MRA Service Company

MRASCo Incident Management Policy

CHANGE HISTORY

VERSION	STATUS	ISSUE DATE	AUTHOR	COMMENTS
0.1	Draft	15/11/2017	Rebecca Odubanjo Data Protection Consultant	Drafting and review
1.0	Final	01/02/2018	Steve Lewis	Finalised
1.1	Final	29/03/2018	Kunal Sharma	Update following review by 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

CONTENTS

1. SCOPE

This policy applies to all organisations with access to either Electricity Central Online Enquiry Service (ECOES) or the Green Deal Central Charge (GDCC) databases, who are involved in an actual, threatened or potential incident which involves a breach of information security.

2. POLICY STATEMENT

This policy is in line with the current Information Commissioner's Office (ICO) guidance for reporting, managing and investigating breaches of personal data.[1]

The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of data breach to the ICO, including some cases where the individuals affected need to be notified.

The implementation of this policy will ensure that incidents are reported to MRASCo Security Committee (MSC) and MRASCo Executive Committee (MEC) without undue delay.

3. INTRODUCTION

MRA parties as Data Processors are responsible for protecting the information it holds on behalf of MRASCo the Data Controller, and is legally required under the Data Protection Act 1998 (DPA) and GDPR to ensure the security and confidentiality of personal information processed on the ECOES and GDCC databases, especially records that constitute personal data, e.g. Meter Point Administration Numbers (MPANs) and customer addresses. MRA Parties must adhere to the guidelines presented in this policy in case personal data is compromised by malicious activity or by negligence. These responsibilities also apply to other organisations with access to these databases and information distributed by the MRA Administrator, Gemserv Limited (Gemserv) on behalf of MRASCo.

This policy focuses on the detection of incidents, and assessment of the requirement to report to MRASCo depending on the level of risk associated with the personal data involved.

Failure to notify a reportable incident to the ICO can lead to an administrative fine up to €10,000,000 or in case of an undertaking, up to 2% of MRASCo's worldwide annual turnover of the preceding financial year, whichever is higher.

[1] 2012 https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

4. OBJECTIVE

The objective of this Incident Management Policy is to detect, investigate and resolve any actual, suspected or potential breaches of security of the ECOES or GDCC databases. This policy will also advise on actions to take that will avoid, or reduce the impact or probability of a further similar reoccurrence.

This policy supports MRASCo's strategic business aims and objectives by:

- Ensuring that MRASCo has implemented an effective information incident management and response capability that supports the sharing of lessons learned;
- Ensuring that there is an agreed incident response and communications plan available, including the reporting of 'perceived' or 'actual' breaches to the MRASCo Board;
- Ensuring that the MRASCo Board's investigation and reporting of data protection incidents to the ICO conforms to GDPR requirements and does not conflict with the organisation's policies and procedures; and
- Facilitating MRASCo with the analysis of incident records to determine common threat patterns and existing threat vectors, to raise awareness among MRA parties to implement preventative measures or mitigation.

5. PERSONAL DATA BREACH EXAMPLES

Examples of a Personal Data Breach include the following:

- Unlawful disclosure or misuse of confidential data;
- Using personal data in a way incompatible with the originally specified purpose;
- Recording or sharing of inaccurate data;
- Information security breaches and inappropriate invasion of people's privacy;
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals;
- Inappropriate access controls leading to unauthorised use; and
- Any incident which involves actual or potential failure to meet the requirements of the GDPR and/or the common law of confidentiality.

Please note that the above list is not an exhaustive list of Personal Data Breach examples.

6. DEFINITIONS

TERM	DEFINITION
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.
Data Processors	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Subject	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Encryption	The process of encoding a message or information in such a way that only authorised parties can access it.
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.
MRA Parties	Authorised Users & Organisations granted direct to access to ECOES or the GDCC databases and parties with indirect access to data held on these databases.
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]
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.

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

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.

7. REPORTING PROCESS

MRA Parties are required to report incidents to MRASCo within 16 hours of becoming aware of it.

