DRAFT

End-to-End Switching Arrangements

Data Protection Impact Assessment

Version: **V1.4**

Date: **20/09/17**

Table of Contents

1 Executive Summary

The EU General Data Protection Regulation (GDPR)[1] requires that the rights and freedoms of data subjects are protected.

Where data processing is likely to result in a high risk to the rights and freedoms of data subjects, then the GDPR requires a Data Protection Impact Assessment (DPIA) to be conducted[2]. This document is the draft DPIA for the Switching Programme, which will be revised as the programme proceeds.

Data privacy risks identified in this document will be managed in accordance with the wider programme information security risk management framework.

The key conclusions of this document are set out below.

1.1 Personal Data

A small number of data types that can potentially be associated with consumers have been identified as part of the data that will be processed within End-to-End Switching Arrangements (E2ESA). None of this data comes under the special categories of personal data as defined in the GDPR.

Ultimately, the question of precisely what data counts as personal data can only be determined by case law in the courts. However, it would be prudent to treat as personal data the combination of a premises address with either an MPxN[3] or objection indicator. This approach is consistent with the Information Commissioner's Office (ICO) Ruling on the Electricity Central Online Enquiry Service ECOES[4]

From both a commercial and legal perspective, the lowest risk approach (to prevent future challenge) is to treat such data as if it were personal and apply a low intervention approach to its management. Treating the data as if it were personal data allows proportionate measures to be built into the system design from the beginning, and reduces the risk of additional security requirements being introduced late in the design and development process when they would be much more costly to implement.

1.2 Data Controller Role

It is prudent for the CSS Provider to fulfil the role of Data Controller. Although it would be possible to make a case that the CSS Provider is merely a Data Processor as defined by the GDPR, this option creates the risk that a subsequent legal challenge will find that the CSS Provider should have fulfilled the Data Controller role. As the Data Controller, the CSS Provider will be responsible for ensuring that consumer personal data within the Central Switching Service (CSS) is protected adequately.

1.3 Lawful Basis

Where feasible and proportionate, obtaining consent from the Data Subject (in accordance with article 6(1) (a) of the GDPR) automatically gives the Data

[1] Regulation 2016/679. See https://gdpr-info.eu/
[2] GDPR Article 35.
[3] A Meter Point Administration Numbers (MPAN) or Meter Point Reference Numbers (MPRN)
[4] see reference 2 in section 6

Controller the lawful basis to process the data. However, where this is not feasible and proportionate, other grounds for lawful processing may be asserted.

Article 6(1) (c) of the GDPR – legal obligation – provides an appropriate and sufficient ground for lawful processing by the CSS Provider, where obtaining consent is not feasible and proportionate. The licence conditions set by the Gas and Electricity Markets Authority (GEMA) are understood to constitute “Member State Law” for the purposes of the GDPR, thus creating a legal obligation. The Data Controller would, however, need to be a licensee in its own right for this provision to be relied upon. This could be achieved, for example, by Ofgem imposing obligations through a new Retail Energy Code, which the CSS Provider would be required to be party to.

1.4 Privacy Risks

A separate document - the Programme’s Information Risk Assessment (IRA) – identifies, scores and proposes mitigations for all security risks relating to the programme. These include risks to personal data and privacy as well as other security risks.

2 Introduction

2.1 The General Data Protection Regulation (GDPR)

The GDPR entered into force on 24th May 2016 and, following a two-year implementation period, will come fully into effect (and be fully enforceable) from 25th May 2018. Because of this timeline, the Switching Programme has been assessed against the GDPR requirements, instead of requirements found under the UK Data Protection Act 1998 (the DPA).

The GDPR contains a number of changes to the existing data protection regime under the UK in the current DPA. Key changes impacting on the Switching Programme include:

- Compliance: Strict new compliance requirements will be imposed. For example, entities will have to create written compliance plans, which they will have to deliver to regulators on demand. Entities will need to be able to prove that they are complying with the GDPR by being able to produce evidence to that effect.

- Usage controls: Personal data will be subject to strict new usage controls. These include ‘data minimisation’, ‘data portability’ and ‘right to be forgotten’ principles, which will require entities to limit the use of data, and will give individuals, under some circumstances, rights to take their data with them at the end of a relationship and to delete and destroy data on request.

- Consent: Where processing is based on consent, such consent must be ‘freely given, informed, specific and unambiguous’. This is a toughening up of the language used compared to the DPA, which reserved this level of certainty solely to sensitive personal data. In relation to the processing of sensitive personal data, there is an additional threshold that consent must be explicit.

