the RecorDER Project. We set out below our responses to these questions and our advice on any other issues that were identified as part of our review.

1.11 Our review focused on the proposed sharing of data within certain specified data fields. More information on the categories of data to be shared is set out in Appendix 2. In this report we call this data "**SWRR Data**".

1.12 The advice is based on the law of England and Wales. We are aware that some of the data may relate to sites in Scotland. Our view is that the legal and regulatory issues identified below will be equally relevant to the position under the laws of Scotland.

2. EXECUTIVE SUMMARY

2.1 Energy Regulation

2.1.1 Prohibitions to the disclosure of information of the type expected to be shared under the RecorDER Project exist within (i) both European and UK legislation and (ii) UK regulation:

(a) Utilities Act 2000 s105 - prohibits the disclosure of information obtained under specific legislation (including the Electricity Act 1989) in respect of individuals and businesses.

(b) REMIT – prohibits persons who possess inside information in relation to a wholesale energy product from disclosing that information to any other person unless such disclosure is made in the normal course of the exercise of their employment, profession or duties.

(c) Standard Licence Conditions (distribution) and Electricity Codes – contain confidentiality requirements.

2.1.2 These restrictions may not apply where the information has already been made public, an individual or business (as relevant) has given its consent to the disclosure, or there is a requirement at law for disclosure.

2.1.3 Not all SWRR Data is already in the public domain and that the process to acquire consent from all connected decentralised assets (current and future) is not, at this stage, considered viable for the project, although it is recommended at section 2.5 below that stakeholders consider whether the RecorDER Project could be designed in such a way that appropriate consents are obtained from the relevant individual and business asset owners before data relating to them is included in the RecorDER Project. Again, we understand that this is not a viable solution, as even if consent were obtained from current owners, there would be logistical difficulties in ensuring that the consent of all future owners is obtained. As such, we have considered whether a modification to the current regulatory regime could make disclosure of SWRR Data, as envisaged by the RecorDER Project, lawful. We do not consider that it is necessary to amend UK primary legislation, given that the UA s105(3)(c) allows disclosure where such disclosure is made by a licence holder and is required to be made by a condition of the licence. A modification to either the Standard Licence Conditions (distribution) or the Electricity Codes could alleviate the prohibitions under UK law and regulation, to the extent that inconsistencies across the Electricity Codes are dealt with.

2.1.4 In terms of European law, specifically REMIT, disclosure as anticipated by the RecorDER Project may be permitted to the extent that disclosure of the SWRR Data would not have a significant effect on the prices of wholesale energy products. We do not have the ability to assess what information may or may not have an impact on energy pricing; however there is a risk that disclosure of the SWRR Data to specific entities would be prohibited under REMIT. If information not already known to the trading public is to be disclosed as part of the RecorDER Project, then a commercial analysis would need to be undertaken with an energy trading analyst to determine whether disclosure of SWRR Data is likely to have a significant impact on the pricing of wholesale energy products and fall foul of REMIT.

2.2 Confidentiality, Privacy and Data Protection

2.2.1 **Law of Confidence:** much of the information that will be shared under the RecorDER Project is in the public domain and, as a result, will not have about it the 'quality of confidence' that is necessary for that information to be protected under the common law of confidence. Nonetheless, certain categories of data to be shared under the RecorDER Project are not in the public domain and are non-trivial in nature. That data is the confidential information of the relevant connectee or asset operator to whom it relates. As it stands, disclosure of such data without the consent of such connectee or asset operator could constitute an actionable breach of confidence.

2.2.2 **Express Obligations of Confidentiality**: certain contracts[1] under which SWRR Data is shared contain express obligations of confidentiality and non-use, which may restrict disclosure or use of that data. As is common practice, the contracts we examined contain a range of exceptions to the confidentiality and non-use obligations. These range from general exceptions to enable disclosure of information that is in the public domain or that is required by law or a court order, to more industry-specific exemptions, such as a right to disclose information as required by industry agreements, codes and licence conditions. As it stands, it appears not all of the SWRR Data to be disclosed as part of RecorDER will fall within those exceptions and so disclosure without the consent of the other party would constitute a breach of contract.

2.2.3 **Breach of a duty of confidence - consequences:** breach of a duty of confidence (whether express or under the common law) may result in the party to whom such confidential information relates taking action against the disclosing party to recover the loss it suffers as a result of such breach or to obtain an injunction or order requiring the delivery up of the relevant information.

2.2.4 **Consent**: obtaining appropriate consent from the person to whom the duty of confidence is owed would address concerns that its use in RecorDER would constitute a breach of confidence. Unfortunately, we do not believe that obtaining express consent is a practical

[1] We examined a range of contracts provided by RecorDER project partners including forms of connection agreement and connection terms and conditions, short term operating reserve (STOR) standard terms and conditions, fast reserve SCTs.

or viable solution due to the volumes of data and the number of asset owners / counter-parties. Even if consent was obtained for all relevant assets, if ownership of an asset changes, then continuing use of updated information would likely require a further consent to be obtained from the new asset owner. However, note that it is recommended in section 2.5 that stakeholders consider whether obtaining consent to disclosure from participating asset owning individuals and / or businesses is a practically feasible option in terms of the design of the RecorDER system.

2.2.5 **Privacy and Data Protection and Data/Network Security Analysis:**

(a) Personal data is not limited to identifiers such as the customer name, and removing the customer name would not exclude SWRR Data from qualifying as personal data. Where the different fields of data are (or can be) linked together, it would not be the case that the identifier is personal data, and the associated technical data (e.g. point of supply) is not. All the information associated with that identifier would qualify as personal data. It is not necessary for information to directly identify an individual for it to qualify as personal data as long as it relates to an individual who can be identified, even if indirectly.

(b) Privacy and Data Protection Laws (GDPR and Data Protection Act 2018) (PDPL) will only apply to SWRR Data that relates to individuals; i.e. it will be Personal Data. A significant amount of the SWRR Data will likely relate to legal persons and not individuals. However, we do understand that some SWRR Data will be subject to PDPL. In particular: (i) we understand that certain assets may be operated by individuals or sole traders; and (ii) we anticipate that the pilot / RecorDER Project may be extended in the future to smaller assets and that this may, ultimately, include assets on domestic or small business premises.

(c) Where SWRR Data constitutes personal data, there is not an automatic prohibition on sharing and use of that data, however PDPL gives rise to various compliance obligations which; (a) must be met to permit the sharing and use of the data, and (b) could limit the sharing and use of SWRR Data.

(d) SWRR Data would not be personal data if it is aggregated in such manner that it is no longer possible to link it to an individual. The aggregation must be such that it cannot be reversed. Aggregation may also have a significant adverse impact on the value of the data but if it is possible to only disclose aggregated data to DNOs, such data would not constitute personal data in the hands of the DNOs (although the Data Access Controller would still process the underlying SWRR Data).

(e) In addition to privacy and data protection compliance, there must be compliance with related security and compliance requirements, whether imposed under codes of conduct, practice or in respect of sensitive sites, or critical infrastructure. These may apply whether or not the information is personal data.

2.3 Competition Analysis

2.3.1 While potential competition law risks can arise with a data sharing project of this type, we would consider that this risk can be managed given the overall nature of the project, together with the proposed controls and protocols which RecorDER will put in place.

2.3.2 From our understanding of the proposals for the project, we understand that commercially sensitive information is unlikely to be exchanged given that a large degree of the information is in the public domain, that controls are placed to prevent undertakings at the same level of the market from viewing one another's information, and that information which could affect the pricing of wholesale energy projects will not be exchanged.

2.3.3 To manage the competition law risks, we set out a number of recommendations summarised below.

2.4 Recommendations

2.4.1 Energy Regulation

(a) Achieve a modification under either the Standard Licence Conditions or the Electricity Codes to require DNOs to share certain information (the SWRR Data) with NGESO and third parties in respect of decentralised assets. Note that an amendment to the Standard Licence Conditions is likely to be a more straightforward process than modifications to the Electricity Codes, which would require multiple modification processes, due to different Electricity Codes containing different restrictions. The project partners should discuss those options and engage with Ofgem and / or the relevant Code administrators, as appropriate, on the options available.

(b) As at November 2019, a DCUSA mod 350 is under consideration, but not all SWRR Data fields have been included in the modification request. It is recommended that a discussion take place between the RecorDER project partners and the DCP 350 Working Group to what extent the requested data fields can be expanded. Also consider whether timescales are appropriate for the RecorDER Project. Note that if DCUSA mod 350 was amended to capture all of the SWRR fields and the modification was subsequently implemented to permit the sharing of SWRR Data under DCUSA, this would permit the sharing of SWRR Data under the remaining Electricity Codes, save for the Distribution Code, which does not contain the relevant equivalent carve out from confidentiality set out in the other Electricity Code. Accordingly, the issue caused by the restrictions under the Distribution Code would require to be addressed through either a Distribution Code amendment or appropriate Standard Licence Conditions amendments as recommended under section 2.4.1 (a) above.

(c) Discuss with Ofgem the inconsistencies across the Standard Licence Conditions and the Electricity Codes and the process for rectification of this (as it stands, the modification of one Electricity Code will not alleviate the prohibition on disclosure of confidential information under all of the Electricity Codes, in particular the Distribution Code, whereas modification of the Standard Licence Conditions could be drafted to take precedence over restrictions in the Electricity Codes).

(d) Consider to what extent the disclosure of SWRR Data (not already available to the trading public) is likely to have a significant impact on the prices of wholesale energy products and limit SWRR Data fields to those fields that would not be likely to have a significant effect on the prices of wholesale energy products. It is not immediately apparent to us based on our understanding of the nature of the SWRR Data that the proposed sharing of data under the RecorDER Project will have such an effect but we recommend that the partners in the RecorDER Project take further steps to analyse the position including with input from specialists and / or analysts engaged in the wholesale energy trading market.

(e) Consider whether obtaining consent to disclosure from asset owning individuals and / or businesses is a practically feasible option in terms of the potential next steps identified in section 2.5.

2.4.2 Confidentiality, Privacy and Data Protection

(a) **Confidentiality**:

(i) by following the Energy Regulation recommendations set out in section 2.4.1 a DNO would be required by law to disclose the SWRR Data that they hold. If that is the case, then compliance by a DNO with that requirement would not be in breach of the common law of confidence and such disclosure would fall within the exceptions to the express obligations of confidentiality in the sample contracts reviewed by us.

(ii) Consider whether obtaining consent to disclosure from asset owning individuals and / or businesses is a practically feasible options in terms of the potential next steps identified in section 2.5.

(b) **Privacy, Data Protection and Data/Network Security:**

(i) Any sharing of personal data through the requirement of 'consent' under the Utilities Act, will for the purpose of data protection laws, need to meet the GDPR 'consent' conditions and other compliance requirements. The Energy Regulation recommendations set out in section 2.4.1, if followed, would require the disclosure of SWRR Data by law and will provide an alternative legal base for the data sharing and use. A different legal processing ground will be less administratively burdensome.

(ii) GDPR compliance obligations and accountability will need to be considered and incorporated into the project's procedures and polices as they are being developed to ensure that a) personal data will be identified when it will be shared as part of the SWRR Data and, b) the procedures will be applicable for ensuring GDPR compliance by all the participants.

(iii) As part of developing the technical model for sharing the data and the overall governance model or structure, decisions need to be made about which participants have decision-making responsibilities for the SWRR Data, as this may impact whether all participants are joint controllers for all project processing, or there are individual data controllers. The governance and participation agreement will need to cover all GDPR contractual requirements, and related issues such as liability depending on the relationship of the different participants.

(iv) In addition to the general GDPR compliance for sharing and use of SWRR Data, the use of the type of blockchain technology will need to be considered, as some blockchain technology will create greater GDPR compliance obligations. Additionally, due to the nature of the technology, processes will need to be designed to ensure that 'functionally' some data subject rights can be exercised. Further, there will need to be GDPR compliance for the blockchain participants. The agreements for participation will need to include provisions for GDPR compliance and related issues, such as different levels of security (i.e. sensitive and critical sites) and liability.

2.4.3 Competition Law

(a) Given that the sharing of commercially sensitive information can raise competition law risks, RecorDER and the data providers (the DNOs) should carefully consider, and continue to monitor, what data is commercially sensitive and to which type of market participant each type of information should be given or be restricted. Information such as provider information, contractual descriptions, connection queue management position, asset capacity and exclusivity terms is likely to be commercially sensitive, and should be within the category of information which participants should only be able to view their own data. Any data sharing should not go beyond that required to generate the benefits of the RecorDER Project (described in section 1 (Introduction)), and any feedback to market participants of any aggregation of data by third parties (e.g. aggregators) should be carefully considered for competition law risk.

(b) A data protocol should be put in place and reviewed by legal counsel. This should set out clearly how the data is to be stored and displayed; the types of data which will be shared with which parties; protections built in to the RecorDER Project to

prevent any inappropriate disclosure; and the role of any third party audit function.

(c) RecorDER should ensure that its agreements with each of the data providers (DNOs), and with those undertakings which access the data (which, initially at least, will be the participating DNOs and National Grid), specify clearly the scope of the data included and its intended purpose.

(d) The terms upon which parties are given access to the RecorDER Project must be considered, and should be fair and reasonable terms in order to prevent any form of 'collective boycott' or discrimination between participants. Where relevant, third parties may need to be offered access but such may be limited on the basis of objective justifications, such as complying with other regulatory obligations (e.g. under REMIT, which prohibits access to be given to certain information).

2.5 Addressing legal and regulatory data issues in the RecorDER Project – Practical Next Steps

2.5.1 **Working Assumptions**:

(a) we understand that SWRR Data in certain data fields has already been placed in the public domain by DNOs and is accordingly already accessible. A summary of the project partners' understanding of the position in respect of the SWRR Data that is currently published by individual DNOs is set out in Appendix 2.

(b) not all SWRR Data contained in the data fields identified in Appendix 2 is in the public domain or already accessible and there is not a universal approach to making information available, i.e. certain DNOs make information available and others do not;

(c) it has been recognised that there may be personal data shared as part of the RecorDER Project, whether personal data relating to sole trader operators of >1MW sites under the current RecorDER Project proposals or (in the future) data relating to individuals at domestic or small business sites should the RecorDER Project be extended to smaller DER assets. This means that GDPR and other privacy law considerations need to be considered in the design of the RecorDER Project.

2.5.2 **Public Domain Data**

(a) the act of further sharing, as part of the RecorDER Project, of data that is publicly available already shall not *per se* be a breach of confidence or a breach of applicable energy legislation, Licence Conditions and Electricity Codes that restrict the disclosure of certain information;

(b) as that public data may contain personal data the RecorDER Project needs to address GDPR considerations in its design and in the way is used and makes available personal data. Options for enabling GDPR compliance in the design of the RecorDER Project including segregating data are set out in sections 4 and 6;

(c) in respect of the application of REMIT, in order to be classified as having been "made public", data must be made available to the "broad trading public". It is not currently clear from our desktop review that all of the data contained in the data fields identified in Appendix 2 as being published have necessarily been made available to the broad trading public in this way (see section 3.5.4). Further analysis to determine whether any REMIT risk exists is needed with commercial input from an appropriately qualified person engaged in wholesale energy product trading / pricing;

(d) the fact that certain data identified in section 2.5.1(a) is publicly accessible mitigates competition law risk but the competition law recommendations set out

in section 2.4.3 and in section 7 should be actioned in the design and implementation of the RecorDER Project.

