

AEMO COMPLIANCE NOTIFICATION

PREPARED BY: Tim Sheridan, Gas Retail Market Development

VERSION: 1.0

RELEASE DATE: 6 June 2012

Provision of Bulk AEMO Standing Data

Introduction

This document outlines an apparent breach in terms of the confidentiality provisions in **section 91G(1)(a)** the National Gas Law (**NGL**) due to an apparent breach by AEMO of **clause 23(1)** of the Retail Market Procedures (South Australia) (**Procedures**) in relation to the provision of bulk standing data.

Section 91G(1)(a) of the NGL states that AEMO must take all reasonable measures to protect from unauthorised use or disclose of information given to it in confidence. Section 91G(3) states that AEMO makes unauthorised disclosure of protected information if the disclosure is not authorised under the NGL, the National Gas Rules (**NGR**), the Procedures or the Regulation.

91G—Protected information

- (1) AEMO must take all reasonable measures to protect from unauthorised use or disclosure information (**protected information**)—
 - (a) given to it in confidence; or
 - (b) given to it in connection with the performance of its statutory functions and classified under the Rules, the Procedures or the Regulations as confidential information.
- (2) AEMO makes unauthorised use of protected information if (and only if) it uses the information contrary to this Law, the Rules, the Procedures or the Regulations.

Note—

Section 91FD authorises AEMO (subject to the Law, the Rules, the Procedures and the Regulations) to use information (whether obtained by market information instrument or in any other way) for any purpose connected with the exercise of any of its statutory functions.

- (3) AEMO makes an unauthorised disclosure of protected information if the disclosure is not authorised under this Law, the Rules, the Procedures or the Regulations.

Clause 23 of the Procedures states the following:

23. AEMO to provide bulk AEMO standing data

- (1) In this clause, “**bulk AEMO standing data**”:
 - (a) in relation to a *network operator* – means the *AEMO standing data* for every *delivery point* in the *network operator’s GDS*; and
 - (b) in relation to a *user* – means the *AEMO standing data* for every *delivery point* which the *user* is the *current user*.

{Note: The purpose of this clause is to allow AEMO and *participants* to compare their databases at a particular time.}

AEMO in attempting to meet its obligations under clause 23 of the Procedures made an unintended and unauthorised disclosure of protected information in contravention of section 91G of the NGL and clause 23(1) of the Procedures, as the file intended for the Network Operator was delivered to a User instead.

This document outlines the details of AEMO’s apparent breach of section 91G of the NGL and clause 23(1) of the Procedures.

Circumstances of Apparent Breach

Clause 23(1) of the Procedures outlines the requirement for AEMO to provide bulk AEMO standing data in relation to Users and the Network Operator. The bulk AEMO standing data is provided to Users and the Network Operator on a monthly basis by Logica, AEMO's service provider for the Gas Retail Market Systems (**GRMS**).

On 1 April 2012, Logica completed its monthly processing of bulk AEMO standing data which involves sending emails to participants to notify them of the delivery of bulk AEMO standing data. In accordance with Logica's operational procedure for this process, for large participants the file is considered too large to email and is placed in the participant Outbox and an email is then sent to the participant notifying them of the delivery of the file.

On 24 April 2012, Logica received an email from a User (Origin Energy) informing them that they had incorrectly received a bulk AEMO standing data file for another participant. This file belonged to the Network Operator (Envestra) and the User indicated that the file had caused corruption within their systems which may have a confidentiality impact in the market.

On 26 April 2012, Logica responded to the User and acknowledged that a breakdown in the operational procedure had resulted in the incorrect file being placed in the User's Outbox. Logica provided the User with the correct file and apologised for the corruption to the User's systems caused by the error. Logica also requested that the User remove any reference to the incorrect file and notify AEMO when this has been done.

On 26 April 2012, Logica then notified AEMO of the delivery of the bulk AEMO standing data file to the wrong participant and indicated that remedial action had already been taken by Logica to rectify the problem. AEMO requested that Logica prepare an incident report that contained a full description of the matter.

On 2 May 2012, Logica delivered the incident report. AEMO received confirmation from the User that the physical copy of the bulk AEMO standing data file had been deleted from the User's systems. However, it would be likely to be at least a week until the data was deleted from the User's production systems.

On 16 May 2012, the User confirmed that the data had been deleted from its production systems.

AEMO Decision: Apparent Breach is Material

In applying the criteria outlined in the AEMO Compliance Process (see **Attachment A**), AEMO regards the apparent breach of section 91G of the NGL and clause 23(1) of the Procedures to be material in nature for the following reasons:

Materiality

Criterion 1: financial impact

The apparent breach resulted in the release of confidential and commercially sensitive information relating to User operating in the SA market.

Criterion 2: market system impact

There was a minor corruption to the User's system due to the receipt of the bulk standing data file. However, there were no deleterious impacts on the User's systems or market impacts due to the system impact of the breach on either the market participants: AEMO (including the GRMS); and AEMO Stakeholders that AEMO is aware of. The information was removed from the Users system

in a reasonable time therefore there was no opportunity for the information to be used inappropriately.