- Bundling: The provision of a service that is conditional upon the individual giving permission for their data to be used for non-essential purposes (such as marketing) will be curtailed.

- Supplier/Partner relationships: An entity handling another organisation’s information will be directly liable under the GDPR for failure to meet certain obligations. The current DPA only indirectly applies to organisations receiving instructions to process personal data, for example, through a contract. Under the GDPR, the obligations are more extensive and include direct liability.

- Breach disclosure: Entities will be required to report serious contraventions of the law to the regulators and to people affected. Such disclosure to the regulator will need to be made within 72 hours of the entity being aware of the breach. Public disclosure of failure is likely to fuel regulatory sanctions and compensation claims, as well as causing damage to brand and reputations.

- Fines: Serious contraventions of the law will be punishable by fines of up to either 4% or €20 million of group annual worldwide turnover.

- Litigation: Citizens and pressure groups have the right to engage in group litigation (‘class actions’) to recover compensation for mere distress caused by contraventions of the law.

2.2 Background and Context

In February 2015 the Office of Gas and Electricity Markets (Ofgem) published a decision to lead a programme of work to implement reliable and fast switching for consumers between gas and electricity suppliers using a Centralised Registration System (CRS). At the same time, Ofgem published a target operating model to act as a reference and a guide for the design and implementation of the programme. This service is being designed by the Switching Programme and will provide simple, streamlined and efficient switching. The Switching Programme will also harmonise switching arrangements for gas and electricity and design a set of clear, unambiguous processes that, wherever possible, work for both the gas and electricity markets.

The End to End Switching Arrangements (E2ESA) are the set of arrangements that govern the storage, processing and exchanges of information associated with switching a customer between energy suppliers. The participants in the E2ESA include the industry actors who are the organisations participating in switching. The set of actors includes organisations such as Smart DCC (DCC), in its delivery and management roles, and any commercial entities supporting those functions.

The CSS will support E2ESA and the Switching Programme objective[5] as stated in the Ofgem Switching Programme Strategic Outline Case.

Data privacy risks identified in the DPIA will be managed in accordance with the wider programme information security risk management framework. The privacy requirements will be provided to the Programme Design and Architecture teams such that the privacy risks are addressed at an early stage in the design of the switching arrangements and appropriate privacy solutions developed.

Given that the design is in development, there are still a number of decisions to be made regarding the finer detail of the proposed processing, including that for personal data. This document therefore addresses risks at a generic level; future iterations of the DPIA will be refined as the solution is finalised.

The requirement for a DPIA remains for as long as data that could be classified as personal data are processed. Privacy risks may change as the design of the E2ESA matures and should be reviewed regularly.

2.3 Why is a DPIA necessary?

Whilst conducting a DPIA has been regarded as best practice by the Information Commissioner's Office for many years, the GDPR makes DPIAs and 'Privacy by Design' an explicit requirement during the design phase of a new processing purpose or system.

An initial Privacy Impact Assessment (PIA) was conducted for the Switching Programme in June 2016 to identify key data protection and data privacy concerns under the GDPR and to report on associated risks applicable to strategic themes as they were known. This PIA identified the requirement for further iterations of the PIA (now called a DPIA to align with GDPR terminology).

[5] "Our overarching programme objective is to improve consumers' experience of switching, leading to greater engagement in the retail energy market, by designing and implementing a new switching process that is reliable, fast and cost-effective. In turn this will build consumer confidence and facilitate competition, delivering better outcomes for consumers".

The important benefits to performing a DPIA include:

- To reduce the potential for future additional costs to mitigate privacy and data protection risks;
- To gain an early understanding of the key risks;
- To demonstrate compliance with relevant legislation;
- To improve the quality of personal data (minimisation, accuracy);
- To improve decision making for data protection;
- To raise the issue of privacy awareness.

In addition, the GDPR requires that an assessment is made to determine the impact on individuals if their data is processed using 'new technologies' that could result in a high risk to their rights and freedoms[6]. Although the definition of 'new technologies' is open to interpretation, the requirement to protect consumer data on IT systems within the E2ESA remains.

The E2ESA will store, process and communicate the data of consumers who conduct switches. The compromise of this information (through unauthorised use, release or adulteration) could impact those consumers.

