CESI

REPORT   CONFIDENTIAL   DRAFT   B9023365

Client	AFESD – Arab Fund for Economic and Social Development
Subject	Developing the Interconnection Grid Code for the Pan Arab Electricity Market
	Data Exchange Code
Order	Arab Fund Grant Number 6/2018 dated 9/5/2019
Notes	-

N. of pages	10	**N. of pages annexed**	-
Issue date	16/12/2019		
Prepared	Antonio Carrano		
Verified	Daniele Canever		
Approved	Bruno Cova		

Mod. RAPP v. 11

Table of Contents

1 SCOPE OF APPLICATION

J.[1] The scope of application provides elements for a proper understanding of the provisions set in this Code.

In the building of an efficient integrated **Pan-Arab Electricity Market (PAEM)**, information exchange and data management shall become more connected. Increased information access and exchange lead to substantial efficiency gains not only does in grid operation and planning, but it also lowers market access barriers, ensures transparency in consumers' usage and creates new market.

In **PAEM**, data from **TSOs** and **Non-TSOs** are required for various operational tasks and case studies. This document addresses the general rules for the data handling and the rules that the **Parties** shall follow for the provision and usage of these data between **TSOs** and/or **Non-TSOs**. This **Code** is a complementary document to rules described in the "*League of Arab States Pan Arab Electricity Market General Agreement (2019/06/20)*", especially concerning issues regarding the protection of information as detailed in Chapter 10 of the above-mentioned document.

2 ROLES, RESPONSIBILITIES AND QUALITY OF DATA EXCHANGE

J. Each **Person** is responsible for the availability, reliability and validity of the data he provides, according to the specified requirements.

Each **TSO** shall be responsible for providing and using high quality data and **Information**. The availability, reliability, validity and accuracy of the exchanged data shall be ensured by **TSOs** to fulfill the requirements provided for in the **Arab Grid Code**. If nothing is specified, **Best Effort** shall be applied for the specific **Data Exchange**.

All **TSOs** shall jointly agree on key organizational requirements, roles and responsibilities in relation to **Data Exchange**. They shall apply to all **Data Exchange** and shall include organizational requirements, roles and responsibilities for the following elements:

   a) obligations for **TSOs** to communicate, without delay, to all neighboring **TSOs** any changes in the protection settings, thermal limits and technical capacities at the **International Interconnections** between their **Control Areas**;
   a) obligations for the adjacent **TSOs** to inform each other within agreed timescales of any changes in the data and information pursuant to the **Arab Grid Code**;
   b) detailed contents of the data and information established pursuant to the **Arab Grid Code**, including main principles, type of data, communication means, format and standards to be applied, timing and responsibilities;
   c) The frequency of information exchanges for **Real-Time Data Exchange**, scheduled data and update of structural data shall be defined.

The organizational requirements, roles and responsibilities shall be published by **PAEM**.

---

[1] **J.**: Justification

The **Market Secretariat** shall be appointed as the coordinator for each data collection related to a specific **Operational TSO Business**. The coordinator observes and checks the implementation of the **Data Exchange** and detects potential trouble and bottlenecks. At time intervals agreed by the contributors, he examines data set contents and procedures concerning the **Data Exchange**, and corrects them, if necessary.

3   DATA EXCHANGE AMONG TSOs

More information, regarding the **Data Exchange**, in the several parts of the **Arab Grid Codes** are reported. In **Operation Code**, **Planning Code**, **Connection Code**, **Scheduling & Dispatching Codes**, several Articles are dedicated to the **Data Exchange** among **Parties** to improve efficiently the security operation of the interconnection system. This Chapter highlights the structural and forecast **Data Exchange** to perform static load flow computation and dynamic assessment of the system. Further, in real time, each **TSO** shall exchange data on the **Operating Conditions** of its **Grid** with the other **TSOs** of the same **Synchronous Area**, using the IT tool for real-time **Data Exchange** at Pan Arab level as provided by **PAEM**.