2.5.3 **Other Data**

(a) disclosure of data that is not currently publicly available without the consent of the relevant individual or business asset owner may be a breach of confidence or a breach of applicable energy legislation, Licence Conditions and Electricity Codes that restrict the disclosure of certain information;

(b) for that data additional steps are needed before it can be shared as part of the RecorDER Project. Options include:

(i) implementing the proposed regulatory changes recommended under section 2.4.1;

(ii) designing the RecorDER Project such that appropriate consents are obtained from the relevant individual and business asset owners before data relating to them is included in the RecorDER Project. This would address energy regulation and confidentiality concerns, although if ownership of an asset is sold then a new consent would be needed and, therefore, there are practical challenges to be overcome before a consent-based model could be developed;

(c) consent may also be a basis for processing any personal data under the RecorDER project, but would need to be obtained again if an individual transferred ownership of an asset to another individual. Other options for enabling fair processing are set out in sections 4 and 6;

(d) data that is not available to the "broad trading public" falls within the application of REMIT and so additional analysis involving commercial input from a wholesale energy trading specialist is needed to assess whether there is any risk that making available that data in the manner proposed under the RecorDER Project is likely to have a significant impact on the pricing of wholesale energy products;

(e) if information is not publicly accessible, then the risk of it being regarded as commercially sensitive for competition law purposes is increased; albeit our understanding is still that information shared under the RecorDER Project is unlikely to be commercially sensitive for the reasons given in section 7.4. The competition law recommendations set out in section 2.4.3 and in section 7 should be actioned in the design and implementation of the RecorDER Project.

3. ENERGY REGULATION

3.1 In this section we consider questions identified by the RecorDER Project partners. The questions are set out in full and our advice is set out below each question. In answering the questions, we were asked to consider:-

(a) whether the legislation / regulation applies to all SWRR Data or only select data fields;

(b) the extent to which legislation / regulation limits with whom SWRR Data can be shared; and

(c) what use it can be put to- sanctions for non-compliance.

3.2 **Key Legislation**: We have set out below the key pieces of legislation which contain restrictions in relation to the sharing and publishing of SWRR Data.

Utilities Act 2000

3.2.1 S105 of the Utilities Act 2000 (the "**UA**") prohibits the disclosure of information obtained under specific legislation in respect of individuals and businesses during the lifetime of the individual or for so long as the business continues to be carried on. The relevant information is any which has been obtained under:

(a) the UA;

(b) Part I of the Gas Act 1986;

(c) Part I of the Electricity Act 1989 (the "EA");

(d) s184(5) or 185(5) of the Energy Act 2004;

(e) Part II or s27 or 28 of the Energy Act 2010;

(f) s50 or 51 of the Energy Act 2013;

(g) s41 or 100 of the Energy Act 2008; or

(h) the Domestic Gas and Electricity (Tariff Cap) Act 2018.

3.2.2 The above legislation covers a wide range of information, including information submitted by applicants for a generation licence about themselves and their generation assets and information to be submitted by those applying for a grid connection. Having reviewed the SWRR Data fields, we believe that the restriction in the UA will apply to all of the SWRR Data.

3.2.3 There are certain exceptions to the prohibition set out in the UA, including where consent has been given by the individual or the person carrying on the business (s105(2). There is also an exception for any disclosure made for the purposes of facilitating the performance of any functions of, amongst others, the Secretary of State and the Gas and Electricity Markets Authority (the "**Authority**") under relevant legislation (s105(3)(a)). We do not believe that the creation of a shared asset register would currently fall under the functions of the Secretary of State or the Authority. The exemptions which may be relevant (and that we consider below – see *options for making the sharing of data lawful*) are s105(3)(c) and s105(3)(d).S105(3)(c), which allow disclosure where such disclosure is made by a licence holder and is required to be made by a condition of his licence. Note that this exemption is not currently applicable to the RecorDER Project as there is no requirement in the distribution licence to publish / share information the same as or similar to the SWRR Data. The exemption in s105(3)(d) permits a disclosure made by one licence holder to another and is required by that other licence holder for purposes connected with the carrying on of

his licensed activities. Even if a distributor was only sharing such information with another distribution or transmission licensee (as we understand will be the case initially), there is no obligation in the licence conditions to create a shared asset register, and therefore such disclosure could not properly be said to be required by that licence holder for purposes connected with his licenced activities. However, we consider below the possibility of amending the licence to require disclosure to the RecorDER Project of data the same as or similar to the SWRR Data.

3.2.4 A person who discloses any information in contravention of the prohibition in the UA is guilty of an offence and liable to (i) a fine on summary conviction or (ii) a fine or a prison term of up to two years, or both, on conviction on indictment.

Electricity Act 1989

3.2.5 The EA previously contained a provision (s57) which prohibited disclosure of information obtained under the EA. This provision was repealed by the UA, which now includes such a prohibition as part of s105 (see above).

3.2.6 S48 of the EA permits the Authority to publish information which would promote the interests of consumers in relation to electricity conveyed by distribution systems or transmission systems. In publishing such information, the Authority must have regard to the need for excluding any information relating to the affairs of a particular individual or body of persons, where publication of that matter might seriously and prejudicially affect the interests of that individual or body. This section is aimed at benefiting consumers, and it is unclear whether the creation of a shared asset register would satisfy the requirement of "promoting interests of consumers", as its primary aim would be to make information more accessible for industry stakeholders including users of electricity networks, as well as a visibility and planning tool for use by distribution network operators and National Grid ESO. In any case, before publishing any information under this section, the Authority is required to consult with any particular individual or body to which the information relates, which could be a drawn-out process considering the potential number of affected individuals. It is also important to note that it is solely the Authority who is permitted to publish such information under the EA and therefore the RecorDER Project would fall outside the scope of s48.

REMIT

3.2.7 Under Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency ("**REMIT**"), there is a prohibition (Article 3(1)(b)) on persons who possess inside information in relation to a wholesale energy product from disclosing that information to any other person unless such disclosure is made in the normal course of the exercise of their employment, profession or duties.

3.3 **Question**: could the SWRR Data be considered to be "inside information in relation to a wholesale energy product"?

3.3.1 "inside information":

(a) means "information of a precise nature which has not been made public, which relates, directly or indirectly, to one or more wholesale energy products and which, if it were made public, would be likely to significantly affect the prices of those wholesale energy products".

(b) can include:

(i) "information relating to the capacity and use of facilities for production / storage / consumption…of electricity", including planned or unplanned unavailability of these facilities (Article 2(1)(b) and paragraph 5.2 of ACER (Agency for the Cooperation of Energy Regulators) guidance on the application of Regulation (EU) No 1227/2011 of the European

Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency[2] ("**ACER Guidance**"));

(ii) any information that a reasonable market participant would be likely to use as part of the basis of its decision to enter into a transaction relating to, or to issue an order to trade in, a wholesale energy product (Article 2(1)(d) and ACER Guidance para 5.2).

3.3.2 "wholesale energy product":

(a) includes contracts and derivatives relating to the supply and transportation of electricity irrespective of how and where they are traded (Article 2(4)(a) to (d))

(b) excludes contracts for the supply and distribution of electricity for the use of final customers consuming less than 600GWh per annum (Articles 2(4) and 2(5))

(c) excludes contracts for green certificates and emission allowances (ACER Guidance para 3.2)

3.3.3 In terms of whether information relates to (or is considered to be in relation to) a wholesale energy product, our view is that information which is likely to have significant effect on the prices of a wholesale energy product if disclosed, would be considered to relate (either directly or indirectly) to that wholesale energy product (see analysis in section 3.5 on what would be considered to have a significant effect on pricing of wholesale energy products).

3.4 **Question**: has the SWRR Data already been *made public*?

3.4.1 ACER Guidance (para 5.3) states that "in general, information is deemed to be public knowledge if such information has been made available to the broad trading public, i.e. an unspecified number of individuals." ACER Guidance also makes it clear that there is a requirement to make such information available simultaneously to the broad trading public, ensuring equal access: "publishing information only to selected market participants, for example via an energy exchange information service or news board, which is available exclusively to exchange members, does not satisfy the requirement of informing the broad trading public." However, information can be made public via a subscription service, as long as the broad trading market can subscribe for such information if desired.

3.4.2 We note that the majority of the SWRR Data fields are already published by all or some of the DNOs and NGESO[3] and made available to the broad trading market. However, there is inconsistency between DNOs as to what information is published (i.e. they do not all publish the same SWRR Data fields). Also, the data fields published do not cover all Distributed Energy Resource (**DER**) assets (whether over or under 1MW). As such, there is no straightforward answer to this question for the RecorDER Project, as each asset would need to be looked at on a case by case basis to understand if the information in relation to that asset was already available to the broad trading market before it was included on the RecorDER asset register. In addition, information in respect of DER assets would need to be made available to the broad trading market before it could be added to (or amended on) the RecorDER asset register, so there would need to be administrative protocols in place to ensure that this happened, otherwise the made public argument could not be relied on. If all DNOs took a consistent approach to making available the relevant data fields to the broad trading market (to the extent that they are permitted to do so) then this uncertainty would be removed. The RecorDER Project partners should consider whether taking such a consistent approach, and putting in place appropriate administrative protocols to ensure that this approach is followed, is a practicable option.

3.5 **Question**: could the SWRR Data, if disclosed, have a significant effect on the prices of a wholesale energy product?

[2] https://documents.acer-remit.eu/wp-content/uploads/20190627_4th-Edition-ACER-Guidance_4thupdate.pdf
[3] http://www.energynetworks.org/electricity/futures/open-networks-project/der-information/overview.html

3.5.1 In relation to the SWRR Data that is not already available to the broad trading market, consideration will need to be given as to whether the disclosure of such information would be likely to have a significant impact on the pricing of wholesale energy products. ACER currently considers that the following should be taken into consideration as useful indicators of whether information is likely to have a significant price effect:

(a) the type of information is the same as information which has, in the past, had a significant effect on prices;

(b) pre-existing analysts research reports, price reporter publications and opinions indicate that the type of information in question has effects on prices;

(c) the market participant itself has already treated similar events as inside information;

(d) another reasonable market participant has already treated similar events as inside information (ACER Guidance para 5.4).

3.5.2 The ACER Guidance lists, as a "related document", Commission Directive 2003/124/EC of 22 December 2003 implementing Directive 2003/6/EC of the European Parliament and of the Council as regards the definition and public disclosure of inside information and the definition of market manipulation ("CD 2003/124/EC"). Directive 2003/6/EC contains a similar prohibition to REMIT on the disclosure of inside information, expect that it relates to financial instruments rather than wholesale energy products. CD 2003/124/EC provides guidance on how inside information under Directive 2003/6/EC should be interpreted. CD 2003/124/EC applies the following test in relation to whether information (if made public) would be considered to have a significant effect on pricing of financial instruments: "information a reasonable investor would be likely to use as part of the basis of his investment decisions". This test is replicated in REMIT as part of the definition of information at Article 2(1)(d): "information that a reasonable market participant would be likely to use as part of the basis of its decision to enter into a transaction relating to, or to issue an order to trade in, a wholesale energy product".

3.5.3 It would therefore be reasonable to conclude that disclosure of any SWRR Data to a market participant (and not to the broader trading public) that could be used by such market participant as part of the basis of its decision to enter into a transaction relating to, or to issue an order to trade in, a wholesale energy product, would be in breach of REMIT.

3.5.4 We note from the information that we have been provided with that a significant amount of the SWRR Data is already available to the trading public. However, it appears to us that the information available is held in different resources / locations and is incomplete, and therefore it may not be possible in respect of all (or even the majority of) decentralised assets to pull together the full list of SWRR Data from what has already been made public. As such, there is a real possibility that disclosure of all or part of the SWRR Data to certain entities (but not the broader trading public) could put those entities in possession of information that the broader trading public would not itself be able to access (for example linking company name with asset location, connection status, export capacity and the type and duration of balancing service being provided by that asset). As legal advisors, we do not have the ability to assess what information may or may not have an impact on energy pricing4. A commercial analysis will need to be undertaken to determine whether disclosure of SWRR Data not already known to the trading public (which may include having certain information linked together in respect of a particular asset) is likely to have a significant impact on the pricing of wholesale energy products. The answer to this question will depend on a number of things, including:

[4] We discussed whether it would be possible to give a clearer view on this in the report. However, following consideration, we do not consider that we are best placed to take a view on wholesale energy product pricing. We have provided further information as to what should be taken into consideration when assessing this point, but we cannot provide a definitive answer. Discuss how this should be addressed in the report.

(a) what information is disclosed and to whom;

(b) when such information is disclosed; and

(c) whether the disclosee could use that information as part of the basis of its decision to enter into a transaction relating to, or to issue an order to trade in, a wholesale energy product.

3.6 It is our recommendation that such commercial analysis with appropriate energy trading analyst and legal input be carried out as a next step in the development of a legal framework to support the RecorDER Project.

3.7 **Question**: could disclosure of the SWRR Data be considered to be disclosure made in the normal course of the exercise of a person's employment, profession or duties?

3.7.1 We consider that it would be difficult to argue that disclosure was in the normal exercise of the disclosing person's employment, profession or duties unless there was an express legislative or regulatory requirement for such information to be disclosed. We discuss below whether a change to the distribution licence or the Electricity Codes, to make disclosure an express regulatory requirement, could provide a mechanism for sharing and/or publishing the SWRR Data. From the perspective of REMIT, although there is an argument that a change to the regulatory regime in the UK to require DNOs to share information the same as or similar to the SWRR Data could make such disclosure in the normal course of a person's employment, profession or duties, we consider that, were such regulatory change to allow disclosure to specific entities / persons only (and not the broader trading public), there is a real risk that such disclosure would still be in breach of the Article 3(1)(b) prohibition to the extent that it has the potential to significantly affect the pricing of wholesale energy products. While the ACER Guidance does not give any detail on what would be considered to be in the normal course of a person's employment, profession or duties, we do not consider that it would be permissible for a member state to bring forward a regulatory change in contravention of the sprit of REMIT, as this could open the door to member states enacting local regulatory changes that disapplied aspects of EU legislation in the member state.

3.8 **Question**: are there any other areas of relevant energy legislation besides S.105 Utilities Act, Electricity Act 1989 and REMIT Regulations?

3.8.1 We have not found any other relevant pieces of legislation in relation to this issue, but note sections 3.10 and 3.11 in respect of the Electricity Codes.

3.9 **Question**: which legislation takes precedent if/when there are conflicts? The Utilities Act 2000, or the Electricity Act 1989 (where licence conditions are specified)?

3.9.1 We do not consider that there is a specific conflict between the UA and the EA in terms of a prohibition on the disclosure of energy information. This is because the original EA prohibition (s57) has been repealed by the UA (see above). As such, we have not considered this question in further detail.

3.10 **Question**: are there any specific restrictions on sharing and publication of information similar to the SWRR Data in the Electricity Codes?

3.10.1 **The Electricity Codes**: We have set out in Appendix 3 the relevant electricity codes ("Electricity Codes") and any provisions which they contain which restrict the sharing or publication of information. It is important to note that whilst these codes will apply to entities which are licenced under the EA, many of the embedded generators will not be licenced as they will fall under the small generators exemption under the EA (those with a capacity of 5MW or less).

3.11 **Question**: are the Electricity Codes considered legally binding?

3.11.1 The Electricity Codes set out above can be categorised as either (i) industry codes in the form of documents with which an individual or entity must comply, or (ii) agreements which an individual or entity must enter into or accede to. In relation to both types of code, the electricity licences require licensees to comply with the codes (see conditions 20-22 of the distribution licence). The Authority (through Ofgem) has the power under s27 of the EA to impose penalty on any person contravening a condition or requirement of their licences. Such penalty would take the form of a fine and potential personal liability of directors of a company which failed to comply. Therefore all of the Electricity Codes can be considered legally binding. In addition, codes which take the form of contracts (DCUSA, CUSC and MRA) would be considered legally binding as between the parties if properly executed. Failure to comply with the agreement would therefore allow the other party or parties to bring an action against a non-compliant party for breach of contract.