2.4 Purpose of this Document

The purpose of this document is to identify key data privacy concerns and provide an explanation of their associated risks. It will be used by the Switching Programme to:

- Identify privacy requirements that must be addressed by the programme in accordance with the GDPR;
- Understand how those requirements impact all Stakeholders, including users of the new registration systems;
- Obtain clarity as to the business need that justifies any identified unavoidable negative impacts on privacy

[6] Article 35(1).

2.5 Summary of Stakeholder Engagement

In writing this document, the following industry stakeholders[7] were consulted:

Company	Company Representatives
EDF*	Senior Business Analyst
Elexon	Senior Market Advisor
Gemserv	Data Protection Specialist
Npower	Legal Team Data Protection and GDPR specialist
	Data Protection Team Representative
Utiligroup	Lead Information Security Analyst
Xoserve	Compliance Manager & Data Protection Officer
Xoserve	Security Manager

[7] All stakeholders named provided written confirmation of their willingness for company names to be used with respect to the limited due diligence exercise conducted. Everyone involved is clear that no specific guidance or advice was sought nor given.

3 Key Determinations

The key determinations required for the DPIA are:

A. Does the CSS store, process or transfer personal data?

B. If yes, is the CSS Provider[8] a Data Controller or a Data Processor for personal data?

C. What is the legal basis for the processing of the personal data, if it exists?

3.1 Does the CSS store, process or transfer personal data?

3.1.1 ICO Ruling on ECOES

The original PIA in June 16 concluded that for domestic consumers the information held should be regarded as personal data. This view was based largely upon the ruling from the ICO for the ECOES system and its access by Price Comparison Website (PCWs).

The consumer data which could be considered personal data and which are currently expected to be processed within the CSS are shown in Table 1. Such data asset types will be limited in number, however, there will be significant numbers (millions) of each type.

Data Asset	Description
Meter Point Administration Number (MPAN)	This is the unique number associated with an electricity meter located at the point of delivery for a property or site.
Meter Point Reference Number (MPRN)	This is the unique number associated with a gas meter located at the point of delivery for a property or site. MPAN and MPRN are collectively referred to as MPxN.
Address	This is the address of the property or site that is associated with the MPxN. This is also referred to as the *premise server address*, and may be different to the *location* of the physical meter or the address of the bill payer.
Objection Indicator	This is a binary flag used by the losing supplier to indicate if they object to a consumer request to switch suppliers. When the switch is for a domestic consumer, an objection from the losing supplier is usually due to an outstanding debt, therefore this asset could indicate a consumer debt[9].

Table 2: Personal Data Assets

The ICO has responded formally on questions regarding MPANs (with the same argument for MPRNs) and stated that they are personal data. The relevant section from that ruling states:

[8] This document uses the term "CSS Provider". The terms of the relationship between the CSS Provider and the CSS contract manager, including the degree of control over the Provider's actions exercised by the contract manager, have not yet been fully specified. Therefore, references in this document to CSS Provider could include or be replaced by references to the contract manager for that service, depending on the final contractual relationship between those parties.
[9] Debt of less than £500 is generally accepted by the gaining supplier. Above that level a Debt Assignment Protocol is implemented between the Gaining Supplier, Losing Supplier and the Consumer.

> *"An MPAN uniquely identifies an electricity supply point, which is often a particular property. Where data is linked to the MPAN of a domestic property (or a commercial property where the business owner is a sole trader), it is likely to be personal data, even if the name of the individual (or individuals) who live there is not known. This is because an organisation is still able to single out a particular property and make decisions or take actions which will have a direct effect on the resident of that property."*

The ICO ruling was given in response to a query about the specific context of PCWs accessing ECOES be given access to the ECOES database (meter point reference numbers) in order to allow them to facilitate the switching process for customers.

None of the personal data asset types identified are 'Special Category'[10] personal data as defined in the GDPR.

No other data assets currently intended to form part of the processing conducted as part of E2ESA constitute personal data.

3.1.2 Assessment and Recommendation

Ultimately, the question of precisely what data counts as personal data can only be determined by case law in the courts. However, it would be prudent to treat as personal data any combination of the data defined in Table 2 that includes an address. This approach is consistent with the ICO Ruling on ECOES and professional advice commissioned by the Programme.

From both a commercial and legal perspective, the lowest risk approach (to prevent future challenge) is to treat such data as if it is personal and apply a low intervention approach to its management. Treating the data as if it is personal data allows proportionate measures to be built into the design from the beginning, and reduces the risk of additional security requirements being introduced late in the design and development process when they would be much more costly to implement.

