MRA Service Company

MRASCo GDPR Policy

CHANGE HISTORY

VERSION	STATUS	ISSUE DATE	AUTHOR	COMMENTS
0.1	Draft	27/12/2017	Natasha Singh- Senior Consultant	Initial Drafting
1.0	Final	16/02/2018	Natasha Singh- Senior Consultant	Finalising
1.1	Final	29/03/2018	Kunal Sharma – MRA Administrator	Updated following review from MRA parties

DOCUMENT CONTROLS

REVIEWER	ROLE	RESPONSIBILITY	DATE
Kunal Sharma	MRA Administrator	Quality Review	01/02/2018
Kunal Sharma	MRA Administrator	Quality Review	29/03/2018

Gemserv

MRA Service Company

CONTENTS

Gemserv

MRA Service Company

1. INTRODUCTION

This policy governs the expected behaviours of all the Master Registration Agreement (MRA) parties and third parties, including Price Comparison Websites (PCWs) who are not party to the MRA but have access to the information processed in the Electricity Central Online Enquiry Service (ECOES) and Green Deal Central Charge (GDCC) databases, especially in relation to records that constitute Personal Data.
The General Data Protection Regulation (GDPR) expands on the Data Protection Act 1998 (DPA). Under Article 4(1) of the GDPR, Personal Data means any information relating to an identified or identifiable natural person ("Individual"); an identifiable person is one who can be identified, directly or indirectly. In the MRA context, personal Data includes customer addresses, Meter Point Administration Number (MPAN), an identification number and location.

An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. To the extent that a party to the MRA acts as a Data Controller in performing their obligations and in relation to the ECOES and GDCC databases, that party shall be responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Similarly, to the extent that third parties have access to information in the ECOES and GDCC databases that constitutes Personal Data, these third parties shall be responsible for ensuring compliance with the Data Protection requirements laid out in this policy.

MRA parties and third parties need to ensure continued and effective implementation of this policy. Non-compliance may expose the MRA parties and third parties to complaints, regulatory action, fines and/or reputational damage.

.

2. SCOPE

2.1. This policy applies to all MRA parties where a Data Subject's Personal Data is processed in the context of their business activities for the provision or offer of services to Data Subjects, particularly, in relation to the Personal Data processed in the ECOES and GDCC databases.

2.2. This policy also applies to third parties where a Data Subject's Personal Data is processed in the context of their business activities for the provision or offer of services to Data Subjects, particularly, when they have access to the ECOES and GDCC databases.

2.3. This policy applies to the processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

2.4. This policy has been designed to establish a baseline standard for the processing and protection of Personal Data by all MRA parties and third parties. Where national law imposes a requirement, which is stricter than that imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

2.5. The protection of Personal Data belonging to the employees of the MRA parties is not within the scope of this policy. This policy governs the processing of Personal Data of Data Subjects who are offered a service only.

3. DEFINITIONS

TERM	DEFINITION
Data Subject	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an address, a Meter Point Administration Number (MPAN), an identification number, location data, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controller	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Personal Data	Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Note, the Information Commissioners Office (ICO) classes the MPAN as personal data *where data is linked to the MPAN of a domestic property (or a commercial property where the business owner is a sole trader).*[2]
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Information Commissioner's Office (ICO)	An independent Public Authority in the UK responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear

[2] ICO Response to the CMA Energy Market Investigation: notice of remedies paper

	affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Third Country	Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

4. POLICY

4.1. Governance – Policy Dissemination and Enforcement

All MRA parties and third parties must ensure that all their employees who are responsible for the Processing of Personal Data in the ECOES and GDCC databases are aware of and comply with the contents of this policy. In addition, MRA parties and third parties will make sure that any party engaged to Process Personal Data on their behalf (i.e. their Data Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Data Processors, whether companies or individuals, prior to granting them access to Personal Data. In the event that Data Processors are already processing Personal Data on behalf of MRA parties and third parties, the latter must carry out a due diligence exercise as soon as possible to evaluate compliance with this policy and secure assurance thereof.