3.12 **Question**: where there are such legislative / regulatory impediments, what are the available options for making the sharing of such information lawful? To consider the following options (including what SWRR Data may be able to be shared / published in respect of these options):-

3.12.1 consent in Connection Agreements or otherwise?

3.12.2 a change in the licence conditions / Electricity Codes?

3.12.3 DCUSA modification 350?

3.13 There are a number of different approaches to making the sharing of the SWRR Data lawful under the existing regulatory regime. We have set out below the key options, but we note that a combination of these may be required.

3.13.1 **Connection Agreements**: amending standard form connection agreements to provide for consent to the disclosure of the SWRR Data would allow such information to be shared in respect of new generators, as the consent condition under s105(2) UA and certain Electricity Codes would be fulfilled. However, there are a vast number of connection agreements already in place containing restrictions which would have to be similarly amended. This would be a costly and time consuming task, and parties to such agreements are unlikely to be willing to bear such costs themselves. Also query whether existing generators would be willing to agree to such disclosure. The project partners should discuss whether obtaining consent to disclosure, whether through the Connection Agreements or otherwise, is a practically feasible solution.

3.13.2 In addition, some of the Electricity Codes (e.g. DCUSA) do not permit disclosure of confidential information (defined as information held in respect of a connectee which it has acquired in its capacity as operator of a distribution business) with consent. In addition, the DCUSA contains a more blanket restriction on how information can be used e.g. that such information may not be used for commercial advantage of the DNO or its affiliates in the operation of a supply business (e.g. DCUSA).

3.13.3 **Licence Conditions**: under standard condition 20.7 of the distribution licence, Ofgem can grant a derogation to a licensee which relieves it of its obligations under any core industry document. This could provide for an exception to confidentiality requirements for individual licensees, although we note it is unlikely that Ofgem would take the route of granting multiple derogations as this would be a time consuming process. In addition, a licence derogation would not affect those Electricity Codes which take the form of contractual agreements, as these would remain enforceable as between the parties to them.

3.13.4 Alternatively, Ofgem may modify the standard licence conditions for all licensees under s11A of the EA. A change in licence conditions (e.g. a blanket permission to disclose for purposes of creating an asset database) would have a more widespread effect than individual derogations or amendments to individual connection agreements. A benefit of permitting the publishing and sharing of data to create an asset database under the licence conditions is that it does not require any participation from individual licensees in the way that an amendment to connection agreements would, as DNOs would not need to sign up to an amendment agreement. However, although a change in licence conditions would

apply automatically to existing and future licensees once implemented, Ofgem would need to consult on any such changes in accordance with s11A before they took effect, which may take a number of months. We also note that an amendment to the licence conditions by Ofgem may not allow for information to be shared with third parties such as aggregators if, for example, Ofgem takes the view that any data should be shared only between distributors and transmission network operators for the purpose of improving access to information, rather than as a commercial tool for selling services.

3.13.5 **Electricity Codes**: parties to the Electricity Codes may propose modifications to them, some of which require approval by Ofgem. Similarly to an amendment to standard licence conditions, code administrators are likely to be required to consult on any modification to the Electricity Codes. All Electricity Codes would need to be similarly amended so that there is no conflict between codes which could allow for restrictions on sharing of information to remain. We have not been able to find any guidance as to which Electricity Code would take precedence in the event of a conflict between codes. However, we note that a number of the codes permit disclosure of information where such disclosure is permitted under another Electricity Code (all of those set out above except the Distribution Code), and so amendment to a single code may have the effect of permitting disclosure under a number of other codes, although not all of them.

3.13.6 It should be borne in mind that as of November 2019, there is an ongoing BEIS/Ofgem consultation regarding the reformation of energy industry codes including proposals to consolidate and simplify codes and introduce a "code manager" (i.e. a single rule making body) and a strategic function. This would aid a strategic push toward creating a register and ensure that the various codes do not contain conflicting terms in relation to sharing of information. It is recommended that partners in the RecorDER Project consider engaging with BEIS / Ofgem to discuss whether the outputs of that consultation could be used to heal address some of the barriers to data-sharing as part of the RecorDER Project that are identified in this report.

3.13.7 Where a party to an Electricity Code is a licence holder, they are required to comply with the relevant Electricity Codes under the standard conditions of their licence, which are implemented pursuant to the EA. We would therefore suggest that the licence conditions take precedence over the codes, although this is not a point that has been dealt with expressly in the legislation or tested at common law. Any amendment to the standard licence conditions which allowed for the sharing of the SWRR Data would therefore override restrictions around confidentiality in the Electricity Codes, although we would suggest that for clarity any amendment to the standard licence conditions should expressly state that such permission is notwithstanding any contrary code provisions. For this reason, we would suggest that a change to standard licence conditions would be the easier route than a change to the Electricity Codes, particularly as it would involve a single process rather than multiple modification proposals under various codes, and would bind all licensees rather than parties to individual codes. However, we note that a change to standard licence conditions or Electricity Codes does not necessarily remedy any conflicting confidentiality restrictions in contractual agreements and, as noted in the confidentiality commentary below, whilst most confidentiality clauses will have an exception allowing disclosure where required by law, this would not ordinarily extend to disclosure permitted by law.

3.13.8 It is worth noting that most connection agreements will state that the parties have entered into a CUSC Framework Agreement by which they intend the CUSC to be binding between the parties, so there would be an argument that disclosure permitted by CUSC would also be permitted under a connection agreement.

3.13.9 **DCUSA Modification 350**: as at November 2019, DCUSA modification 350 ("**mod 350**"), originally proposed by Solarplicity Supply Limited (now in administration) on behalf of the BEIS Panel of Technical Experts, is being considered by the DCP 350 Working Group. The modification would require DNOs to create a national, public register of all sites that use their networks and influence the operation of the GB power market. The register would contain details of each connected site and would be kept up to date by the DNOs. The modification proposal suggests a number of data items for inclusion on the register for

decentralised assets >1MW initially. There is significant overlap between these data items and the SWRR Data fields; however, we note that the following are not included in the proposal:

(a) date contracted;

(b) date connected;

(c) MPAN;

(d) service provider;

(e) type of service;

(f) contract duration; and

(g) exclusivity.

3.13.10 None of the data fields set out in Appendix 2 to this report in relation to reinforcement works are included in the proposal. We note that the proposal is for the creation of a "public" register which is not what we understand is intended for the RecorDER Project. In particular, the modification proposal states that such publicly available information would influence operations and investments by funders and DSR/storage owners. We understand from our discussions with you that the RecorDER Project would initially only be for use by transmission and distribution network operators, although is expected to extend to other industry stakeholders in future including in respect of use of SWRR Data.

3.13.11 As at November 2019, the DCP 350 Working Group has actions to engage with ENA Open Networks, discuss mod 350 with BEIS and to take legal advice in respect of the same. It was originally expected that mod 350 would be consulted on in October 2019, with implementation expected on 27/02/2020. However, the DCP 350 Working Group has agreed to take legal advice prior to issuing for consultation, so these timescales may be extended. We would expect appointed legal advisors to consider the same restrictions as we have identified in this report. Also, responses received under consultation could change the implementation date. It is worth noting that, as the modification proposes creating a public database that third parties (e.g. aggregators) could access, there may be opposition against such wide access from licence holders and other interested parties under a consultation. A closed register as proposed by the RecorDER Project may be more palatable to the wider market. Whilst it is not possible for a party other than the original proposer to directly amend modification 350 to meet the requirements of the RecorDER Project, it will be possible to put forward suggestions or proposals once the modification reaches the consultation stage, however there is no guarantee that any such suggestions would be implemented.

3.13.12 If implemented as proposed, mod 350 would legalise the sharing of information as under the DCUSA (and therefore also under the majority of the Electricity Codes, with the exception of the Distribution Code). However, the timescales may not be suitable for implementation of the RecorDER Project.

3.13.13 **REMIT**: see sections 3.2.7, 3.3, 3.4, 3.5 and 3.6 above.

3.14 Recommendations

3.14.1 Achieve a modification under either the Standard Licence Conditions or the Electricity Codes to require DNOs to share certain information (the SWRR Data) with NGESO and third parties in respect of decentralised assets. Note that an amendment to the Standard Licence Conditions is likely to be a more straightforward process than modifications to the Electricity Codes, which would require multiple modification processes, due to different Electricity Codes containing different restrictions. The project partners should discuss those options and engage with Ofgem, as appropriate, on the options available.

3.14.2 As at November 2019, a DCUSA mod 350 is under consideration, but that not all SWRR Data fields have been included in the modification request. It is recommended that a discuss take place between the RecorDER project partners and the DCP 350 Working Group to what extent the requested data fields can be expanded. Also consider whether timescales are appropriate for the RecorDER Project. Note that if DCUSA mod 350 was amended to capture all of the SWRR fields and the modification was subsequently implemented to permit the sharing of SWRR Data under DCUSA, this would permit the sharing of SWRR Data under the remaining Electricity Codes, save for the Distribution Code.

3.14.3 Discuss with Ofgem the inconsistencies across the Standard Licence Conditions and the Electricity Codes and the process for rectification of this (as it stands, the modification of one Electricity Code will not alleviate the prohibition on disclosure of confidential information under all of the Electricity Codes, in particular the Distribution Code, whereas modification of the Standard Licence Conditions could take precedence over restrictions in the Electricity Codes).

3.14.4 Consider to what extent the disclosure of SWRR Data (not already available to the trading public) is likely to have a significant impact on the prices of wholesale energy products and limit SWRR Data fields to those fields that would not be likely to have a significant effect on the prices of wholesale energy products. It is not immediately apparent to us based on our understanding of the nature of the SWRR Data that the proposed sharing of data under the RecorDER Project will have such an effect but we recommend that the partners in the RecorDER Project take further steps to analyse the position including with input from specialists and / or analysts engaged in the wholesale energy trading market.

3.14.5 Consider whether obtaining consent to disclosure from asset owning individuals and / or businesses is a practically feasible options in terms of the potential next steps identified in section 2.5.

4. PRIVACY AND DATA PROTECTION

4.1 In this section we consider questions identified by the RecorDER Project partners in relation to the extent to which the application of data protection law and other information laws and regulations may prevent or restrict the sharing of data envisaged under the RecorDER Project. The questions are set out in full and our advice is set out below each question.

4.2 **Question**: what are the confidentiality, privacy and data protection impediments to sharing and publishing the SWRR Data? In answering the questions, consider:

4.2.1 whether the legislation / regulation applies to all SWRR Data or only select data fields;

4.2.2 the extent to which legislation / regulation limits with whom SWRR Data can be shared and what use it can be put to;

4.2.3 the differences in legislation limitations between legal persons and natural (residential) customers;

4.2.4 sanctions for non-compliance.

4.3 **Privacy and data protection law ("PDPL")**: where SWRR Data constitutes personal data (as defined by PDPL), PDPL does not prohibit the sharing and use of that data, however PDPL gives rise to various compliance obligations which could limit the sharing and use of SWRR Data.

4.3.1 PDPL in the UK consists of the General Data Protection Regulation (GPDR), Data Protection Act 2018 (DPA18), and relevant guidance, codes of practice and case law relating to the processing of personal data applicable in the UK.

4.3.2 Primarily, it is only possible to share and use (process) SWRR Data that comprises personal data for specific, clearly defined purposes, which are communicated to the individuals to whom the SWRR Data relates by means of a privacy notice. More information about purpose limitation and the provision of privacy notices is set out in below.

4.3.3 Any processing of the relevant SWRR Data would require a legal basis of processing. Consent is one of the available legal bases of processing, but is not the only legal basis available. This is discussed in more detail below.

4.3.4 Other compliance limitations include the requirements of data minimisation (i.e. limiting the data which is processed to that which is necessary to achieve the purpose of processing), data retention (i.e. only keeping data for as long as is required to achieve the purpose), giving effect to the rights of data subjects under PDPL (such as the right of access and the right of erasure), implementing appropriate security measures, and putting in place mandatory contractual clauses in certain circumstances.

4.4 **Question**: will PDPL apply to all SWRR Data or only to specific data fields?

4.4.1 PDPL will not apply to all SWRR Data since not all SWRR Data will relate to individuals. In fact, a significant amount of the data will likely not relate to individuals. However, we do understand that some SWRR Data may be subject to PDPL. In particular: (i) we understand that certain assets may be operated by individuals or sole traders; and (ii) we anticipate that the pilot / RecorDER may be extended in the future to smaller assets and that this may, ultimately, include assets on domestic or small business premises.

4.5 **Question**: to what extend will PDPL limit with whom SWRR Data can be shared and to what use it can be put?

4.5.1 If SWRR Data is personal data and subject to PDPL it would only be possible to process such for specific, clearly defined purposes. Such purposes would need to be communicated to the individuals to whom the SWRR Data relates by means of a privacy notice, at the time

when the data is collected if it is collected directly from the individuals. If the data is not collected directly from the individual (i.e. it is obtained from a third party) the privacy notice must be provided to the individual within one month from when the data is collected or (sooner) before the data is shared.

4.5.2 Apart from the purposes of processing, other information needs to be provided to individuals in the privacy notice, such as information about the specific categories of recipients with whom the information may be shared.

4.5.3 It is difficult to process data in a manner which is different from that which is described in the privacy notice which has been provided to the individual. Unless it can be demonstrated that the purpose of any new processing activity is *compatible* with a purpose of processing set out in a privacy notice, it would only be possible to carry out the new processing activity if the individual *consents* to the new purpose of processing. If there was a legal obligation to process the personal data for a specific purpose (as envisaged by the recommendations in the energy regulation section of this report) the processing for that defined purpose provides a lawful ground to permit the processing.

4.5.4 To determine if the new purpose is compatible an assessment of the new purpose needs to be conducted, by reference to the original purpose. This has to consider; whether there is a link between the purposes, the context in which the data was initially collected and in particular the relationship with the individual, the nature of the data, whether this sharing will have any consequences for the individuals, and safeguards that can be put in place (such as the use of pseudonymisation, which is being considered for the SWRR Data).

4.5.5 The GDPR requirement of 'fairness' is also a relevant consideration. Fairness is not defined. Once the Data Access Controller provides a privacy notice to a customer setting out the purposes for which SWRR Data can be used by DNOs, any use by a DNO recipient of the SWRR Data for a different purpose could constitute a breach of the requirement of fairness, even if the DNO provides a privacy notice to the individual setting out the additional purpose of processing. Since the application of the GDPR, the data protection regulators consider transparency and fairness requirements to be of significant importance for compliance.

4.5.6 The concept of fairness and lawfulness for processing personal data is not limited to the PDPL. The UA requirements set out above, if breached, would be taken into account by the data protection regulator in any determination of whether there is PDPL compliance, particularly with regard to the first data protection principle - processing must be 'transparent, lawful and fair'.

4.5.7 Clarity (and limitations) on the purposes of processing and the identity of the recipients of the SWRR Data is needed from the outset.

4.5.8 **Use of Blockchain technology**: the RecorDER Project intends to use blockchain technology, which raises some additional PDPL compliance challenges. There is no agreed GDPR level of guidance on the use of blockchain and but it has been confirmed by a number of the data protection authorities including the ICO in the United Kingdom that the use of blockchain for processing personal data will need to comply with the GDPR. Blockchain, of itself, is not a 'processing purpose' but it operationally processes personal data for the defined purposes. There are a number of different types of 'blockchain' technology.