3.1   Structural and Forecast Data Exchange

Neighboring **TSOs** shall at least exchange the following structural information related to the **Observability Area**:
   a)   the regular topology of substations and other relevant data, by voltage level;
   b)   technical data on transmission lines;
   c)   technical data on transformers connecting MV/LV network, demand facilities and generators' block-transformers;
   d)   the maximum and minimum active and reactive power of **Power-Generating Modules**;
   e)   technical data on phase-shifting transformers;
   f)   technical data on **HVDC Systems**;
   g)   technical data on reactors, capacitors and static volt-ampere reactive (VAR) compensators;
   h)   operational security limits defined by each **TSO** for each network element.
To coordinate the protection of their **Transmission Systems**, neighboring **TSOs** shall exchange the protection setpoints of the lines for which the contingencies are included as external contingencies in their contingency lists.
To coordinate their operational security analysis and to establish the common grid model, each **TSO** shall exchange, with at least all other **TSOs** from the same **Synchronous Area**, at least the following data:
   a)   the topology of VHV (Very High Voltage) and HV (High Voltage) **Transmission Systems** within its **Control Area**;
   b)   a model or an equivalent of the **Transmission System** with voltage below HV with significant impact on its own **Transmission System**;
   c)   the thermal limits of the **Transmission System** elements;
   d)   a realistic and accurate forecasted aggregate amount of injection and withdrawal, per primary energy source, at each node of the **Transmission System**, for different time-frames.
To coordinate the dynamic stability assessments, each **TSO** shall exchange with the other **TSOs** of the same **Synchronous Area** or of its relevant part the following data:
   a)   data concerning **Power-Generating Modules** relating to, but not limited to:

    i.   electrical parameters of the alternator suitable for the dynamic stability assessment, including total inertia;

    ii.   protection models;

    iii.   step-up transformer description;

    iv.   minimum and maximum reactive power;

    v.   prime movers' models and excitation system models suitable for large disturbances;

b) the data on type of regulation and voltage regulation range concerning tap changers and network transformers;

c) the data concerning **HVDC Systems** and FACTS devices on the dynamic models of the system or the device and its associated regulation suitable for large disturbances.

3.2 Real Time Data Exchange

J. Requirements to data collection describing current situation in order to support the **TSOs** in monitoring, coordinating and operating the **Transmission System**.

Real-Time Data Exchange is the focus of **Pan Arab Communication Network** (PACN). The measurements and grid topology from neighboring **TSOs** are important for the secure operation of the **Transmission System**. The type and the amount of data to be exchanged in **Real-Time Data Exchange** shall be mutually agreed upon between participating **TSOs** within the framework of the **ENTSO-E RG CE** policies. The **PACN** is meant for **Data Exchange** which helps the **TSOs** in monitoring and coordinating operation of the **PAEM Electricity System**. It is recommended not to use the exchanged data through **PACN** for real-time control applications.

The **Data Exchange** between communication partners is coordinated on a bilateral basis. The **Data Exchange** shall be agreed among the participating **TSOs**.

AS a minimum, each shall gather the following information, at least, about its **Observability Area** and shall exchange this data with all other **TSOs** to the extent that it is necessary for carrying out the operational security analysis:

a) frequency;

b) area control error;

c) measured active power interchanges between **Load Frequency Control areas**;

d) setpoint of the load-frequency controller;

e) aggregated generation infeed;

f) consumption;

g) planned outages and substation topologies; and,

h) **Operating Condition** (normal, alert, emergency).

Each **TSO** shall exchange, with the other **TSOs** in its **Observability Area,** the following data about its **Transmission System** using real-time **Data Exchanges** between the **TSOs'** supervisory control and data acquisition (**SCADA**) systems and **EMS**:

a) actual substation topology;

b) active and reactive power in each line bay, including transmission and lines connecting **Power-Generating Modules**;

c) regulating positions of transformers, including phase-shifting transformers;

d) measured or estimated busbar voltage;

e) reactive power in reactor and capacitor bay or from a static VAR compensator;

f) restrictions on active and reactive power supply capabilities with respect to the **Observability Area**. Each **TSO** shall have the right to request all **TSOs** from its **Observability Area** to provide real-time **Snapshots** of state estimated data from that **TSO**'s **Control Area** if that is relevant for the operational security of the **Transmission System** of the requesting **TSO**.

4 RULES TO HANDLE THE DATA

> **J.** Requirement to organize handling of **Operational TSO Business** data in such a way that it minimizes the risks of abusing the code of conduct and works in a sense of good faith and cooperation for joint benefit.