It should be noted that treating the data as if it is personal data does not mean that mitigating risks needs be excessive or expensive. The purpose of information security risk management is to define common sense measures appropriate to the context, not to over engineer the solution.

[10] Article 9.

3.2 Data Controller or Data Processor?

3.2.1 Definitions

The GDPR defines the following two key roles:

- The 'Data Controller' determines the purposes and means of the processing of personal data. They shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

- The 'Data Processor' processes personal data on behalf of the Data Controller under the terms of a contract that sets out the subject-matter and duration of the processing.

3.2.2 Assessment and Recommendation

The CSS Provider is likely to have discretion to determine the means of processing. It will be making decisions as to data processing (beyond the limited discretion a Data Processor might be expected to operate under), creating new data and managing it under rules it will decide (or will be decided via the relevant procurement and commercial arrangements).

The fact that the CSS Provider's role would assist other parties (e.g. suppliers) does not in itself mean that the CSS Provider is acting merely as a Data Processor for suppliers. Similarly, although the CSS Provider will be bound by legal regulations, these are unlikely to fetter their discretion to the point that they would not meet the test to be a Data Controller. No third party (e.g. supplier) instructs the CSS Provider how to perform their functions. In particular, the creation of new data items with the Central Registration System adds weight to the argument that the CSS Provider is the Data Controller.

It is therefore prudent for the CSS Provider to fulfil the role of data controller. Although it would be possible to make a case that the CSS Provider is merely a Data Processor, this option creates the risk that a subsequent legal challenge will find that the CSS Provider should have fulfilled the Data Controller role.

As the Data Controller, the CSS Provider will be responsible for ensuring that consumer personal data within the CSS is protected adequately.

3.3 Lawful Basis for Processing

Article 6(1) of the GDPR defines the grounds on which processing of personal data can lawfully be carried out. To be lawful, at least one of six conditions must apply:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;

3.3.1 Assessment and Recommendation

Where feasible and proportionate, obtaining consent from the Data Subject (in accordance with Article 6(1) (a)) automatically gives the Data Controller the lawful basis to process the data. However, where this is not feasible and proportionate, other grounds for lawful processing may be asserted.

Article 6(1) (c) of the GDPR – legal obligation – provides an appropriate and sufficient ground for lawful processing by the CSS Provider, where obtaining consent is not feasible and proportionate. The licence conditions set by GEMA are understood to constitute "Member State Law" for the purposes of the GDPR, thus creating a legal obligation. The Data Controller would, however, need to be a licensee in their own right for this provision to be relied upon. This could be achieved, for example, by Ofgem imposing obligations through a new Retail Energy Code, which the CSS Provider would be required to be party to.

Of the other possible conditions, Article 6(1) (b) is useful for "customer facing" data processing. For example, a customer might sign up to a time-of-use tariff in the knowledge that performance of this contract requires the supplier to process their consumption data half-hourly. It may also be possible for suppliers to gain consent for further onward processing by other parties upfront, as part of a switch. However, it is less likely to be useful to the CSS Provider, which is not directly customer facing. Articles 6(1) (d) – 6(1) (f) are less relevant to the E2ESA arrangements.

It should be noted that relying on Article 6(1) (c) would limit the requirements placed on the CSS Provider in their Data Controller role:

1. The "right to be forgotten" is provided for by Article 17 of the GDPR. However, Article 17(3) makes clear that this right does not apply where processing is necessary for compliance with a legal obligation.

2. Article 20 of the GDPR provides for the right to data portability. This means that the data subject has a right to receive personal data concerning them via a subject access request, as well as the right to transmit that data to another controller. However, these rights only exist when processing is based on the consent of the subject, or is necessary in performance of a contract that the subject is a party to (Article 20(1) (a)). As such, whilst it may apply between suppliers involved in the switching process, it would not apply to the CSS Provider to the extent that it is processing data pursuant to a legal obligation.

3. Data subjects have a right to object to processing of their data, subject to Article 21(1) of the GDPR. However, this only applies where processing is based on grounds (e) or (f) of Article 6(1).

4 System Overview

4.1 Switching Programme Data and Information Flows

In order to identify the risks to consumer personal data within E2ESA, an understanding of how data is stored, processed and communicated is necessary.