4.5.9 The main properties of blockchain technology that give rise to the GDPR concerns are:

(a) **transparency**: the participants can view all the data recorded, which may allow 'access' to data beyond what is necessary for each participant.

(b) **security**: several copies of the blockchain co-exist on different computers.

(c) **irreversibility**: once recorded, it cannot be altered or removed, and

(d) **decision-making**: whether there will be consensus decision-making or one participant (or another body) will be delegated the decision-making responsibilities. We understand that there will be dedicated governance oversight.

4.5.10 The type of blockchain that we understand will be used in implementation of the RecorDER Project will have an affect on the approach taken to GDPR compliance for any SWRR Data that comprises personal data. The aspects for GDPR compliance that need to be considered for use of blockchain in the RecorDER Project are:

(a) **Type of blockchain; public, permissioned, or private**: private blockchain raises the fewest GDPR issues as it functions similar to a distributed database.

(b) **Awareness of the two types of data processing; participant and, 'payload' or stored data:** the participant data will be personal data, if individuals have identifiers for access to the blockchain. For access and security, it is likely there may be personal ID's rather than company IDs, but this is a matter to be considered. Where the stored data is SWRR Data relating to individuals, it will be personal data.

(c) **Demonstrating compliance accountability**: for example, the blockchain can be used for demonstrating consent and that confirmation of the operations of the shared data.

(d) **The roles the parties will perform; e.g. participant or miner**: this is discussed further as the role of the party will impact whether the party is acting as a data controller or processor.

(e) **Rights of data subjects**: while blockchain can facilitate some data subject rights, others are more challenging, based on the nature of the right and the nature of the blockchain. In particular, the right to erasure, right to rectification, and the right to object are problematic to realise. Once data is on the blockchain it remains there. It may be possible to effectively make the data 'practically inaccessible', which some data protection authorities have indicated, may be a practical solution.

(f) **The GDPR requires privacy by design and default:** the use of blockchain will likely require a DPIA to be conducted at various stages of the development, to ensure the processing has adequate safeguards for the data subjects, their rights can 'effectively' be exercised, roles of the parties are defined and responsibilities and obligations are documented.

4.6 **Question**: what differences are there in PDPL limitations in respect of data relating to legal persons and date relating to natural persons, e.g. residential energy customers?

4.6.1 The distinction between legal persons and natural persons is essential to the application of PDPL and crucial for assessing PDPL risks arising in connection with the RecorDER Project. PDPL only applies to information which relates to living natural persons (i.e. individuals). Therefore, at this point in the development of the RecorDER Project, given the scale of DER assets under consideration, the PDPL risk is not as high as it would be if smaller assets and a higher proportion of residential sites were included. However, "**natural persons**" includes individuals acting in the course of their profession or trade, and unincorporated partnerships and as identified in section 4.4.1 could include sole traders operating larger generation assets, such as PV assets on a farming site.

4.7 **Question**: what are the sanctions for non-compliance with PDPL?

4.7.1 In the UK PDPL is enforced by the Information Commissioner ("**ICO**").

4.7.2 The risk of enforcement action is relevant to all parties processing SWRR Data.

4.7.3 Monetary penalties are the most well-known sanctions for non-compliance. The highest penalties which may be imposed for breaches of PDPL are €20,000,000 or 4% of global annual turnover. These may vary greatly and depend on numerous factors including the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, and the categories of personal data affected.

4.7.4 Monetary penalties are not the only enforcement power available to the ICO. The ICO may require the production of information, carry out mandatory audits, and issue enforcement orders requiring the taking of specific action (or refraining from taking action). These can include an order to stop sharing or otherwise processing data.

4.8 **Question**: do the SWRR Data data fields proposed fall within scope of the General Data Protection Regulations? If so, which ones?

4.8.1 Where SWRR Data relates to an individual, it is likely that all the relevant SWRR Data will constitute personal data.

4.8.2 Personal data is not limited to identifiers such as the customer name, and removing the customer name would not exclude SWRR Data from qualifying as personal data.

4.8.3 Where the different fields of data are (or can be) linked together, it would not be the case that the identifier is personal data, and the associated technical data (e.g. point of supply) is not. All the information associated with that identifier would qualify as personal data.

4.8.4 It is not necessary for information to directly identify an individual for it to qualify as personal data as long as it relates to an individual who can be identified, even if indirectly.

4.8.5 More information on the qualification of combinations of data fields as personal data, and the possibility of excluding the scope of PDPL by eliminating personal data, is included in the section 4.9.9.

4.8.6 Note that personal data does not need to be private in nature.

4.9 **Question**: in terms of the application of PDPL to the RecorDER Project:

- are the types or combinations of connection data contained within the SWRR Data personal data?
- Is it possible to anonymise or reduce data points to make it non-personal data?
- If the GSP/BSP is considered to be 'personal' data, is the aggregation of customers at a voltage level higher than where they are connected sufficient to protect anonymity?
- Is capacity and load information considered personal data?

4.9.1 We understand that under the RecorDER Project all the data fields will be held together and they cannot be disaggregated (although we understand that customer names may be removed – but this will not, in and of itself, prevent the data from being personal data – see detailed explanation below).

4.9.2 Technical data, such as information relating to a primary substation, would not, on its own, constitute personal data. If it is linked to an individual it may nevertheless constitute personal data.

4.9.3 Personal data is information which relates to an identified or identifiable individual. According to the guidance of the European Data Protection Board (Opinion 4/2007), information may relate to an individual because:

(a) it is about the individual; or

(b) it is processed for evaluating or making decisions which affect an individual; or

(c) its use is likely to have an impact on an individual's rights and interests.

4.9.4 When connection data is linked to other data which constitutes personal data, such connection data is also likely to satisfy one of the above conditions.

4.9.5 If a data field ('a') which is essential for linking other data fields ('b') to an individual, is separated from the other data fields in such manner that the other data fields ('b') can no longer be linked to an individual, the other data fields ('b') would no longer constitute personal data. However, it must not be possible to reverse the separation (i.e. reconnect the essential data field ('a') with the remaining data fields ('b')), which can be achieved by deleting the essential data ('a'). This would likely have a significant adverse impact on the value of the data.

4.9.6 A direct identifier is not necessary for information to be linked to an individual and qualify as personal data. This is because the definition of personal data includes information which relates to an *identifiable* individual. An individual is identifiable not only when a direct identifier (e.g. a customer name) is used, but also where the information is unique so that it only relates to a particular individual or a household and the individual can be identified by combining that information with additional information, even if that additional information is held by a third party. Therefore, removing the customer's name is unlikely to be an effective means to exclude the application of PDPL to the information. For example, if a customer's name was replaced by an automatically generated ID but data associated with or generated over time in respect of that ID is unique to that ID and that unique information combined with other information could be used to identify the relevant individual.

4.9.7 Customer names are also not the only form of identifier. MPANs, being unique numbers, constitute an identifier when they relate to a household, and information linked to an MPAN would be personal data. Although a household may include more than a single individual, the information associated with that household is likely to reveal information relating to one member of that household (e.g. the bill payer). Information relating to a group of people may also constitute personal data of members of the group who are identifiable. It is now accepted that IP addresses constitute personal data. The MPAN is similar and comparable to an IP address.

4.9.8 SWRR Data would not be personal data if it is aggregated in such manner that it is no longer possible to link it to an individual. The aggregation must be such that it cannot be reversed or reverse engineered. Aggregation may also have a significant adverse impact on the value of the data but if it is possible to only disclose aggregated data to DNOs, such data would not constitute personal data in the hands of the DNOs (although the Data Access Controller would still process the underlying SWRR Data).

4.9.9 Although anonymization and aggregation may be difficult to achieve, pseudonmysation is an effective security measure which should be considered. Pseudonmysation involves separating information which is required to identify an individual from other information, and ensuring that the two are kept separate. Whilst this does not achieve anonymization since it would be possible to recombine the data, pseudonmysation helps satisfy the obligations of PDPL and may significantly reduce the risks associated with processing personal data.

4.10 **Question**: in the future SWRR Data may also include more installations such as domestic roof-top PV, domestic batteries and Electric Vehicles where it is more likely that personal data will be shared. From a GDPR perspective, who would be the data controller(s) and who would be the processor and for what lawful purposes?

4.10.1 The classification of controllers and processors depends on the practical context of the data processing and should be revisited once the governance model is finalised.

4.10.2 DNOs would process any SWRR Data they are provided access to for their own purposes and benefit. As a result they would be controllers of such data.

4.10.3 The role of the Data Access Controller is also likely to be that of a controller if it has autonomy in relation to matters such as what data is put on the platform and which DNOs are given access to the data. However if such decisions are made on the basis of specific pre-defined criteria set by the DNOs or other third parties (e.g. a separate governing body), such that the role of the Data Access Controller is relegated to that of an administrator of those criteria, the Data Access Controller may be considered a processor acting on behalf of the controller (or controllers) which sets the criteria.

4.10.4 If the SWRR Data is not held by the Asset Owners or Operators, or by the Data Access Controller or a DNO, the host is likely to be a processor of the data if its role is limited to hosting the data and does not involve making decisions relating to the data (other than technical decisions).

4.10.5 There is a possibility that parties involved in setting up the register and pooling in data are considered to be joint controllers because they jointly determine the purpose of the processing.

4.10.6 The use of blockchain technology will also have to be considered to determine whether a party is acting a participant (in which case they are likely to be considered as a controller), or as a miner (in which case they are likely to be considered as a processor). If the parties are jointly making the decisions for the - e.g. there is a common purpose, there is a risk they will be considered as joint controllers. However, if an association is set up for governance and decision-making (or a participant is given that role), then it is arguable they will be the data controller.

4.10.7 These matters should be considered in more detail when the governance model is being finalised.

4.11 **Question**: what are the possible legal conditions available or restrictions for the sharing or publication of Special Category or Conviction and Offences Data?

4.11.1 It is unlikely that SWRR Data would constitute special category or criminal offences data. This would however need to be considered on a case by case basis. Although the possibility may be remote, if data linked to an MPAN enables information to be inferred which, for example, relates to an individual's health or religious beliefs, it would potentially constitute special category data.

4.11.2 The lawful bases for processing such data are restrictive and explicit consent may need to be obtained.

4.12 **Question**: what changes would be required to the respective DNOs' privacy policies and other compliance policies?

4.12.1 DNOs would need to communicate the purposes for which they process SWRR Data and other information required by the GDPR to be provided by means of privacy policies, such as information about automated decision-making involving the SWRR Data, to individuals whose personal data is processed. If DNOs are not able to provide such information directly it may be appropriate to flow down the obligation to provide such information to the Data Access Controller, although they would need to ensure that appropriate information is provided and, that the information is actually provided.

4.12.2 DNOs would also need to update their records of processing to take into account the processing of SWRR Data.

4.12.3 In addition, DNOs would need to consider if a DPIA should be carried out before processing SWRR Data, and if any existing DPIAs relating to ongoing processing activities need to be updated to reflect the involvement of SWRR Data. A DPIA is required where the processing may involve a high risk to individuals. The matching of datasets and use of new technology are relevant factors to determine whether a DPIA is required, and we are of the view that a DPIA is likely to be required before processing SWRR Data. It is possible for all DNOs to

prepare a combined DPIA which covers the use of SWRR Data, although each DNO would need to ensure that the DPIA remains relevant to its individual processing activities.

4.12.4 Finally, DNOs would need to consider what updates may be required to their procedures for responding to data subjects rights, and their security policies and procedures.

4.13 **Question**: what are the options for who is responsible for dealing with data subject requests and the Information Commissioner's Office for the shared or published data?

4.13.1 Responsibility for dealing with data subject requests rests with the controller of the data. The answer to this question therefore requires the role of the parties to be conclusively determined.

4.13.2 An independent controller may delegate responsibility for dealing with data subject requests to a third party however the controller would remain ultimately responsible for compliance with such requests.

4.13.3 In practice the Data Access Controller may be better placed to coordinate efforts to respond to requests. If it is assessed to be a controller in relation to the hosting of data on the platform and the sharing of data with DNOs, it would also have legal responsibility for dealing with requests relating to such processing.

4.13.4 In the event that any of the parties are considered to be joint controllers in relation to certain processing activities, they would be required to have arrangements in place which set out how such requests are dealt with. Responsibility for responding to such requests may be shared (e.g. each controller deals with requests it receives) or delegated to one of the controllers. In the latter case the assistance of the other controllers would still likely be required.

4.13.5 As a practical and financial matter for discussion once the governance structure and role(s) of the parties are finalised; there are associated costs and resource implications for the party that undertakes this responsibility (or has shared/joint responsibility). At times data subject requests (and other compliance obligations) and, potentially associated complaints to the ICO or other regulators can incur actual costs and a significant amount of time in handling those enquiries and responding. When considering the governance structure, there should be an appreciation of these additional compliance obligations when the parties allocate responsibilities.

4.14 **Question**: what would happen if a customer objected to the sharing of the data:

- would the DNO be compelled to remove the data in question?
- What happens to the data if site no longer has a customer or active service use?
- does the data need to be removed?
- what happens to the data if there is a change of account holder?
- how long is the data stored for?

4.14.1 The applicability of the rights of data subjects depends on the legal basis relied upon.

4.14.2 If consent is relied upon as a legal basis of processing, the customer could withdraw consent at any time and the DNO would need to ensure that the customer is able to do so. This would not affect the validity of processing already carried out on the basis of consent before it is withdrawn, however it would require the DNO not to further process the data for RecorDER purposes and the data may need to be deleted unless there is another legal basis for processing it.

4.14.3 However as noted above consent is not the only legal basis available to DNOs and other legal bases may be more appropriate.

4.14.4 Necessity for legitimate interests may be a more appropriate legal basis and is available where the rights and freedoms of the individual do not outweigh the legitimate interests pursued. Where this legal basis is relied upon the customer would be able to object to the processing on grounds relating to his or her particular situation, however this would not automatically stop the processing. The DNO would need to consider if it has compelling legitimate grounds to continue the processing which override the rights and freedoms of the individual. If it is able to demonstrate such compelling legitimate grounds, it may continue the processing (although the customer would still have a right to complain to the ICO as parts of the data subject rights an individual has under UK PDPL). On the other hand, if it is not able to demonstrate such compelling legitimate grounds, it would need to cease the processing and, similar to when consent is withdrawn, the data may need to be deleted unless there is another legal basis for processing it.

4.14.5 Data does not need to be deleted until it is no longer needed for the purpose for which it is processed. PDPL does not prescribe specific retention periods but allows for commercial and practical considerations to be taken into account. Although a customer may request the erasure of personal data, this right is not absolute and, does not apply where the data is still required for the purpose for which it is processed (unless consent is relied upon as a legal basis and is withdrawn or, the customer makes a successful objection to processing based on legitimate interests).

4.14.6 If data does not relate to an individual customer, it would not constitute personal data and there would be no requirements under PDPL to delete the data.

4.14.7 What happens when there is a change in account holder depends on the legal basis relied upon. If consent is relied upon the consent of the new account holder would likely be required, however this is another reason why consent may not be the most appropriate legal basis.

4.15 **Question**: are there any other areas of relevant privacy legislation besides PDPL?

4.15.1 **NIS:** The potential implications of NIS need to be considered further. In the field of **electricity**, NIS applies to electricity supply and electricity transmission where a minimum threshold is met for the service to qualify as an essential service.

4.15.2 Even if NIS does not apply directly, incidents affecting RecorDER may have an impact on the ability of DNOs who become reliant on the continued availability of SWRR Data, to comply with their obligations under NIS.