7.1. Incident severity assessment

Not all incidents have the same potential to adversely impact on the individuals whose data are involved. Assessing the severity of an incident relies on several factors, and there is no simple definition that covers what a serious incident entails. An incident that may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa.

Although the full extent of an incident is only known after it has been thoroughly investigated, there is a need to ascertain whether the risk could be classified as serious at an early stage, so as to act upon it for containment and reporting.

MRA parties are to evaluate their need to report data breaches to MRASCo, following the guidelines set out in this section 7 as closely as possible.

A reporting template is provided in Appendix A, which can also be used to log actions taken once the incident has been reported, as well as the outcomes of the incident.

The key factors for assessing the severity level of an incident are:

- The number of individual data subjects (customers) affected;
- The potential for significant distress or damage to the customer;
- The potential for reputational damage to MRASCo;
- The potential for litigation;
- The potential for media interest; and
- The type or category of personal data breach.

7.2. MRA Parties - Security of Information

The accountability principle under the GDPR requires MRASCo to be responsible for and to be able to *“demonstrate”* and *“evidence”* compliance with the Data Protection Principles.

MRA Parties must put in place adequate technical and organisational safeguards, to prevent incidents and have a common law, ‘duty of care’ and statutory obligation to protect confidential information against such events. Technical safeguards can be thought of as physical protection ranging from ICT passwords and firewalls to building security, whilst organisational safeguards are aimed at employees such as ensuring adequate training, policies, and procedures are in place.

An Incident can be caused by a number of factors such as:

- Negligence or human error;
- Unauthorised or inappropriate access, including processing confidential personal data without a legal basis;
- Loss or theft of information or equipment on which information is stored;
- Systems or equipment failure;
- Accidents;
- Unforeseen circumstances such as fire, flood and other environmental factors;
- Unauthorised access, using other people’s user IDs and passwords;
- Poor physical security;
- Inappropriate access controls allowing unauthorised use;
- Lack of training and awareness; and
- ‘Blagging’ offences where information is obtained by deception, by an unauthorised person.

All MRA Parties should already have an existing Incident Response Plan (IRP) covering Disaster Recovery, Business Continuity and the development of effective Communications Plans. It is recommended that this checklist is incorporated into the IRP.

7.3. Initial Reporting

Suspected Incidents

Initial information is often sparse and it may be uncertain whether an incident has actually taken place. Suspected incidents and ‘near misses’ should still be reported, investigated, and logged as lessons can often be learnt from them, once full facts have been obtained, these suspected incidents should be logged as closed, but remain documented.

Early Notification

MRA Parties must ensure incidents are reported to the MRASCo CAS team as soon as the organisation becomes aware of incidents, and no later than **16 hours**.

The limit of 16 hours is in place where it is suspected that a data breach has taken place, to ensure that MRASCo is in a position to respond to enquiries from third parties and to avoid unnecessary delay in MRASCo being notified.

For cyber incidents, you should notify the person responsible for any operational response, e.g. your internal IT team to contain the incident in the first instance. All MRA Parties should have robust policies in place to ensure that appropriate senior staff are made aware of all serious incidents, and a process is in place to notify the CAS team.

The immediate response to the incident and the escalation process for reporting and investigating this will vary according to the severity of the incident.

Where incidents occur out of hours, organisations should have arrangements in place to ensure on call Directors or other nominated individuals are informed of the incident and act to inform the appropriate contacts.

7.4. Out of hours reporting

MRASCo's Technical Service Provider, C&C Group Holdings Limited (C&C) are responsible for assessing the severity of incidents on the ECOES and GDCC databases.

In the event that a critical incident i.e. ECOES and/or GDCC are completely unavailable to Users, occurs outside 8am-6pm Monday to Friday C&C would receive an alert, assess the severity, and immediately contain the incident, if deemed as critical. On the next working day C&C with the support of Gemserv's Solution Design Support (SDS) team the issue would be further investigated and remediated. SDS would liaise with CAS to ensure that MRASCo's senior management are advised of the incident, and disseminate details to MRA Parties and customers (if personal data was affected).

Major/Minor incidents, i.e. a User is unable to access a record they should have access to, Users are to contact C&C via email, and the issue would be dealt with by C&C on the next working day.