The **TSOs'** data needed, used for or resulting from operation of the interconnected **PAEM Electricity System** have to be handled under general rules concerning data confidentiality, acquisition, coordination and usage, back-up procedures and intellectual property. All **Parties** involved have the same rights and must comply with the same obligations at supporting **PAEM**'s internal tasks and its external communication policy in the limits set off herein.

4.1 Basic requirements

4.1.1 Data Handling
The **TSOs** shall exchange different kinds of data for **Operational TSO Business**, as described in the relevant parts of **Arab Grid Code** or stipulated by bilateral or multilateral agreements among **TSOs**. They are required to organize handling of their **Operational TSOs' Business** data to fulfil this part of **Code**.

4.1.2 Data Format
Each **TSO** shall use the standardized format for **Data Exchange** as agreed within **PAEM**. In case of no standardized format, the format shall be agreed among the **TSOs** concerned.

4.1.3 Data Access
A **TSO** participating in the creation of **Common Information** related to a specific **Operational TSO Business** based on the data provided by other **TSOs** must share this **Common Information** or the data derived from it with other contributing **TSOs**. The contributing **TSO** has the right to extend or restrict this use into more precise agreements. Such a restriction or extension shall be duly recorded in writing.

4.1.4 Data Confidentiality.
Any individual and/or common information falling into one of the following categories shall be considered **Confidential Information**:

a) Any **Information** pertaining to the interests of any **Party** developed or acquired by any **Party** and that is proprietarily or competitively sensitive.

b) Any critical energy infrastructure **Information** about proposed or existing asset, which is related to the generation, transmission or distribution of electricity and which could be used for planning an attack or for any other similar type of misuse. Critical infrastructure comprises existing and proposed systems and assets (whether

physical or virtual) of which the incapacity or destruction would negatively affect security, economic security, public health or safety or any combination of those factors.

c) Any investigation report and any records produced for or during an investigation of disturbance in the system.

d) Cybersecurity information that could damage cybersecurity.

e) All other information recognized as confidential however not falling into any of the categories above.

Confidentiality does not apply to the following data:

a) Data in the public domain other than by reason of breach of the Article 4.1.4; or any other relevant bi- and/or multilateral agreement on confidentiality protection;

b) Data already lawfully in the possession of the **Receiving Party** prior to its receipt from the **Disclosing Party**;

The **Disclosing Party** shall mark as confidential any information submitted to the **Receiving Party** that it reasonably believes to be confidential. Any **Common Information** which involves **Confidential Information** shall be treated as confidential.

Only the **TSOs** may use the **Confidential Information,** strictly for their **Operational TSO Business** needs, or otherwise agreed or in the case of request from authorized authorities under national or international law. This **Confidential Information** may only be disclosed to the managers, employees, advisers and representatives of the **TSOs** if those persons are bound by an obligation of confidentiality.

4.1.4.1 Non-Disclosure of Confidential Information

No disclosure of **Confidential Information** is allowed in any way, matter or form, in whole or in part, to any **Party** as a rule. By derogation to this, disclosure is allowed in case of:

a) the explicit consent of the **Disclosing Party** and to the conclusion of a non-disclosure agreement which provides for, at least, equivalent obligations of confidentiality as provided for in this Article 4.1.4.

b) A **TSO** becomes legally compelled, or expects that it will be legally compelled, to disclose the **Confidential Information** to any authority. In such a case it will, unless it is not authorized to do so because of national or international law, provide prompt notification of it to the **TSO** that has provided that **Confidential Information**. The **Parties** agree on the content and extent of the **Confidential Information** to be divulged, in accordance with the relevant law, the authority orders and the general rules applied within **PAEM**. The disclosure of the Confidential Information is made in a proper and discreet manner. The **TSO** who discloses **Confidential Information** under this Article shall inform the **Receiving Party** of the confidential nature of the **Confidential Information** and shall ask the **Receiving Party** to treat the information, if possible, under the same terms and obligations as this Article.

4.1.4.2 Confidential Information handling

The **TSO** shall organize its data handling in such a way as to minimize the risks of misuse or unauthorized access or disclosure of **Confidential Information**.