4.15.3 There are no other specific e-privacy issues concerned with RecorDER for sharing data. If the data is used to for sending unsolicited electronic marketing to an individual, this will be in violation of the UK Privacy and Electronic Communications Regulations (PECR), but we do not believe this is an intended use case under the RecorDER project. The EU proposed a new ePrivacy Regulation to replace the current ePrivacy Directive. As at November 2019, the proposed new regulation, remains in the EU legislative process. It should be monitored during the development of RecorDER to ensure any new requirements or proposed changes are known and considered.

4.15.4 **Commercial or government sensitive sites:** There is a potential that certain sites will be either commercially sensitive (such as major data-centres) or security sensitive (such as a government site; e.g. owned by the Ministry of Defence). Often there may be a term within contracts prohibiting the use by another party of the data for any purpose other than the provision of the service. Similarly, for government sites, there may be security classification indicating that information about the site such not be used or disclosed for any other purpose without express prior permission. There should be a mechanism for 'tagging' or noting such sites to ensure that the site details or location data is not placed on the platform without appropriate clearance, or subject to additional measures.

4.16 **Recommendations**

4.16.1 Any sharing of personal data through the requirement of 'consent' under the Utilities Act, will for the purpose of data protection laws, need to meet the GDPR 'consent' conditions and other compliance requirements. The Energy Regulation recommendations set out in section 2.4.1, if followed, would require the disclosure of SWRR Data by law and will provide an alternative legal basis for the data sharing and use. A different legal processing ground will be less administratively burdensome.

4.16.2 GDPR compliance obligations and accountability will need to be considered and incorporated into the project's procedures and polices as they are being developed to ensure that a) personal data will be identified when it will be shared as part of the SWRR Data and, b) the procedures will be applicable for ensuring GDPR compliance by all the participants.

4.16.3 As part of developing the technical model for sharing the data and the overall governance model or structure, decisions need to be made about which participants have decision-making responsibilities for the SWRR Data, as this may impact on whether all participants are joint controllers for all project processing, or there are individual data controllers. The governance and participation agreement will need to cover all GDPR contractual requirements, and related issues such as liability depending on the relationship of the different participants.

4.16.4 In addition to the general GDPR compliance for sharing and use of SWRR Data, the use of the type of blockchain technology will need to be considered, as some blockchain technology will create greater GDPR compliance obligations. Additionally, due to the nature of the technology, processes will need to be designed to ensure that 'functionally' some data subject rights can be exercised. Further, there will need to be GDPR compliance for the blockchain participants. The agreements for participation will need to include provisions for GDPR compliance and related issues, such as different levels of security (i.e. sensitive and critical sites) and liability.

4.16.5 As the RecorDER Project develops, then in its procedures and polices there will need to be consideration given as to whether it is necessary to identify 'sensitive' sites that may require additional permissions or protections under contract or due to government security classification before that data is used.

5. LAW OF CONFIDENCE AND CONFIDENTIALITY

5.1 In this section we consider questions identified by the RecorDER Project partners in relation to the extent to which the application of the law of confidence and confidentiality undertakings may prevent or restrict the sharing of data envisaged under the RecorDER Project.

5.2 As well as addressing the general application of the law of confidence to the RecorDER project and the application of express obligations of confidentiality in relevant industry contracts, the questions addressed in this section include:

5.2.1 If the contracts we have on file are silent on confidentiality (or in the absence of a contract), does this mean that no confidentiality law applies to the use of SWRR Data or is there other applicable UK legislation that may prevent publication?

5.2.2 how should we treat sites of national security, first responders (i.e. MOD, hospitals) where agreements do not specifically refer to confidentiality or where the agreement is absent?

5.2.3 notwithstanding any legislation of universal applicability, are there any specific legislative issues connected with sharing information that may directly or indirectly relate to critical national infrastructure such as sewerage/water treatment sites/major transport infrastructure (such as rail, tube and airports) and prisons as well as MOD and hospital sites?

5.3 **Introduction**: Confidential information may be protected through statutory provisions, under the common law or by express contractual obligations. In this section of the report we consider each and the implications for the RecorDER Project and the proposed use of information under it. Building on the commentary in the Energy Regulation section above, we conclude that it is possible that certain classes of information which will be shared as part of the RecorDER Project may be regarded as the confidential information of third parties (primarily connectees and asset operators) and that this may act as an impediment to the proposed data-sharing. This creates a potential risk for the participants in the RecorDER Project. In this section of the report we assess that risk and suggest steps that might be taken to mitigate or otherwise address that risk.

5.4 **The common law of confidence**

5.4.1 Under the common law it is settled that, for information to be protected as confidential, it must:

(a) have the necessary 'quality of confidence', and

(b) be imparted in a 'situation imposing an obligation of confidence'

5.4.2 Where these criteria are met, the recipient of the information will owe a duty of confidence and any unauthorised use to the detriment of the 'owner' of the information may give rise to a cause of action. These requirements are attributed to the *Coco v Clark* case*(Coco v A. N. Clark (Engineers) Ltd* [1969] RPC 41*)* and were approved in *Attorney General v Guardian Newspapers (No 2) (Attorney-General v Guardian Newspapers (No 2)* [1990] 1 AC 109 case *)*.

5.4.3 Taking these requirements in turn:

(a) **The necessary 'quality of confidence'**: the first requirement to be satisfied is that the information must have the necessary 'quality of confidence'. Generally, this means the information must **not** be something which is in the public domain, trivial or lacking in any usefulness or which has been developed or derived independently already by the recipient of the information. In many cases it will be readily apparent that information has the necessary 'quality of confidence', however this is also an area which can give rise to disputes and it can be difficult to define what exactly is claimed as confidential and to justify why this should be so. Equally, it may not necessarily follow that because information (or part of it) may be accessible publicly in some way that a data-set of which it forms part falls within the public domain.

For example, a set of information may have been collated within an organisation in circumstances where the information has value and where significant effort has been put into collating it, but some of the information might have been gathered from public domain sources. This does not mean that the collated information is non-confidential. For example, in *The Racing Partnership Limited v Done Brothers (Cash Betting) Limited*, it was held that the information about specific horse racecourses had the necessary quality of confidence because although the information was potentially publicly available, the ability to collect it and distribute it could be (and had been) limited.

(b) **Situations imposing an obligation of confidence**: an obligation of confidence may arise through a contract or through equity as a result of the nature of the relationship between the parties concerned. Whether an obligation of confidence arises will depend on the facts in each case. In *Coco v Clark* the question was posed as follows:

'if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable

grounds the information was being given to him in confidence, then this should suffice to impose upon him the equitable obligation of confidence.'

This means that the nature of the information is also relevant to whether there would be a situation imposing an obligation of confidence. For example, if someone was accidentally given the secret recipe to a well-known drink, it might be deemed reasonable for them to know that it was confidential, such that a duty of confidence arose, without in fact being expressly told that that was the case.

5.4.4 **Breach of confidence**: a breach of confidence arises in the situation where, once it has been determined that a duty of confidence exists, the recipient of the information makes an unauthorised disclosure or use of the confidential information. A breach does not always require a disclosure of the information in question. A use of the information which goes beyond the purpose for which it was provided, and to the detriment of the party who provided it, may also be a breach. For this reason it may often be difficult to establish that information lawfully in the possession of a party has actually been misused.

While in many cases it will be obvious that confidential information has been disclosed or used in breach of a duty of confidence, there are also a number of grey areas. In particular, as noted above, whether that obligation has been breached, may depend on the circumstances in which the information was received and the nature of the information in question.

To establish a breach, one must demonstrate that unauthorised use of that information has occurred and that is to the detriment of the person communicating it.

5.4.5 **Remedies**: the remedies available in an action for breach of confidence are similar to those obtainable for infringement of intellectual property rights. They are:

(a) **Damages**: the usual measure of damages is compensatory i.e. the defendant should compensate the claimant for the losses caused by the breach. Commonly damages are assessed on a reasonable royalty, i.e. what would the claimant (as a willing licensor) have charged the defendant (as a willing licensee) in order to use the information for the purposes for which they have been used;

(b) **Account of profits**: as an alternative to damages, a claimant may be awarded an account of profits. This is an equitable remedy according to which the defendant must pay the profits generated as a result of the breach to the claimant. Frequently however, it is extremely difficult to calculate the proportion of the defendant's profits which are attributable to the breach and therefore the remedy is only really pursued in exceptional cases.

(c) **Injunction**: essentially the same principles apply here as apply to injunctions for infringements of other IP rights. The difference is that, with breach of confidence, more often than not, the need is to have an injunction restraining disclosure which has not happened yet but is threatened. However, it is also possible, once an unauthorised disclosure has been made, to obtain an injunction to prevent its further use or dissemination. The courts recognise that, even if information is no longer confidential, it could still be appropriate for there to be an injunction because the fact the breach has occurred does not relieve the person of the duty to keep that information confidential and not misuse it. There is a general springboard principle that a wrongful activity should not be allowed to be used as a head start to get into the market.

(d) **Delivery up or destruction**: where confidential information which is the subject of a dispute is contained in physical materials, a claimant may ask the court to order that these are returned to the claimant or destroyed. Such an order may

also extend to products which are generated as a result of the misuse of information.

5.5 Application of common law of confidence to the RecorDER Project

5.5.1 Based on our understanding of the data fields proposed for use in the RecorDER Project much, but not all, of the information within those data fields is already in the public domain and would appear not to have the necessary quality of confidence about it. We also understand that in respect of a number of the data fields the information has not *per se* been obtained by the relevant DNO directly from a customer in circumstances in which one might infer an obligation of confidence.

5.5.2 Nonetheless, as is described in the commentary on energy regulation above, we understand that certain information within the relevant data fields may not already be in the public domain and may be regarded by the connectee or operator of the relevant asset as confidential. Examples include customer name, site and sub-station information. To the extent that such information has been obtained from, or imparted by, the relevant asset operator or connectee, and is not either in the public domain or trivial in nature, there is a reasonable risk that such information would be protected by the common law of confidence and that unauthorised publication of that information, whether by disclosure to other participants in the RecorDER Project or through wider publication as is anticipated in the Open Networks SWRR project, would be actionable.

5.5.3 As part of our discussions with RecorDER stakeholders it was also noted that it is possible that information may be in the public domain as a result of a DNO or other person having previously breached the common law of confidence. In that scenario, whilst a third party unaware of that prior breach may be able to rely on the fact that the information no longer has the necessary quality of confidence, the original disclosing party may not be able to do so and they may be liable for any further loss resulting from that subsequent (and potentially wider) disclosure.

5.5.4 In the scope of work and questions above we are asked to consider whether it matters if the data in question relates to critical infrastructure or site of national security. We address this from the statutory perspective of the NIS Regulations elsewhere in this report, but from a law of confidence perspective, clearly, if that information is more sensitive because of the nature of the site to which it relates and it is not already readily available in the public domain, then it is more likely to have about it the necessary quality of confidence and to satisfy the other requirements of the law of confidence. Therefore, in the round, these sites can be regarded as higher risk from the perspective of a potential breach of confidence.

5.6 Risk profile

5.6.1 The question then arises, what risk flows from the unauthorised disclosure or use of confidential information obtained from an asset operator or connectee. Based on our understanding of the data being shared, in most cases we do not envisage significant economic harm or loss arising from disclosure or use of the data fields identified as part of the RecorDER Project. As such, the legal remedies available to the person whose confidential information is disclosed may be limited, in the absence of any easily identifiable loss or specific harm.

5.6.2 However, even with a relatively low risk profile, we doubt any DNO will wish to knowingly breach the law of confidence and potentially damage the commercial relationship with a counter-party. In any event, the fact that such disclosure will likely result at the same time in the breach of statutory and regulatory obligations (see energy regulation comment above) means that taking an aggressive view to risk from a law of confidence perspective is, we would have thought, a moot point if that will also result in a breach of energy law or regulatory obligations, which may have more obvious and serious repercussions for a regulated DNO. Therefore, we envisage that the participants in the RecorDER Project will wish to explore ways in which to mitigate or the risk of breaching the law of confidence.

5.7 Mitigating Action / Potential Resolutions

5.7.1 What then is to be done to address the apparent risk that sharing certain of the categories of data fields as part of RecorDER Project may result in a breach of confidence.

(a) **Express consent**: we understand that to obtain express consent from each person who may have provided information that is protected by the law of confidence and is to be shared as part of RecorDER is a significant undertaking and not currently a particularly attractive practical solution, with the real risk that organisations may not respond or refuse to grant consent, on the basis that this will be an easier course of action than to issue an informed consent to the proposed disclosure. If a blanket approach was taken, it also creates an inference that all of the data fields are confidential in nature, when in fact it appears that only a number fall into that category. There is also a justifiable concern, which has been identified by participants in RecorDER already, that on transfer of an asset to a new owner, consent given by the previous asset operator may need to be replaced with a consent from the new asset operator in respect of any confidential information relating to their identity or their use of the asset. Nonetheless, consent from asset owners is an option for addressing law of confidence concerns and is accordingly identified as such in section 2.5.

(b) **Implied consent**: it might be possible to write to the counter-parties to whom the information relates to advise them of the project and to explain the categories of information (some of which may relate to them) that is intended to be shared as part of RecorDER and to invite any objections within a specified period. If no objection is forthcoming one may infer consent. This would still be time-consuming and would not create the certainty of obtaining express consent. Unlike obtaining express consent, it would also not overcome some of the parallel challenges that arise from the perspective of energy law and regulation as outlined above and would not address the issue of change of asset ownership highlighted above.

(c) **Contract remediation**: one might embark on an industry-wide contract remediation programme, such as has been done to enable GDPR compliance, with a view to providing the express rights of disclosure for the relevant data fields in the relevant industry contracts. The benefits and challenges of taking this approach are much the same as with obtaining a stand-alone express consent as are the costs and time involved. Accordingly, we do not believe that this is a practical option.

(d) **Audit data fields**: we understand that much of the SWRR Data is in the public domain and the sharing of that data will not *per se* constitute a breach of confidence. It may be possible to audit the data fields proposed for disclosure and remove those most likely to contain information that may be the confidential information of another person from the ambit of the RecorDER Project. We understand that tis might be time-consuming and impractical and impact adversely on the potential benefits to be gained from RecorDER.

(e) **Change of law / regulation**: if the law required a DNO to disclose or publish the data fields in question for the purposes and use anticipated by RecorDER, then such disclosure or publication would not constitute a breach of the law of confidence. This aligns with recommendations made above with respect to issues arising from an energy regulation perspective. However, the disclosure requirement would have to be established as a legal obligation rather than an exception to energy legislation restrictions on data disclosure if it is to be effective from a law of confidence perspective. One might look to freedom of information laws in the UK for as example of legislation which requires the disclosure of information with limited exemptions.

5.8 Express obligations of confidentiality

5.8.1 It is common practice in commercial contracts to include a confidentiality clause that supplements the common law and sets out in express terms the obligations of confidentiality that exist between the parties to that contract. The advantages of doing so include contractual certainty as to the scope of the duties of the parties and making it easier to infer that a duty of confidence exists from the circumstances of the disclosure.

5.8.2 We have been advised that many of the connection and related agreements that are in scope here do not include express confidentiality obligations. We have examined a sample of such agreements and found that to be the case. However, we have also examined a sample of agreements that do contain such provisions. We have found that the confidentiality obligations, whilst, in many ways, relatively standard in form, they do contain certain provisions that are quite industry specific.

5.8.3 In many cases the issues arising from a confidentiality perspective are not significantly different than would arise under the common law of confidence and the remedies for breach of such provisions are essentially as set out above. However, it is noted that in some contracts the terms of the contract and details set out in them are expressly prohibited from disclosure and we understand that those details may in certain cases fall within the data fields that fall to be shared under the RecorDER Project.