7.5. Assessing the Severity of the Incident

The main factors for assessing the severity level of an incident are:

- The number of individual data subjects affected;
- The potential for significant distress or damage to the data subject;
- The type of personal data breach;

- The potential for media interest;
- The potential for reputational damage; and/or
- The potential for litigation

7.6. Reporting to MRASCo

When reporting an incident to the CAS team, please provide the following information, using the template found in Appendix A:

- Contact name and telephone number of person reporting the incident, as well as the name of the organisation;
- The type and volume of data affected;
- Location of the incident;
- Date and time;
- Confirmation that documented incident management procedures are being followed and disciplinary action will be invoked when appropriate;
- A factual description of what happened, e.g. theft, accidental loss, inappropriate disclosure, procedural failure etc. specifying the circumstances;
- The number of individual data subjects involved;
- The number of records involved;
- The format of the records (paper or electronic);
- If electronic records, whether these are encrypted or not;
- Whether the incident is in the public domain;
- Whether the media are aware or there is potential for media interest;
- Initial assessment of the severity level (final score); and
- Immediate action taken, including whether any staff have been suspended pending a full investigation.

7.7. Incident Management

An individual needs to be assigned internally by the reporting MRA party to attend to the incident and to liaise with MRASCo. The appointed individual, will be responsible for communicating and coordinating activities, as well as maintaining an audit trail of events and evidence. An investigation needs to be conducted to determine the causes of the breach, the scope, and possible remediation, along with expected outcomes and the identification of stakeholders.

7.8. Managing the Incident

MRA Parties should:

- Identify who is responsible for managing the incident and coordinating separate but related incidents, e.g. Master Admin User (MAU) and IT department;
- Identify who is responsible for the investigation and performance management;
- Identify expected outcomes;
- Identify stakeholders;
- Develop and implement an appropriate communications plan;
- Preserve evidence;
- Investigate the incident;
- Adopt formal documentation including configuration management and version control;
- Maintain an audit trail of events and evidence supporting decisions taken during the investigation;
- Institute recovery actions if possible;
- Institute counter measures to prevent recurrence;
- Invoke the disciplinary procedure as appropriate and document where a decision was taken not to take action (if it would be of relevance to a third party);
- Set target timescale for completing investigation and finalising reports;
- Produce a final report and obtain sign-off from the MRASCo Board and MRASCo Security Committee (MSC);
- Disseminate lessons learned to ECOES Users and members of the MRASCo Board/MSC; and
- Ensure that all investigations have been completed and any disciplinary action against staff has been settled to enable the incident to be closed.

7.9. Personal Data Breach Register

The MRA parties must maintain a record of all personal data breaches in the form of a register. Specific stakeholders identified by the MRA parties will record all actions that have been taken in relation to the breaches. The register will be maintained documenting each incident “comprising the facts relating to the personal data breach, its effects and the remedial action taken”.

The register should be maintained and regularly reviewed by the identified stakeholders to monitor patterns. The register should be stored locally in a shared folder with restricted access on a need to know basis.

The incident reporting template will also form part of the audit trail and should be retained with the register for completeness.

APPENDIX A: TEMPLATE TO LOG AND REPORT INCIDENTS TO MRASCO

INTERNAL INCIDENT REPORT FORM		
Date	Time	Location
Organisation name		
Name of person reporting incident		
Job title (MRA Contract Manager/MAU/ User) – *Please delete*		
Phone number		
Email address		
Description of incident:		
Level of incident		
Number of customers affected		
Volume of data affected		
Data format (paper / electronic)		
If electronic, are records encrypted?		
Is the incident in the public domain?		
Is the media aware of the incident?		
Immediate action(s) taken:		
Remedial action(s) taken:		
For MRASCo CAS Team use		
Incident reference number		
Received by		
Forwarded for action to		
Remedial action(s) taken		

Gemserv Limited

8 Fenchurch Place
London
EC3M 4AJ
Company Reg. No: 4419 878

T: +44 (0) 20 7090 1000
W: www.gemserv.com