4.2. Governance – Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process prior to implementation.

MRA Parties and third parties must ensure that a Data Protection Impact Assessment (DPIA) is conducted, for any new and/or revised systems or processes which could affect ECOES or GDCC. A Data Protection subject matter expert must be consulted during the course of completing the DPIA. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection subject matter expert to assess the impact of any new technology uses on the security of Personal Data in ECOES and GDCC.

4.3. Governance – Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by the MRA parties and third parties in relation to this policy, the MRA Executive Committee (MEC) will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess compliance with this policy and the operational practices in relation to Personal Data, including:

- The assignment of responsibilities in relation to the use of the ECOES and GDCC databases;
- General data protection awareness;
- Assurance sought in relation to any Data Processor activities;
- Adherence to the MAP 15 and MAP 18
- Compliance with access agreements obligations
- Obtaining consent as lawful ground for processing Personal Data, where applicable and recording consent and
- The adequacy of procedures for redressing poor compliance.

Any major deficiencies identified will need to be reported to and monitored by an executive management team of the MEC.

4.4. Principles – Data Protection

MRA parties and third parties should adopt the following principles to govern their Processing of Personal Data in relation to ECOES and GDCC.

PRINCIPLE	DEFINITION
Principle 1: Lawfulness, Fairness and Transparency	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the MRA parties and third parties must tell the Data Subject, what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
Principle 2: Purpose Limitation	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means the MRA parties and third parties must specify exactly what Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.
Principle 3: Data Minimisation	Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.

	This means the MRA Parties and third parties must not store any Personal Data beyond what is strictly required.
Principle 4: Accuracy	Personal Data shall be accurate and kept up to date. This means the MRA parties and third parties must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.
Principle 5: Storage Limitation	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means the MRA parties and third parties must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.
Principle 6: Integrity & Confidentiality	Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. The MRA parties and third parties must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

4.5. Data Collection

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation.
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data;
- At the time of first communication, if used for communication with the Data Subject; or

- At the time of disclosure, if disclosed to another recipient.

4.6. Data Collection – Data Subject Consent

MRA parties and third parties will obtain Personal Data only by lawful and fair means and, where applicable, with the knowledge and Consent of the individual concerned.

Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, the MRA parties and third parties are committed to seek such Consent.

MRA parties and third parties shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for Consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

4.7. Data Collection – Data Subject Notification

MRA parties and third parties will, when required by applicable law, contract, or where they consider that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data in relation to the ECOES or GDCC.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

4.8. Data Use – Data Processing

The use of a Data Subject's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

MRA parties and third parties will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, the MRA parties and third parties will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- 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.
- Processing is necessary for compliance with a legal obligation to which the MRA parties and third parties are subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- 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 MRA parties and third parties.
- Processing is necessary for the purposes of the legitimate interests pursued by the MRA parties and third parties or by their Data Processors (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected.

4.9. Data Use – Data Quality

MRA parties and third parties will adopt all necessary measures to ensure that the Personal Data they Process is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by the MRA parties and third parties to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

- Restriction, rather than deletion of Personal Data, insofar as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the Data Subject.
    - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

4.10. Data Retention

To ensure fair Processing, Personal Data will not be retained by the MRA parties and third parties for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time for which the MRA parties and third parties need to retain Personal Data should be set out in a data retention policy. This should consider the legal and contractual requirements, both minimum and maximum duration. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

4.11. Data Protection

MRA parties and third parties will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to the ECOES and GDCC databases in which Personal Data is Processed.
- Prevent persons entitled to use the ECOES and GDCC databases from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data is not kept longer than necessary.

4.12. Data Subject Requests

The GDPR enhances existing data subject rights provided under the EU Directive and introduces new data subject rights. To the extent that MRA parties and third parties are acting as a Data Controller, they have certain obligations under the GDPR relating to Data Subjects rights and must take the

necessary steps to help the exercise of Data Subject rights. The process for attending to Data Subject rights must be outlined for attending to requests from individuals in a timely manner.

4.13. Law Enforcement Requests and Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty; or
- By the order of a court or by any rule of law.

4.14. Data Protection Training

The employees of all the MRA parties and third parties and employees of their Data Processors that have access to the Personal Data in the ECOES and GDCC databases will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, the MRA parties and third parties are encouraged to provide regular Data Protection training and procedural guidance for their staff.