5.8.4 More helpfully the contracts we examined that do have express obligations of confidentiality contain a range of exceptions to the confidentiality and non-use obligations. These range from a general exception to enable disclosure of information required by law or a court order, to more industry-specific exemptions, such as a right to disclose information as required by industry agreements, codes and licence conditions. If relevant industry codes and regulations are changed to require disclosure by DNOs of the SWRR Data fields for certain permitted uses, then it appears from our review of the sample contracts provided that express exemptions to contractual obligations of confidentiality would be sufficiently broad to cover the relevant disclosure.

5.9 Confidentiality – Trade Secrets Regulations

5.9.1 In June 2018, the Trade Secrets Directive was implemented in the UK via the Trade Secrets (Enforcement, etc) Regulations 2018, SI 2018/597 (the Trade Secrets Regulations) which brought the protection of confidential information onto the UK statute book for the first time.

5.9.2 Regulation 2 of the Trade Secrets Regulations introduced a definition of ‘trade secret’ as follows:

(a) '"trade secret" means information which meets all of the following requirements:

(i) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

5.9.3 Based on our understanding of the nature of the SWRR Data, we do not believe that this data constitutes a "trade secret" (as defined under the Regulations) and so the report does not address the specific application or affect of the Regulations on the RecorDER Project.

5.10 Recommendations

5.10.1 By following the Energy Regulation recommendations set out in section 3 a DNO would be required by law to disclose the SWRR Data that they hold. If that is the case, then compliance by a DNO with that requirement would not be in breach of the common law of

confidence and such disclosure would fall within the exceptions to the express obligations of confidentiality in the sample contracts reviewed by us.

5.10.2 Obtaining consent to data use from the relevant asset owners would also remove the risk of a breach of confidence, but currently it is questionable whether it is practically feasible to implement such a recommendation.

6. CONSENT

6.1 In this section we consider questions identified by the RecorDER Project partners in relation to the extent to which obtaining consent from those to which SWRR Data relates may enable the sharing of data envisaged under the RecorDER Project.

6.2 Specifically, we were asked to consider the following questions:

6.2.1 Is it possible to share and publish SWRR Data without the consent of the relevant customer?

6.2.2 Where there is express consent from a customer (whether in the Connection Agreement or otherwise), would this override the legislative barriers?

6.2.3 Where consent is deemed to be a solution, how will this work in practice over time where the DNO will not know if a customer has sold its interest in a site to a third party who has not consented to data sharing?

6.2.4 Where there is express prohibition from a customer (whether in the Connection Agreement or otherwise) regarding the sharing or publishing of all or any of the SWRR Data, could this be overridden by a change to the licence conditions permitting /requiring the sharing or publishing of data the same as or similar to the SWRR Data?

6.2.5 In the event that specific consent clauses weren't included in the Connection Agreement and there is legislation in place to protect use of data the same as or similar to SWRR Data, what are the legal risks should we choose to publish? What recommendation would you make to mitigate the impact?

6.3 We have addressed these questions in the context of energy regulation and the law of confidence in sections 3 and 5. From a PDPL perspective it is worth looking beyond consent for a basis of processing personal data. Specifically:

6.3.1 For the purposes of satisfying a legal basis under PDPL, consent is not the only legal bases available to process personal data and a more appropriate legal basis may be available.

6.3.2 Necessity for legitimate interests may be a more appropriate legal basis and is available where the rights and freedoms of the individual do not outweigh the legitimate interests pursued. The legitimate interests of third parties can be used for this legal ground. However, it is likely that the parties processing of the SWRR Data will be processing the data for a purpose other than it was initially obtained. As mentioned above, there will need to be an assessment whether this new processing will be compatible with the original processing.

6.3.3 The criteria for the new processing purpose will also need to take into account the balancing exercise for the use of 'legitimate interests' (if this legal base will be used). As the individuals' whose data may be used will vary (initially it will be generators of more than >1MW, but it is anticipated that this will be extended to domestic customers), the assessment will need to reflect the nature and relationship with the different categories of individuals.

6.3.4 This should be considered further once the purposes of processing and conditions of access to the data are more clearly defined. Depending on the outcome of the assessments for legitimate interests and whether other processing purposes; it may be there are

restrictions, or limits on data use and additional conditions built into RecorDER to mitigate against any noted consequences to the individuals.

6.3.5 We note above that there is discussion of possible changes to under the Utilities Act and related legislation to licence requirements to permit, or require certain data sharing (for specific purposes). If such legislative changes were made, this may open up possibilities of additional legal bases for processing personal data under PDPL; such as processing in compliance of a legal obligation, or processing of a task carried out in the public interest. The use of these legal bases will depend on the exact nature of the changes to the other legislation. Even with such sector legislative changes, all other PDPL compliance obligations would still need to be met.

6.3.6 We note the discussion about consent under UA set out in the section on Energy Regulation above. For completeness, the PDPL has now established specific criteria for valid consent to be given if it is used as the legal ground for processing personal data. Any consent that may be relied on from the UA, also must comply with GDPR consent if it is personal data.

7. COMPETITION LAW

INTRODUCTION AND SCOPE

7.1 In this section we consider questions identified by the RecorDER Project partners in relation to the extent to which competition law may apply to the sharing of data envisaged under the RecorDER Project.

7.2 Specifically we were asked to consider:

7.2.1 Consideration of overall nature of the project, i.e. whether the arrangement between competing undertakings raises competition law concerns, or is pro-competitive in nature;

7.2.2 Consideration of data sharing and the competition law concerns this raises;

7.2.3 Consideration of how to manage competition law risks with data sharing, including how data is exchanged, stored and displayed.

7.3 While potential competition law risks can arise with a data sharing project of this type, we would consider that this risk can be managed given the overall nature of the RecorDER Project, together with the proposed controls and protocols which RecorDER will put in place.

7.4 From our understanding of the proposals for the project, we understand that commercially sensitive information is unlikely to be exchanged given that a large degree of the information is in the public domain, that controls are placed to prevent undertakings at the same level of the market from viewing one another's information, and that information which could affect the pricing of wholesale energy projects will not be exchanged.

APPLICATION OF COMPETITION LAW

General principles

7.5 There are two competition rules which could apply to the Project:

7.5.1 Chapter 1 of the Competition Act 1998 (the "**Chapter 1 Prohibition**")[5], prohibits anti-competitive agreements (as well as practices and behaviours that substitute competition for cooperation ("concerted practices"); and/or

7.5.2 Chapter 2 of the Competition Act 1998[6] (the "**Chapter 2 Prohibition**"), which prohibits abuse of a dominant position.

7.1 The Chapter 1 prohibition applies to agreements or concerted practices which have as their *object* or *effect* the prevention, restriction or distortion of competition. Agreements which are anti-competitive *by object* automatically infringe the competition law rules. This usually applies to serious infringements such as price fixing and market sharing.

7.2 Agreements can also infringe Chapter 1 if they have an *appreciable* anti-competitive *effect* on the relevant market. In the case of a horizontal agreement (between undertakings operating at the same level of the market), the effect of an agreement may be *de minimis* where the parties have a combined market share under 10%[7].

7.3 Whether or not an exchange of information has an appreciable anti-competitive *effect* on a market depends on the structure of the market (i.e. whether it is concentrated or highly fragmented), the number and size of the competitors involved in the information exchange (and their respective market shares) as well as the nature of the information exchanged, i.e. how strategic and commercially useful it is.

7.4 An agreement which falls within the scope of Chapter 1 can nevertheless qualify for an exemption provided that it achieves certain benefits or efficiencies which are passed on to consumers, and that any restrictions are the minimum necessary to achieve these benefits/efficiencies, and provided that competition is not eliminated in a substantial part of the market[8].

7.5 Agreements which infringe Chapter 1 are automatically unenforceable and the parties risk being fined up to 10% of their group global turnover. Third parties who suffer loss as a result of the agreement could also take action for damages.

7.6 In terms of Chapter 2, there is no exemption available for abuse of dominance, albeit actions cannot be abusive if they are "objectively justified". To establish dominance, it is usually necessary to define the relevant market. This can be particularly complex in platform and data markets, and usually requires the input of a specialist competition economist. There is a rebuttable presumption of dominance for undertakings which have a market share of 50% or above. An undertaking which abuses its dominant position can be fined up to 10% of group global turnover and third parties could take action for damages.

Information Sharing and competition law

7.7 The sharing of information between companies can raise competition concerns if the information is confidential and commercially useful, even if it is shared via a third party aggregator or platform.

7.8 The competition authorities have recently taken a number of decisions where information sharing (particularly in relation to pricing) has been found to be a serious infringement of Article 101/Chapter

[5] Chapter 1 is the UK equivalent of Article 101 of the Treaty on the Functioning of the European Union ("**TFEU**"), which applies when there is an effect on trade between Member States.
[6] Chapter 2 is the UK equivalent of Article 102 TFEU.
[7] Commission Communication: Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) (De Minimis Notice) (August 2014).
[8] Article 101(3) TFEU and Section 9 Competition Act 1998.

1, even in the case of a one-off exchange during a meeting[9],and in the case of a one-way disclosure[10].

7.9 The exchange of confidential, commercially sensitive ('strategic') information between competitors can amount to a 'by object' infringement of competition law, whether solicited or not; there is a presumption that it will be taken into account by the recipient, distorting the normal conditions of competition.[11] Strategic information is considered to be any non-public and current/future information which reduces strategic uncertainty in the market (e.g. recent or future information relating to prices, customer lists, production costs, volumes, turnovers, sales, capacities, marketing plans, risks, investments and technologies). Of this, future pricing and volumes information carries the highest risk as it will most likely be considered to have automatically infringed competition law as an 'object' infringement.

7.10 Indirect 'hub-and-spoke' exchanges of commercially sensitive information via third parties[12] / cases where third parties have acted as facilitators of exchanges (even ' when not active on the market themselves)[13] have also been captured by Chapter 1/Article 101. It is therefore possible that a software designer (or creator of a piece of algorithmic software) could serve as the 'hub' of an anti-competitive information exchange.[14]

THE TRANSFER OF DATA WITHIN THE RECORDER PROJECT

7.11 We understand that certain information on energy assets will be coordinated by the Project. In this context, there is an agreement between the coordinator and the data providers, or between the data providers themselves, that could fall within the scope of Chapter 1/Article 101 if the level of data sharing oversteps the mark in terms of what would be considered to be acceptable under the competition law rules. If it amounts to anti-competitive data sharing, the coordinating platform (i.e. RecorDER itself) could be held liable as a facilitator.

Genuinely public information?

7.12 Information is not considered to be confidential if it is "genuinely public", i.e. it is equally accessible to all competitors and to customers, both in terms of cost and access. We understand that some data shared by the Project may be "genuinely public", e.g. the information published by National Grid on its website (STOR and FFR information). Based on the information received to date, we consider that it is unlikely that all of the data shared in the Project would be considered to be "genuinely public" information because, although the data might be publically available in the sense that a physical search could reveal the location of assets, and the information on the majority of the data fields is available through public sources, we expect that it would involve logistically prohibitive time and cost to collate all this information, whereas the Project allows it all to be easily collated and available.

7.13 It may be the case that the asset information will be genuinely public in the future, but at the current time we understand that the data is only held by each market participant and not widely shared.

7.14 To the extent that any information on the platform is genuinely publicly available to all, sharing this information on the platform would not cause any competition law concerns. However, the remainder of the information which is or may be commercially confidential would have to comply with the competition rules set out below.

Anti-competitive object or effect

7.15 In this case, the legitimacy of the sharing of the data can be considered in the context of the wider industry aim of facilitating data access. We understand that the UK regulator, Ofgem, is in favour of

[9] See Case C-8/08 *T-Mobile Netherlands* [2009].
[10] *Loan products to professional service firms: investigation into anti-competitive practices.* CMA decision dated 20 January 2011.
[11] See Case C-8/08 *T-Mobile Netherlands* [2009].
[12] See Case CP/0480-01*Argos/Littlewoods/Hasbro* [2003].
[13] See Case C- 194/14 P *AC-Treuhand v Commission* [2015].
[14] See C-74/14 *Eturas* [2016] where an online booking platform automatically capped discounts for certain travel agents, with the administrator of the booking system facilitating the exchange. See also *Asus, Denon & Marantz, Phillips and Pioneer(AT.40465, 49469,40181, 40182)* [2018] where resale prices were fixed by retailers and the impact of this was heighten as the competing retailers used algorithmic software to adapt retail prices to those of their competitors.

the creation of the asset register. The Energy Data Taskforce report provided to UK Government (BEIS, Ofgem and Innovate UK)[15] (the "Report") concluded that data visibility as regards the energy market had clear benefits, summarised as follows[16]:

7.15.1 As the UK energy system becomes more disparate, diverse and decentralised in the future, data sharing will be crucial to coordinate the actors undertaking new roles and ensuring system stability;

7.15.2 Data openness will provide more pricing and market visibility, increase liquidity and drive investment into the correct technologies, locations and solutions;

7.15.3 Increased data visibility should deliver a better system and price outcome for consumers;

7.15.4 Enable faster and cheaper transformation programmes in an increasingly complex market;

7.15.5 Prevent increasingly fragmented datasets which will reduce efficiency;

7.15.6 Visibility of assets, their operation and how the interact with each other at a local and national level will reduce the risk of system stability;

7.15.7 Wide availability of system data will benefit all market participants, and prevent monopoly providers, or providers receiving customer subsidy, from solely benefitting from data access;

7.15.8 Prevent interoperability problems between market participants;

7.15.9 Enable market entry and innovation in order to create new products and technologies to improve 'customer experience, drive efficiencies and deliver carbon reductions.'

7.16 The specific benefits of an assets database are summarised as follows in the Report:[17]

7.16.1 Lower time to identify and plan renewable energy projects;

7.16.2 More efficient planning of future infrastructure across energy vectors;

7.16.3 Better visibility of adjacent sectors such as housing, heavy industry, water, waste etc.;

7.16.4 Enables faster testing of new business models for innovators;

7.16.5 Drive of data standardisation and interoperability;

7.16.6 Greater system resilience achieved through better system visibility.

7.17 This therefore suggests that the sharing of certain information by market participants with other participants / third-parties are likely to be permitted due to the benefits it will bring to the wider economy, and therefore it is unlikely to be considered as an *object* restriction.

7.18 Nevertheless, we understand that some of the information to be shared between the data providers (i.e., the DNOs, who could be considered competitors in related downstream markets for wholesale supply of electricity) may be commercially sensitive. Currently, we understand that this type of information could include customer name, service provider information, contractual descriptions and exclusivity terms, asset capacity, and data regarding 'currently connected' assets and 'accepted to

[15] 'A Strategy for a Modern Digitalised Energy System' report (June 2019)
[16] See Report, page 5 and 9-10
[17] See Report, Recommendation 5, page 46

connect' data regarding ESOs.[18] We note that what is commercially sensitive data may differ in the view of different project participants.

7.19 This information may be confidential in different scenarios, e.g. it may be commercially sensitive between parties at the same level of the market, but not commercially sensitive between parties at different levels of the market who do not compete.

7.20 On balance, we consider that it would be reasonable to assume that the sharing of this type of information for the genuine purpose outlined above is unlikely to be considered as anti-competitive *by object*. The Project could, however, have a potential anti-competitive *effect* on the market due to the risk of sharing commercially sensitive information. This will depend on whether there are restrictions as to the use and/or access to the data (see below).