4.1.1 Populating the CSS and Data Migration

The E2ESA solution will be implemented in the Delivery and Enduring Operation phases of the Programme. Consumer personal data will exist within the CSS prior to the start of operation or the time of the first live switch. Whatever the intended means of delivery of personal data to populate the CSS, the privacy of the personal data will need to be considered as part of the solution.

4.1.2 Switching Process – Brief Overview

The design of the E2ESA has not yet been completed. However the processes that will support switching and that involve consumer personal data can be described in overview.

The switching of a consumer from one energy supplier (the losing supplier) to another (the gaining supplier) begins with the initiation of the switch by the consumer contacting the gaining supplier or Third Party Intermediary (TPI). This initial contact may be via one of a number of communication channels. The normal method is expected to be a consumer who uses an energy supplier website, often following an automated referral from a Price Comparison Website (PCW). The other method is where the TPI is a broker that connects businesses to a supplier.

Switch requests are expected to be submitted by prospective gaining suppliers to the CSS on a case by case basis (as opposed to bulk submissions). The CSS automatically processes each switch request, transmitting a notification of the switch (including associated MPAN, MPRN and address) to the losing supplier.

The losing supplier will inform the CSS (using the Objection Indicator) as to whether there is any legitimate objection to the switch.

- No Objection – If there is no objection, then the switch will go ahead and the CSS will be updated to reflect the change in supplier. A switch will be complete when the final and opening bill are produced by the losing and gaining supplier respectively. However, within the cooling off period (14 days) a consumer can opt to cancel their contract, and agree another contract with another supplier.

- Objection – If there is an objection, then the CSS will automatically inform the prospective gaining supplier and the switch request will be terminated. Outside of the E2ESA, the gaining supplier will communicate directly with the consumer regarding the failure of the switch. Where the objection involves a debt from a consumer with a pre-payment meter, the gaining supplier may agree for the debt to be transferred to them. In this case both gaining and losing suppliers will communicate directly with each other to follow the Debt Assignment Protocol (DAP) and a new switch request could follow.

Other industry systems (such as DES, ECOES, MPRS and UK Link) will be notified of the switch and this will include consumer personal data (MPxN and premise data) provided by the CSS. The provision of any personal data to such industry actors

will be as part of defined processes; industry actors will not have direct access themselves to the data on the CSS.