Criterion 3: operational impact

As the confidential information was destroyed by the User who received it, there was no observed operational impact in the market on either the market participants, AEMO, including the GRMS; and AEMO Stakeholders.

Criterion 4: any other factors

The unauthorised release of confidential information by AEMO, though its agent Logica, could result in the loss of confidence by market participants in the operation of the market by AEMO. If confidential information (especially information that is of a commercially sensitive nature) is provided by market participants to AEMO and this information is not respected or carefully looked after, then market participants may be disinclined to provide further information to AEMO. As market operations rely on information provided by the market participants, the loss of this information could seriously hinder market operations.

This breach highlights the need for AEMO to reinforce the application of its 'Confidential Information Guidelines' and 'Confidential Information Policy' and that AEMO and Logica staff are required to abide by the provisions with regards to the maintenance and safe keeping of confidential information. Further, that AEMO must develop automated processes to ensure that bulk AEMO standing data files are delivered to participants in a correct manner. As such, AEMO, through its agent Logica, has commenced a process of developing an automated scheduler for the delivery of bulk AEMO standing data files and has reminded its and Logica's staff of the need to pay careful attention to the confidentiality of participant data when sending notices to participants.

The occurrence of this breach coincides with the implementation of new processes associated with the implementation of a new model for the delivery of services to AEMO, by Logica, under the recently renegotiated services contract. The new service involved the use of Logica's Manila offices to perform operational IT activities of a routine nature. The failure therefor can be seen as a transitional issue that will be further addressed through, not only the reinforcement of the contract and policy obligations, but also the refinement of the operational processes.

ATTACHMENT A: AEMO COMPLIANCE PROCESS

Criteria AEMO will use in considering whether

- i. An incident is material; and**
- ii. If the incident is material whether it should be referred to AER.**

Criteria to consider in assessing materiality of apparent breach

The following criteria will be used by AEMO in determining whether an apparent breach is material in nature:

1. Whether or not the apparent breach is likely to cause significant financial impact on either of the following:
 - a. Market Participants;
 - b. AEMO, including the GRMS;
 - c. End use customers;
 - d. AEMO stakeholders.
2. Whether or not the apparent breach is likely to cause significant market system impact on either of the following:
 - a. Market Participants;
 - b. AEMO; including the GRMS;
 - c. AEMO stakeholders.
3. Whether or not the apparent breach is likely to use significant operational impact on either of the following:
 - a. Market Participants;
 - b. AEMO; including the GRMS;
 - c. End use customers;
 - d. AEMO stakeholders.
4. Any other factors considered relevant by AEMO.

Criteria to consider in referring a material apparent breach to AER

The checklist is the process AEMO will use to determine whether an apparent breach, if considered material, should be referred to the AER.

In determining whether or not a material apparent breach warrants referral to the AER, AEMO may have regard to the following matters:

1. Whether the complaint is frivolous or vexatious.
2. Whether the apparent breach has resulted in any costs being borne by AEMO (and therefore the market as a whole).

3. Whether or not the apparent breach appears to have arisen as a result of problems with the design/operation of the Procedures.
4. Whether the apparent breach by a Market Participant was caused by the conduct of AEMO.
5. Whether the apparent breach is an isolated event, or indicates a systemic problem with compliance.
6. Whether the apparent breach appears to have been made intentionally or maliciously.
7. Whether remedial action was taken by the Market Participant following discovery of the breach.
8. Whether the apparent breach has a potential anti-competitive effect.
9. Any other matters considered relevant by the AEMO.

National Gas Law

(From National Gas (South Australia) Act 2008—1.7.2009 – note individuals are responsible for using the latest version of the Procedures/legislation)

91MB—Compliance with Retail Market Procedures

(1) AEMO and each person to whom the Retail Market Procedures are applicable must comply with the Procedures.

(2) However, if there is an inconsistency between an applicable access arrangement and the Retail Market Procedures, a person is, to the extent of the inconsistency, not required to comply with the Procedures.

(3) If AEMO has reasonable grounds to suspect a breach of the Retail Market Procedures, it must, after making such inquiries and investigation as it considers appropriate, make a decision as to whether the breach is a material breach.

(4) If AEMO decides the breach is material, AEMO—

(a) must publish the decision and the reasons for it on its website; and

(b) may direct the person suspected of the breach to rectify it or to take specified measures to ensure future compliance (or both); and

(c) may refer the breach to the AER.

(5) A direction by AEMO under subsection (4)(b) must—

(a) specify the breach; and

(b) specify the date by which the direction is to be complied with; and

(c) be addressed to, and given to, the person suspected of the breach.

(6) A person to whom a direction is given under subsection (4)(b) must comply with the direction.

(7) AEMO must give a copy of its decision under subsection (3), its reasons for the decision and (if relevant) any direction under subsection (4)(b) to the AER.

(8) If AEMO decides the breach is not material, AEMO must—

(a) publish the decision and the reasons for it on its website; and

(b) give a copy of the decision and the reasons for it to the AER.

Note—

AEMO may provide the AER with relevant information (including protected information) related to a suspected breach of the Procedures. (For disclosure of protected information, see section 91GC(2)(b).)