The transfer of data between competing undertakings

7.21 In terms of sharing any data, whether or not this could infringe Chapter 1/Article 101 would depend on the nature of the data and who it is shared between (i.e. if shared between companies at the same level of the market): if it is current/recent or future information relating to prices, customer lists, production costs, volumes, turnovers, sales, capacities, marketing plans, risks, investments and technologies, this could raise significant competition concerns. The age of the data and the level of aggregation would also be a relevant consideration; the exchange of "highly aggregated historical data" is unlikely to raise concerns as it would not likely be commercially useful (although this begs the question as to why it would be shared in the first place). The extent to which the data is anonymised would also impact the competition law assessment.

7.22 It may be possible to argue that it is necessary to share certain data to achieve certain legitimate aims. For example, to enable the benefits of the Project data such as understanding infrastructure requirements, operational constraints and investment needs, information on individual generator assets is likely to be necessary to be shared with distribution network operators, but this doesn't meant that granular information should be shared between competing generator companies. To prevent an anti-competitive effect from the Project, it is therefore important that the data sharing does not go further than is necessary to achieve the legitimate aims.

7.23 The fact that data sharing can be pro-competitive has been acknowledged in a number of circumstances in other contexts[19], including where it assists with levelling the competitive playing field between established incumbent competitors and smaller entrants, providing there is "access in a non-discriminatory manner"[20] (see below). In the context of the CMA's energy market investigation, the CMA required the largest energy suppliers to disclose their customer lists and other customer information to other operators to allow these competitors to target new customers. It is clear that benefits will arise from the Project, but nonetheless an effect on competition could result if the data is shared inappropriately.

7.24 It is also well-established in the insurance sector that the sharing of certain risk (and pricing) data is necessary to enable smaller companies to be able to properly price their products. An example of the competition authorities' approach to information exchange is set out in the *WhatIf?* Commitments.[21] This case involved the exchange of pricing information via a third party data provider and was concluded by the parties providing the Office of Fair Trading[22] with binding commitments, including allowing access to certain amounts of appropriate data.

[18] See Open Data Networks website which lists data fields publicly shared: we note that aspects such as customer name, contractual information and capacity are not noted as publicly available. This does differ between parties. http://www.energynetworks.org/electricity/futures/open-networks-project/der-information/overview.html

[19] The Commission's paper on *Competition policy for the digital era* states that pooling arrangements "will frequently be efficient and socially desirable" (though, can be anti-competitive in other circumstances), European Commission, *Competition Policy for the Digital Era* [2019]
[*https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf*].

[20] Case C-238/05, *Asnef-Equifax v AUSB* [2006].

[21] *Decision to accept binding commitments to modify a data exchange tool used by Motor Insurers,* December 2011 (OFT1395).

[22] Now the Competition and Markets Authority ("**CMA**").

7.25 To the extent that data is shared beyond the legitimate aims of the Project as discussed above, it may be necessary to demonstrate that the arrangement meets the exemption criteria under the competition law rules, i.e.:

7.25.1 it achieves certain efficiencies and/or benefits;

7.25.2 these are passed on to consumers;

7.25.3 any restrictions are the minimum necessary to achieve these benefits/efficiencies; and

7.25.4 competition is not eliminated in a substantial part of the market.[23]

7.26 Given the risks around data sharing between competitors, RecorDER will need to ensure that its agreements with each of the data suppliers (i.e., the DNOs) and with those undertakings which access the data specify clearly the scope of the data included and its intended purpose: we understand the final arrangements as regards which legal parties will be subject to these agreements is currently being finalised. The risk will be higher when data is shared between companies at the same level of the market; the risk will be lower when data is shared between parties at different levels of the market.

7.27 We understand that the Project envisages managing the risk by limiting the viewing rights of the data as follows:

7.27.1 Data will be classified according to its type, e.g. open, public, shared and closed.

7.27.2 National Grid and the DNOs (Distribution Network Operators) will have access to the appropriate level of data in its role as the owner and operator of the transmission network in the UK;

7.27.3 ESOs (Electricity Service Operators) will be able to see their own data only;

7.27.4 Third parties will be granted access to the data set in line with their requirements (and subject to compliance with e.g. REMIT).

7.28 We understand that one outcome of the Project will be to facilitate the management and tracking of portfolios of assets within different services, for example by creating data fields for 'Balancing Market Unit IDs', 'Capability Market Unit IDs'. This would involve using the Project to signal which assets are in a Balancing Market Unit or Capacity Market Unit at any given time, and we understand allow an aggregator to adjust which assets are used in a balancing market unit at an appropriate time (e.g. if unavailable due to maintenance). This type of use of the data would be an example of a clear benefit of the project (allowing further efficiency in the market) and also an example of how sensitive data is being shared in a manner that is unlikely to raise concerns (i.e. the data is shared with a party at a different level of the market rather than directly between competitors). To the extent an aggregated version of this information is displayed to market participants, this could however raise information exchange concerns and should be considered carefully. The feedback to market participants of any aggregation of data by third parties of this type should be carefully considered for competition law risk however (as it could reveal the commercially sensitive information of other parties).

7.29 We would consider that the management of the data in this way should manage the risk of any data shared by the platform having an anti-competitive *effect*. We set out further recommendations below. In addition, we would recommend that a data sharing protocol is put in place (as we understand is the envisaged approach) and that this protocol is reviewed by a competition lawyer before being put in place, with careful consideration of the type of information shared between different market participants, and the degree to which it is shared as considered above.

REMIT and competition law

[23] Article 101(3) TFEU and Section 9 Competition Act 1998.

7.30 There is analytical overlap between the requirements of transparency under the REMIT (the EU Regulation on Market Integrity and Transparency) and competition law.

7.31 REMIT makes a number of requirements for certain information to require public disclosure, including capacity and use of facility information, as well as general information that a reasonable market participant is likely to use.[24] We understand that some of the types of information to be displayed as part of the Project fall within the categories of transparency information required under REMIT.

7.32 In general, competition law applies to the autonomous conduct of an undertaking, so does not apply to acts required under other legislation, such as the requirements of REMIT. Competition law would only apply to the extent that information disclosure goes beyond the requirements of the legislation. In any event, given the nature and context of disclosures under REMIT, it would be unlikely that disclosures made under that legislation would be considered to be *object* restrictions under competition law given that REMIT's aim to facilitate energy trading and a level competitive playing field: such disclosures are not designed to restrict or distort competition.

7.33 As a result, to the extent that the Project includes information disclosed under the participants' REMIT obligations (e.g. information on capacity and use of facility information), display of such information through the platform is unlikely to raise any competition law concerns, and in any event should be considered under the recommendations discussed below.

7.34 Conversely, some third party access to certain information may need to be restricted in order to comply with REMIT obligations (see below and section 3 above).

ACCESS TO THE DATA

7.35 There is a risk that any agreement between the Project and certain undertakings, or between undertakings themselves, to exclude access to the data to certain undertakings, could infringe Chapter 1.

7.36 Such an exclusionary agreement could be characterised as a form of collective boycott, which is aimed specifically at preventing competition from new entrants. The European Commission has previously considered that collective exclusive dealing (i.e. with the effect of boycotting a competitor in the market) is an "object infringement" of the Chapter 1 Prohibition.[25] It is therefore possible that the exclusion of certain undertakings could be categorised as a *by object* infringement, which means that it would not be necessary for complainants to demonstrate that the inability to access the data had an impact on their ability to compete on the market.

7.37 The European Court of Justice has found that data pooling can be justified on the basis that it can help level the competitive playing field between established incumbent competitors and smaller entrants, *providing there is "access in a non-discriminatory manner"*[26]. Restricting access to the data could also undermine the legitimate aims of the project as discussed above: to encourage research and new product development.

7.38 As of November 2019, in the insurance sector, the European Commission is currently investigating a data pooling arrangement in Ireland. Its press release explicitly states that data pooling likely contributes to effective competition and benefits consumers and its concerns relate to whether the exclusion of certain companies from access to the data had an anticompetitive effect.[27] This case suggests that limiting access may not in certain circumstances amount to a by object automatic infringement of the competition rules; in these circumstances, any complainant would need to demonstrate that its exclusion had an anti-competitive effect, for example, because the data was not available from other sources and therefore it was effectively foreclosed from being able to compete on the market. It is worth noting that the former Block Exemption Regulation for the Insurance Sector

[24] Article 2 and 4 REMIT
[25] Case C-68/12 *Protimonopolný úrad Slovenskej republiky v Slovenská sporitel* [2013].
[26] Case C-238/05, *Asnef-Equifax v AUSB* [2006].
[27] Case AT.40511 *Insurance Ireland* [2019] [*https://europa.eu/rapid/press-release_IP-19-2509_en.htm*].

(2008) exempted certain data pooling only if it was made "available" for other insurance companies on "reasonable, affordable and non-discriminatory" terms.

7.39 It is also possible that a disgruntled complainant could argue that a refusal to allow access to the data amounted to an abuse of a dominant position by the Project and/or data providers contrary to the Chapter 2 prohibition. This would be a trickier argument to make and, to a certain extent, unnecessary as a Chapter 1 argument would be a more obvious and easier challenge. We have not therefore considered in detail the merits of a Chapter 2 argument but some observations are:

7.39.1 A complainant would need to prove that the Project is in a dominant position in a market, for example 'the provision of a data pooling service for energy asset providers and those providing services to energy asset providers'. This would involve a market definition exercise, which would be complex and would require the input of specialist competition economists. The Project would need to have a share of this market generally in excess of 50% to indicate dominance.[28] Any assessment would also take into account the size and strength of competitors in the market, the level of price competition and barriers to new entrants.[29]

7.39.2 It would also be necessary to demonstrate that the refusal to allow access to the data was abusive. There are cases where refusal to allow access to certain information has been regarded as abusive where it prevented a potential competitor from developing a new product (for example, Magill[30] and *Oscar Bronner*[31]). However, these cases involve a specific set of circumstances. The *Instrument Codes*[32] case may be helpful to a complainant; in this case, in order to avoid an abuse of dominance infringement decision, Thomson Reuters offered commitments to the European Commission to allow financial institutions to use its data collection software (for a monthly fee) in order to access real-time data feeds from sources other than its own.

7.40 The risk of a competition law challenge (based on Chapter 1 and/or Chapter 2) would be higher if there is evidence that certain named undertakings were to be excluded. It would be difficult in these circumstances to argue that access was limited based on objective criteria.

7.41 To avoid any risk of a competition law challenge, the Project should offer access to all competitors on the market, and third parties where relevant (subject to compliance with REMIT), on fair and reasonable terms in line with the agreed protections in the protocol to be put in place. If this is not acceptable from a commercial perspective and we are satisfied that access to the data is not necessary for companies at different levels of the market to develop their own competing products (and there are other sources of the data), access may be limited on the basis of objective and transparent criteria, such as complying with other regulatory obligations (e.g. REMIT, which prohibits access to be given to certain information - see Section [3 of the main report][33]). This may involve restricting access to certain data to certain participants for certain uses, for example. However, it may be difficult to justify (and to police) a restriction which requires data only to be used, e.g. for research purposes (and not to develop new products). If any complaints are made, the criteria could be revisited (to avoid a complaint to the CMA and full investigation).

7.42 **Summary of Recommendations**

7.42.1 Given that the sharing of commercially sensitive information can raise competition law risks, RecorDER and/or the data providers (i.e., the DNOs) should carefully consider, and continue to monitor, what data is commercially sensitive and to which type of market

[28] Case C-62/86 [1991] ECR I-3359, [1993] 5 CMLR 215, para. 60.
[29] *United Brands v Commission* Case 27/76 [1978] ECR 207, [1978] 1 CMLR 429.
[30] Cases C- 241/91 & C- 242/91 P *RTE & ITP v Commission & Magill TV Guide* [1991].
[31] Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitung* [1998].
[32] Case 39654 *Reuters Instrument Codes* [2013].
[33] Note, however, that where such third party access is restricted due to REMIT compliance, the participating DNOs and Electron/RecorDER would also need to ensure that the DNOs' own access to that restricted information is properly ring-fenced internally and limited to the DNO level of the supply chain, in order to prevent that access to that restricted information is given to their own entities active in the downstream wholesale level of the supply chain. In other words, if a third party active at the wholesale level cannot get access to certain information within RecorDER due to REMIT, a competitor of that third party at the wholesale level, which happens to be part of the same vertically integrated corporate group as a participating DNO, cannot be given access to such information either for the same reason of REMIT compliance.

participant each type of information should be given or be restricted. Information such as provider information, contractual descriptions, connection queue management position, asset capacity and exclusivity terms is likely to be commercially sensitive (unless sufficiently historic and aggregated/anonymised), and should be within the category of information for which participants should only be able to view their own data (i.e., once such data is collected from the participants, each participant should then only be able to access their own data of that type from RecorDER in a non-aggregated format, not any such data belonging to other data providers). Any data sharing should not go beyond that required to generate the benefits of the Project, and any feedback to market participants of any aggregation of data by third parties (e.g. aggregators) should be carefully considered for competition law risk.

7.42.2 A data protocol should be put in place and reviewed by legal counsel. This should set out clearly how the data is to be stored and displayed; the types of data which will be shared with which parties; protections built in to the RecorDER Project to prevent any inappropriate disclosure; and the role of any third party audit function.

7.42.3 RecorDER should ensure that its agreements with each of the data suppliers (i.e., the DNOs), and with those undertakings which access the data (i.e., the DNOs and National Grid during Phase 1 of the project), specify clearly the scope of the data included and its intended purpose.

7.42.4 The terms upon which parties are given access to the RecorDER Project must be considered, and should be fair and reasonable terms in order to prevent any form of 'collective boycott' or discrimination between participants. Where relevant, third parties may need to be offered access but such may be limited on the basis of objective justifications, such as complying with other regulatory obligations (e.g. under REMIT, which prohibits access to be given to certain information).

APPENDIX 1

LEGAL AND REGULATORY SCOPE

System Wide Resource Register (SWRR)

Proposed questions for Legal Advisors

General Views on Sharing Distribution Resource Data

It was previously agreed by network company experts that the Utilities Act Section 105 would prevent DNOs from sharing all of the proposed data in Appendix A relating to DER customers. Whilst there are exceptions to the information disclosure restrictions laid out in Section 105, these are not considered to be sufficient to enable implementation of the SWRR.

If new licence obligations relating to providing a SWRR were to be placed on the network companies, or if network code obligations were to be placed on network companies to share information with another party so that an SWRR could be published, these are likely to qualify as exceptions to the information restrictions under Section 105 (3)(c) and could enable the SWRR to be taken forward.

It is also unclear whether the information to be published in the SWRR would be commercially sensitive and whether there are issues from the perspectives of Competition Law or REMIT. (REMIT is an EU regulation on energy market integrity and transparency. In part, REMIT covers the disclosure of commercially sensitive information relating to energy markets.)

A further concern relates to any specific confidentiality clauses that may be included in connection agreements (or commercial service agreements). Whilst changes could be made to new contracts, a large number of existing contracts may need to be altered and this would be a VERY extensive piece of work for network companies and customers. If contracts did need to be changed, each variation would have to be agreed individually. At this stage, it is not clear how many contracts (if any) include confidentiality clauses. Several forms of connection contract have been used over the years. On the basis that the approach to confidentiality clauses in Connection Agreements is likely to be different from DNO to DNO and also may vary within any DNO depending on the version of the Connection Agreement entered into, general advice on the impact of confidentiality clauses is sought.

Another issue is that some customers will not want data to be disclosed in a SWRR as they would prefer not to disclose the identity and location of facilities such as data centres or critical infrastructure sites.

It is generally agreed that GDPR restrictions would apply to disclosing Customer Names if these customers are individuals rather than companies. In these cases, the customer names should not be included on the SWRR.