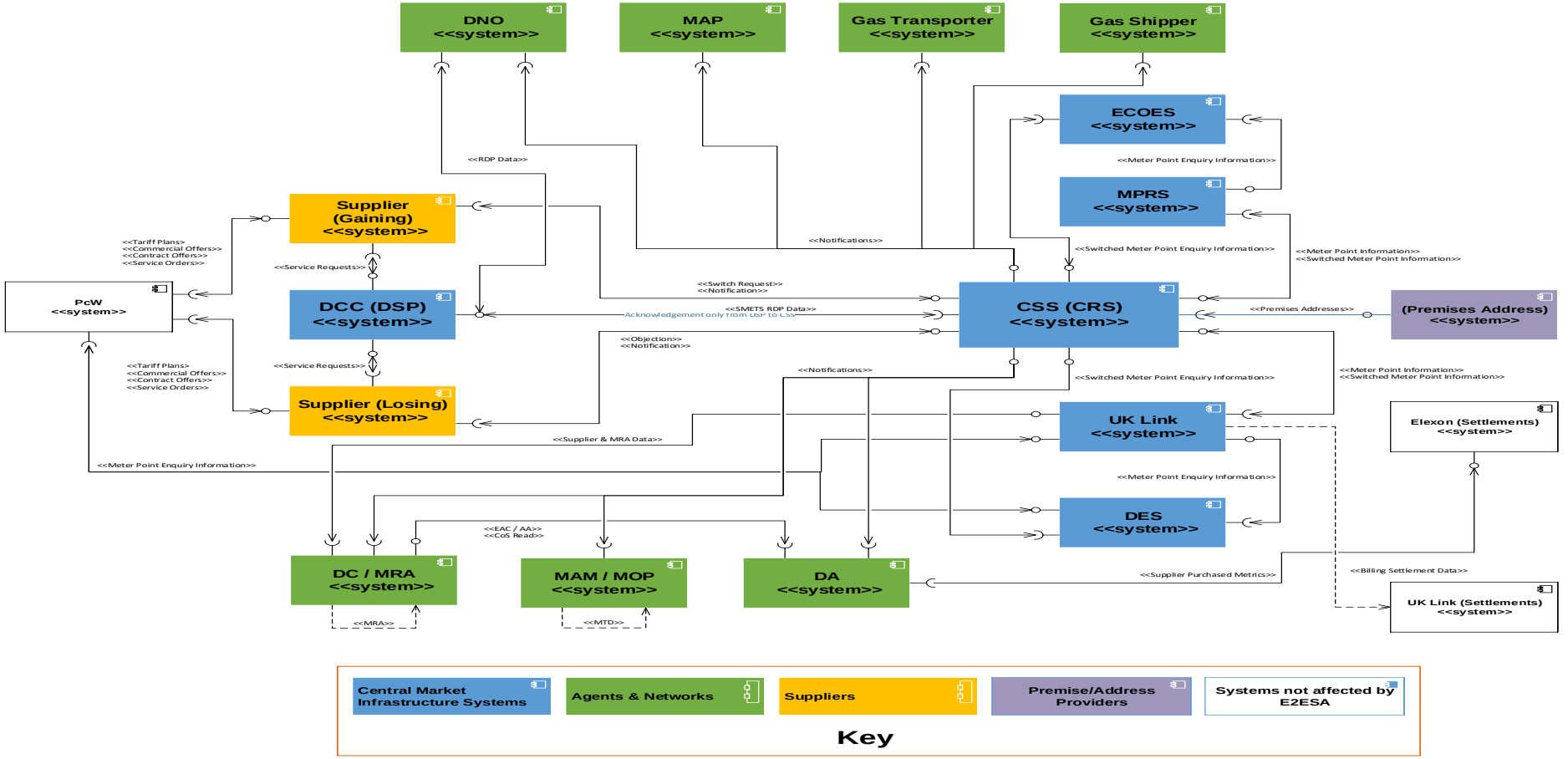
4.1.3 Other Processing

Personal data will be retained within the CSS beyond the switching of a consumer, since records of switches will be held for a time for audit and other purposes (such as market intelligence information under the RP3 option). The manner in which personal data is to be processed and the reasons for it are to be clearly defined and is to be in accordance with GDPR Article 6(f).

If the option for the Consumer Enquiry Service is to be taken forward by the Programme this kind of service will very likely also include personal data and this DPIA will need to be updated if it falls within scope, or a new DPIA for another system may be required.

4.2 Scope

The scope of the DPIA is shown diagrammatically in Figure 1 below.



4.2.1 CSS

The enduring technical solution and infrastructure is yet to be confirmed, but the key component of the CSS is expected to be one or more databases.

Personal data within the CSS will normally exist and be processed in a digital form and there is no requirement for personal data to be stored on digital removable media, or hard copy except in support of Business Continuity and Disaster Recovery solutions, and supporting system administration/maintenance activities. Each of these will be defined in a manner that enables privacy impacts and risk mitigation measures to be considered.

Personal data is expected to be viewed on screens and produced in small quantities in printed form for CSS administration/maintenance purposes. Again, all processing purposes shall be defined.

5 Privacy Risks

A separate document - the Programme's Information Risk Assessment (IRA) – identifies, scores and proposes mitigations for all security risks relating to the programme. These include risks to personal data and privacy as well as other security risks. However, the IRA is not a public document.

6 6 References

1	Switching Programme – Privacy Impact Assessment, Price Waterhouse Coopers for DCC, 03/06/16.
2	The Information Commissioner's response to the Competition and Market Authority's "Energy market investigation: notice of possible remedies" paper. 03/08/2015 Version 1.0 (final)

7 Abbreviations

CSS	Central Switching Service
CRS	Central Registration Service
DAP	Debt Assignment Protocol
DC	Data Collector
DCC	Data Communication Company
DNO	Distribution Network Operator
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
ECOES	Electricity Central Online Enquiry Service
E2E SA	End-to-End Switching Arrangements
GDPR	General Data Protection Regulation
GEMA	Gas and Electricity Markets Authority
ICO	Information Commissioner's Office

IRA	Information Risk Assessment
MAP	Meter Asset Provider
MEM	Meter Equipment Manager
MDD	Market Domain Data
MOP	Meter Operator
MPAN	Meter Point Administration Number
MPRN	Meter Point Reference Number
MPxN	Commonly used term to mean MPAN and/or MPRN
NO	Network Operator
ICO	Information Commissioner's Office
IRA	Information Risk Assessment
PCW	Price Comparison Website
PIA	Privacy Impact Assessment
TPI	Third Party Intermediary