Any **Disclosing Party** and **Receiving Party** dealing with **Confidential Information,** has the right to rule its use, and protection in more precise bilateral agreements. In case of

contradiction or inconsistency between such agreement and this Article, this Article supersedes the bilateral agreement.

4.1.4.3 Use of Individual Information

Each **Party** may make free use of its own **Individual Information** and/or **Common Information** for any purpose without constraints.

4.1.5 Duty to mitigate

If a **TSO** is temporarily unable to provide its required information in due time, it shall inform the other **TSOs** involved immediately and shall use all reasonable efforts to mitigate the effects of the event which has caused the failure.

4.1.6 Non-TSO data

Chapter 4 also applies to data required from **Non-TSOs** for **Operational TSO Business**. These data may be provided by a **TSO** to the **Common Information** of the **PAEM** under the condition that there is an agreement between the **TSO** and the **Non-TSO** allowing such diffusion.

4.1.7 Responsibility

Each provider is responsible for the availability, reliability and validity of the data he provides, according to the specified requirements.

4.1.8 Miscellaneous

4.1.8.1 Property

Common Information derived from the **Individual Information** of all **TSOs** is owned by the **PAEM** while the Individual Information itself is and remains the exclusive property of the **TSO**. If a **TSO** uses data on behalf of another **Party**, the data is treated in the same way as **Individual Information** of the **TSO**, but it remains the property of the disclosing **Party**. Each **TSO** may process the **Common Information** for individual use. No change in the information limits the restrictions on the use of the data.

4.1.8.2 Intellectual property

The **Data Exchange Code** is not to be construed as granting the **Receiving Party** any license or intellectual property rights related to the data and its future use, unless explicitly agreed otherwise in writing.

4.2 Communication Infrastructure

J. Technical infrastructure needed to exchange the requisite data shall be available.

The **PACN** between **TSOs** shall be implemented to provide the necessary infrastructure that facilitates and supports **Data Exchange**s among **TSOs**.
The availability of technical infrastructure needed to **Data Exchange** shall be ensured by the **TSOs**.
The implementation, operation, extension and maintenance of the **PACN** among the **TSOs** is necessary.

The **PACN** shall be a private network dedicated to **Data Exchange** between **TSOs** and operates under the responsibility of the **TSOs** and the management of the relevant **Coordination Center**.

The purpose of **PACN** is to exchange:
a) Telecontrol real time information.
b) Non-real time services such as file transfer for exchange of transmission schedules, network model, planning data or statistics (File Transfer Protocol-FTP).

The primary scope of the **PACN** is the **Real-Rime Data Exchange**, in support of **TSO** operational processes, aimed at enhancing the security of electricity supply in the **Member States**.

As a result of this, real-time data traffic has the highest priority amongst all the other data communicated.

Every **TSO** shall to be connected to the **PACN**.

All other **Non-TSOs** and **Non-PAEM TSOs** can be connected to the **PACN.**

There must not be any direct physical or logical connection between **PACN** and **Internet**. All **Data Exchange** between **PACN** and the outside world should be done under full security procedures. The separation of **PACN** from insecure networks must be guaranteed by use of intermediate gateways or a **Demilitarized Zone**.

4.2.1 *Other communication way*

As fallback communication for **TSOs**, usually the public communication infrastructure (public mobile communication or public landline) is used. In daily operation all partners and market participants can be contacted via public communication. In case of blackout or disturbances situations may occur where these **Parties**, only having public communication access, temporary cannot be contacted anymore.

In case of complete shortfall of regular and fallback communication, the most important partners are provided with satellite communication as contingency communication. Therefore, this form of communication is also a fallback solution for all other forms of communication.

5 PUBLICATION

J. Requirements to define the information (incl. scope, level of aggregation of data and derived information) dedicated to internal and external publication.

PAEM defines the **Information** (including scope, level of aggregation of data and derived information) dedicated to internal and external publication.

PAEM publications are written in English/Arabic language.

The **Market Secretariat** of **PAEM** is responsible for the supervision of the publication and circulation of documents. The list of documents for external publication is kept by the **Market Secretariat**.

Regular publications with mainly recurrent statistical content are validated by the providers. All other publications are approved by the **Arab TSOs Committee**.

Data sent by the **Member States** for periodical publication can be found in monthly, quarterly, half-yearly or yearly publications that can be accessed from the **PAEM** website.