4.15. Data Transfers

MRA parties and third parties may not transfer Personal Data outside of the European Economic area unless the following conditions are fulfilled:

- The MRA parties and third parties have provided appropriate safeguards in relation to the transfer (See Appendix A);
- The Data Subjects have enforceable rights and effective legal remedies;
- The MRA parties and third parties comply with their obligations under the GDPR by providing an adequate level of protection to any Personal Data that is transferred; and
- The MRA parties comply with reasonable instructions notified to them in advance by MRASCo with respect to the processing of Personal Data.

4.16. Data Transfers – Transfers to Data Processors

Where the MRA parties and third parties decide to use Data Processors, they need to secure assurance that the information will be Processed legitimately and protected appropriately by the recipient, as per Article 28.1 of the GDPR.

There is a requirement under Article 28.2 of the GDPR that the Data Processor shall not engage another Data Processor without prior specific or general written authorisation of the Data Controller. If this authorisation is granted, then an adequate Data Processing agreement will need to be entered into with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with the instructions of the MRA parties and third parties. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data, procedures for providing notification of Personal Data Breaches and all the requirements under Article 28.3 of the GDPR.

Regular audits of Processing of Personal Data by Data Processors, especially in respect of technical and organisational measures they have in place, should be undertaken. Any major deficiencies identified will need to be reported to and monitored by an Executive Management team of the MRA parties and third parties to have visibility over risks. Major deficiencies are defined as shortcomings regarding the GDPR principles, where non-compliance is severe.
Article 5 of the GDPR stipulates the conditions under which Personal Data should be processed:

- Personal Data shall be processed lawfully, fairly and in a transparent manner;
- Personal Data shall be collected and processed for explicit and legitimate purposes;
- Personal Data shall be adequate, relevant and limited to what is necessary;
- Personal data shall be kept accurate and up to date;
- Personal Data shall not be kept for longer than necessary; and
- Personal Data shall be processed using appropriate technical and organisational measures to ensure integrity and confidentiality.

Ultimately, where the other Data Processor fails to fulfil its Data Protection obligations, the initial Processor shall remain fully liable to the Data Controller for the performance of that other Data Processor's obligations. This means that the onus lies with the initial MRA party or third party, as per Article 28.4 of the GDPR.

4.17. Breach Reporting

In the event that the MRA parties and third parties suspect a Personal Data Breach has occurred due to the theft or exposure of Personal Data, they must immediately notify the MRASCo Central Administration Service (CAS) Team within 16 hours of a known incident providing a description of

what occurred. An internal breach log should be kept and updated, including pertinent facts relating to the incident, effects and remedial actions taken.

All reported incidents will be investigated to confirm whether or not a Personal Data Breach has occurred.

Further guidance can be found in the MRA Incident Management Policy.

5. POLICY EFFECTIVE DATE

The effective date is 11th May 2018

6. RELATED DOCUMENTS

MRA Incident Management Policy

MRA Service Company

APPENDIX A: ADEQUACY FOR PERSONAL DATA TRANSFERS

The following is a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data:

- EU Countries (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK).
- Iceland.
- Liechtenstein.
- Norway.
- Andorra.
- Argentina.
- Canada (commercial organisations).
- Faroe Islands.
- Guernsey.
- Israel.
- Isle of Man.
- Jersey.
- New Zealand.
- Switzerland.
- Uruguay.
- United States (Privacy Shield certified organisations).

APPROPRIATE SAFEGUARD MECHANISMS

Model Clauses.
Codes of Conduct.
Certification Mechanisms.

DEROGATIONS

- Explicit Consent.
- Compelling Legitimate Interests.
- Important reasons of Public Interest.
- Transfers in response to a foreign legal requirement.
- Data Protection Act approved contracts between Data Controllers and Data Processors.

MRA Service Company

Gemserv Limited

8 Fenchurch Place

London

EC3M 4AJ

Company Reg. No: 4419 878

T: +44 (0) 20 7090 1000

W: www.gemserv.com

Gemserv