Proposed Questions for Legal Review

- What are the legislative impediments to sharing the data as envisaged in Appendix A? Subsidiary questions are:

  (i) to what extent does the legislation limit what use shared information can be put to?
  (ii) to what extent does the legislation limit with whom the information can be shared with?
  (iii) to what extent are the responses to these questions impacted by any provision in a Connection Agreement that purports to allow for the sharing of such information or indeed contains confidentiality provisions?

  A non-exhaustive list of legislation that may be relevant and are: S.105 Utilities Act, Electricity Act 1989, Competition Law including the REMIT Regulations, and GDPR.

  In addition to these are there other relevant areas of legislation? Is there likely to be a general obligation of confidence that has been established through common law.

- Where there are such legislative impediments, what are the available options for making the sharing of such information lawful? For example:

  - Would consent from the relevant customer be sufficient? Where consent is deemed to be a solution, how will this work in practice over time where the DNO will not know if a customer has sold its interest in a site to a third party who has not consented to data sharing?
  - Could a change to the Licence Conditions address the issues? Would the inclusion in network company licences of a specific obligation to publish information for the public interest be more clear than the establishment of a new requirement in a network code?
  - Where historic connection agreements contain confidentiality provisions, would the inclusion of a Licence Condition or network code obligation to share data override these?
- There is an ongoing modification to the Distribution Connection and Use of System Agreement (DCUSA) that would require DNOs to publish embedded capacity registers for resources connected to their networks. This is covered in DCUSA change proposal DCP 350. Under Electricity Distribution Licenses, DNOs must be a party to, and comply with the DCUSA. If the DCUSA modification DCP 350 is agreed and becomes part of the DCUSA, will this provide a basis for DNO's to provide customer information including names and site details?
- We want to be able to publish the data fields as outlined in the Appendix. Where historic connection agreements do not refer specifically to use of data and / or confidentiality of connection information, or in the absence of an agreement, is there any other applicable UK legislation that may prevent publication? If so, which legislation? Subsidiary questions are:
  - If the contracts we have on file are silent on confidentiality, does this mean that no confidentiality law applies to the use of that data?
  - How should we treat sites of national security, first responders (i.e. MOD, hospitals) where agreements do not specifically refer to confidentiality or where the agreement is absent? Notwithstanding any legislation of universal applicability, are there any specific legislative issues connected with sharing information that may directly or indirectly relate critical national infrastructure such as sewerage/water treatment sites/major transport infrastructure (such as rail, tube and airports) and prisons as well as MOD and hospital sites?
  - In the event that specific clauses weren't included in the connection agreement and there is legislation in place to protect use of data in connection agreements, what are the legal risks should we choose to publish? Does the legislation that has been identified apply to all data fields or select fields? what recommendation would you make to mitigate the impact?
- Where legislative restrictions on the sharing and use of such data are addressed, what are the sanctions for non-compliance?
- Do the proposed data fields fall within scope of the General Data Protection Regulations? If so, which ones?
  - Are the types of connection data proposed classed as personal data?
  - If the GSP/BSP is considered to be 'personal' data, is the aggregation of customers at a voltage level higher than where they are connected sufficient to protect anonymity?
  - Is capacity and load information considered personal data?
  - In the future this data may also include more installations such as domestic roof-top PV, domestic batteries and Electric Vehicles where it is more likely that personal data will be shared. From a GDPR perspective it would desirable to get advice on who would be the data controller and who would be the processor and for what lawful purposes? What changes would be required to the respective DNOs' privacy policies?
- What would happen if a customer objected to the sharing of the data – would the DNO be compelled to remove the data in question?
- Which legislation takes precedent if/when there are conflicts? The Utilities Act 2000, or the Electricity Act 1989 (where licence conditions are specified).

Distribution codes direct how the licence conditions in the Electricity Act should be implemented / realised. Are the codes that sit underneath the licence conditions considered legally binding?

APPENDIX 2

DATA CATEGORIES AND DATA FIELDS

If stated "yes" in the table below, then the current understanding is that the data in the relevant data field is already published or otherwise made available.

Type	Sub-type	Field Name	ENW	NPG	SPEN	SSEN	UKPN	WPD	ESO
General		Customer Name	No	No	No	No	No	No	Yes
		Customer Site	No	No	Yes	No	No	No	Yes
		Grid Supply Point (GSP)	Yes	Yes	Yes	Yes	Yes	Yes	No
		Bulk Supply Point	Yes	Yes	Yes	Yes	Yes	Yes	No
		Primary	Yes	Yes	Yes	Yes	Yes	Yes	No
		Licence Area	Yes	Yes	Yes	Yes	Yes	Yes	No
		Plant Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		Managed Connection Arrangement (Y/N)	Yes	Yes	Yes	Yes	Yes	Yes	-
		Connection Status	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connection	Connected	MW / MVA Connected	Yes	Yes	Yes	Yes	No	No	Yes
	Connected	Export Capacity	Yes	Yes	Yes	Yes	No	No	No
	Connected	Date Connected	Yes	No	Yes	Yes	No	No	No
	Accepted	MW /MVA Accepted to Connect	Yes	Yes	Yes	Yes	No	No	Yes
	Accepted	MW / MVA Export Capacity	Yes	Yes	Yes	Yes	No	No	No
	Accepted	Date Accepted	Yes	No	No	No	No	No	No
	Accepted	Target Energisation Date	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Accepted	Connection Queue Management Position	Yes	Yes	Yes	Yes	Yes	Yes	-
	Accepted	Distribution Reinforcement Reference	Yes	Yes	Yes	Yes	Yes	Yes	-
	Accepted	Transmission Reinforcement Reference	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reinforcement		Works Reference	No	Yes	Yes	No	Yes	Yes	Yes
		Works Description	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		Works Completion Date	Yes	Yes	Yes	Yes	Yes	No	Yes
		Reinforcement Driver	Yes	Yes	No	Yes	Yes	Yes	No
		Reinforcement Type	Yes	Yes	Yes	Yes	Yes	Yes	Yes
		Licence Area	Yes	Yes	Yes	Yes	Yes	Yes	No
Services		Distribution Service Provider (Y/N)	Yes	Yes	Yes	Yes	Yes	Yes	-

Type of Service	Yes	Yes	Yes	Yes	Yes	Yes	-
Contract Duration	Yes	Yes	Yes	Yes	Yes	Yes	-
Exclusivity	Yes	Yes	Yes	Yes	Yes	Yes	-
Transmission Service Provider (Y/N)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Type of Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Contract Duration	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Exclusivity	Yes	Yes	Yes	Yes	Yes	Yes	Yes

APPENDIX 3

ELECTRICITY CODES

Code	Parties	Description	Restrictions on sharing or publication of information	Application to SWRR Data
Standard Licence Conditions (distribution licence)	Licenced electricity distributors (DNOs)	The standard licence conditions are those which all licenced distributors must comply with. They place general obligations on licenced distributors in relation to the operation of their distribution networks.	Standard Condition 31B prevents licensees from sharing confidential information (meaning any information derived from the distribution business that is not legitimately in the public domain) with any affiliate or related undertaking who holds an electricity licence. This would prevent a distributor sharing certain information about the generation assets that are connected to its network with a group company that held, for example, a transmission or supply licence. Standard Conditions 20-22 place an obligation on licensees to comply with certain industry codes as set out below. These industry codes also contain specific confidentiality provisions.	The restriction in 31B is limited in scope to the sharing of information between related licensees. It is therefore only likely to apply to a small number of distributors. In addition, it only applies to information which is not already in the public domain. We note that DNOs already publish certain information in relation to certain distribution assets[34].
Distribution Code	Licenced electricity distributors (DNOs)	The Distribution Code sets out technical requirements relating to the connection and use of the electricity distribution licensees' distribution networks.	DIN6 states that a DNO may not, except in pursuance of specific requirements of the Distribution Code, disclose the information it receives from users relating to their intentions without the prior written consent of the information provider. The "specific requirements" of the Distribution Code are considered to be those which expressly	The confidentiality restrictions in DIN6 are likely to apply to all of the SWRR Data fields as the Distribution Code provides for supply of a wide range of information from users to DNOs. We do not believe that either of the specific requirements placed

[34] http://www.energynetworks.org/electricity/futures/open-networks-project/der-information/overview.html

			permit DNOs to share information received from users. These include: • DPC8.2.3 requires DNOs to submit certain planning data or information relating to existing offshore generators to NGESO in accordance with CUSC; and • DPC8.3 permits DNOs to share information received from users that, in its reasonable opinion, may have an impact on the system of any other User.	on DNOs to share information received would apply in respect of all of the SWRR Data, and therefore the Distribution Code acts as an impediment to the sharing of SWRR Data.
Distribution Connection Use of System Agreement ("**DCUSA**")	Licenced electricity distributors, suppliers and generators	The DCUSA is a multi-party contract concerned with the use of the electricity distribution system. It relates to the connection to and use of the electricity distribution networks and contains the charging methodologies used to calculate the charges levied on distributors for connection to, and use of, the electricity distribution networks.	Under Clause 34 of DCUSA, a DNO may not use confidential information (defined as information held in respect of a connectee which it has acquired in its capacity as operator of a distribution business) for any purpose other than as permitted under the DCUSA and any confidential information obtained may not be used by the DNO (or any affiliate or related undertaking) for any commercial advantage for the DNO (or any affiliate or related undertaking) in the operation of a supply business. Confidential information is only permitted to be disclosed (amongst other reasons), where prior written consent is given, for the purpose of effective performance of the DNO's obligation under the DCUSA, for the effective operation of the distribution business, or in compliance with any other requirement of law or a "Relevant Instrument" (the EA, data protection legislation, licence conditions, and certain Electricity Codes). Note that "requirement of law" is not defined and we would therefore consider that Electricity Codes which do not fall within the definition of Relevant Instrument" (e.g. the Distribution Code) would fall under the requirement of law limb as	The definition of confidential information under DCUSA is wide in scope and likely to encompass all of the SWRR Data fields. There are currently no obligations on DNOs under the DCUSA to maintain a shared asset register, and the sharing of such information would therefore not be considered a permitted disclosure. Note that if disclosure was otherwise permitted by a requirement of law or a "Relevant Instrument" then we would consider that such disclosure would be lawful for the purposes of DCUSA but would not by extension automatically permit disclosure under other Electricity Codes. A requirement under licence conditions or under an Electricity Code (provided that such code was listed as a "Relevant Instrument"

			DNOs are legally required under the terms of their licences to comply with them.	under DCUSA, currently the MRA, CUSC and BSC) would enable the sharing of the SWRR Data.
Master Registration Agreement ("**MRA**")	Licensed electricity distributors and suppliers	The MRA is a multi-party agreement which sets out terms for the provision of Metering Point Administration Services (MPAS Registrations), and procedures enabling electricity suppliers to transfer customers.	Clause 38 of the MRA sets out confidentiality obligations on the parties and closely mirrors Clause 34 of DCUSA.	As above.
Balancing and Settlement Code ("**BSC**")	NGESO and all entities licenced under the EA.	The BSC contains the governance arrangements for electricity balancing and settlement and outlines the mechanism by which parties can buy and sell electricity in close to real time to keep the system balanced.	Paragraph H4 of the BSC sets out requirements in respect of confidential information (defined as all data, documents and other information supplied by a party to another under or pursuant to the BSC). Confidential Information may only be disclosed where required pursuant to certain "nominated agreements" which include the Electricity Codes, connection agreements, and contracts for difference, where prior written consent is given, in compliance with "relevant instruments" (the EA, Data Protection Act 1998, the licence and the capacity market rules), legal requirements (meaning an act of parliament, regulation, licence or directive from the secretary of state or Ofgem) or where such information enters the public domain.	Certain of the SWRR Data fields are likely to fall under the confidentiality provisions in the BSC. In particular, point of supply and capacity information is likely to be supplied by DNOs under the BSC. Disclosure of such information would not fall under the scope of "required pursuant to a nominated agreement" as there are currently no requirements in the Electricity Codes, other relevant documents or legal requirements which oblige a DNO to share information for the purposes of creating a shared asset register. However, as noted above, if any of these did require such sharing of information, this would permit disclosure under the BSC only and would not release the DNO from confidentiality restrictions under other Electricity Codes. A requirement under licence conditions would enable the

				sharing of the SWRR Data. Note that the definition of "Relevant Instruments" used in the BSC does not specifically include any Electricity Codes, but a requirement under another Electricity Code may enable sharing of the SWRR Data if such code fell within the catch-all wording as follows: "all […] guidelines and other matters which are required or which a Party acting in accordance with Good Industry Practice would obtain or comply with for the purposes of the Code, of or from any Competent Authority." We suggest that the Electricity Codes set out in this table would satisfy this definition as licensed distributors must comply with them as a requirement of their licence. As stated above, some of the SWRR Data fields would fall under the "information in the public domain" exception[35].
Retail Energy Code ("**REC**")	Licensed electricity and gas suppliers, distributors and gas transporters	The REC is a dual fuel code which sets out the transitional requirements on suppliers, DNOs and gas transporters, to play their part in the design, build and testing of the new systems and processes for faster, more reliable switching.	Clause 18 of REC imposes obligations on parties in respect of their confidential information. Confidential information is defined to include all data or information supplied or made available pursuant to the REC. There are exceptions for disclosure where a party is required or permitted to disclose under its energy licence, the REC or	It is unclear to what extent the SWRR Data would fall under the scope of confidential information under the REC as this is likely to only include information related to switching. However, it is likely that at least some of

[35] http://www.energynetworks.org/electricity/futures/open-networks-project/der-information/overview.html

			another Electricity Code, and where consent is given.	the SWRR Data fields would be classed as confidential information. The exemptions set out in the REC would not apply to the sharing of information for the purposes of creating a shared asset register. A requirement under licence conditions or under an Electricity Code would enable the sharing of the SWRR Data.
Connection and Use of System Code ("**CUSC**")	Licensed suppliers, generators and distributors	The CUSC sets out the principal rights and obligations in relation to connection to and/or use of the national electricity transmission system ("**NETS**") and additionally the provision of Balancing Services. The CUSC also sets out the methodologies used by National Grid to calculate the charges levied for connection to and use of the NETS.	Under section 6.15 of CUSC, NGESO must ensure the confidentiality of protected information. Protected information is defined to mean any information relating to the affairs of a party which is furnished to any employee of NGESO in accordance with CUSC, a bilateral connection agreement, a construction agreement or mandatory services agreement. In particular NGESO must ensure protected information is not used for the purposes of obtaining any right to purchase the benefit of a contract to distribute electricity or any contract for the use of electrical lines or plant etc. The other parties to the CUSC must ensure the confidentiality of all data and other information supplied to it by other parties to CUSC or any bilateral connection agreement, a construction agreement or mandatory services agreement. Disclosure may be made with consent. Disclosure is also permitted where required in compliance with the EA, any requirement of Ofgem or the Secretary of State, in compliance with licence conditions or any document referred to in the licence with which	The relevant information under the CUSC includes any information supplied by generators in accordance with their connection agreements. In the majority of cases this will cover all of the SWRR Data. Consent from the relevant party would be required in order to disclose the data. As noted above, if any of the other Electricity Codes, a licence condition or legislation did require sharing of information, this would permit disclosure under the CUSC only and would not necessarily release the DNO from confidentiality restrictions under other Electricity Codes.

			a user must comply (e.g. the Electricity Codes) or in compliance with any other requirement of law.	
Grid Code	Distributors, generators, and interconnectors	The Grid Code specifies technical requirements relating to the planning, operation, connection to and use of the NETS.	Section C12 of the Grid Code states that the CUSC confidentiality provisions apply to the Grid Code.	See analysis above.