

P7 – Policy 7: Data Exchanges

Chapters

A. Code of conduct and generic rules to handle the data

Introduction

In ENTSO-E RG CE, data from TSOs and Non-TSOs are required for various operational tasks and case studies. This Policy addresses the general rules for the data handling and the rules that the parties have to follow for the provision and usage of these data (Code of Conduct) between TSOs and/or non-TSOs.

Policy 7 is a complementary document to existing rules described in the ENTSO-E Articles of Association and Internal Regulations, especially concerning issues regarding the confidentiality of data.

A. Rules to handle the data - Code of Conduct

Introduction

The TSOs' data needed, used for or resulting from operation of the interconnected ENTSO-E RG CE 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 ENTSO-E's internal tasks and its external communication policy in the limits set off herein.

Definitions

- A-D1. Operational TSO Business.** Real-time, periodical and on request tasks performed for transmission system operational planning, forecast, operation and analysis, that require exchange of data which, or a part of which, is necessary to carry out their work properly.
- A-D2. Operational Data (Data).** Operational data includes inter alia Day Ahead Congestion Forecast Data (DACF), Intra-Day Congestion Forecast Data (IDCF), snapshots, reference data sets, load-frequency control data, frequency monitoring data, k-factors, frequency measurement campaign data, data on power exchanges and WAMS data as well as real-time measurements.
- A-D3. Data Exchange.** Delivery and reception of data between at least two parties.
- A-D3.1 On-request Data Exchange.** Data Exchange which is usually carried out to support a single analysis or report on operational or security aspects.
- A-D3.2 Periodic Data Exchange.** Data Exchange which is carried out on a periodic basis (e.g. hourly, daily, weekly, monthly, yearly or seasonally).
- A-D3.3 Real-Time Data Exchange.** Data Exchange which describes a current situation in the system, done also on request e.g. after a change of status or value.
- A-D3.4 Bilateral Data Exchange.** Data Exchange between two parties only (A-D6).
- A-D3.5 Multilateral Data Exchange.** Data Exchange among more than two parties (A-D6).
- A-D3.6 Internal Data Exchange.** Data Exchange, involving only the ENTSO-E RG CE (A-D6.1) or one or more ENTSO-E RG CE TSO(s) (A-D6.2.1) as participating parties.
- A-D3.7 External Data Exchange.** Data exchange, involving a non-TSO (A-D6.3) or a non-ENTSO-E RG CE TSO (A-D6.2.2).
- A-D4. ENTSO-E RG CE Data.** Data used for the purposes of the Data Exchange, belonging either to an ENTSO-E RG CE TSO (A-D6.2.1) or to a group of ENTSO-E RG CE TSOs or to the ENTSO-E RG CE (A-D6.1).
- A-D5. Non-ENTSO-E RG CE Data.** Data belonging either to a Non-ENTSO-E RG CE TSO (A-D6.2.2) or to a non-TSO (A-D6.3).
- A-D6. Parties.**
- A-D6.1 ENTSO-E RG CE.** ENTSO-E RG CE is the Regional Group established under the System Operation Committee of ENTSO-E in accordance with Article 27 of Internal Regulation of ENTSO-E.
- A-D6.2 TSO.** A TSO means a legal entity responsible for operating the transmission system in a given area and/or a company which fulfils Operational TSO

Business tasks on behalf of one TSO or a group of TSOs and which is owned by one or more TSOs.

A-D6.2.1 ENTSO-E RG CE TSO. TSO which is a member of ENTSO-E RG CE, or any affiliate of at least one ENTSO-E RG CE TSO and performing Operational TSO Business tasks on behalf of this (or these) ENTSO-E RG CE TSO(s)

A-D6.2.2 Non-ENTSO-E RG CE TSO. TSO which is not a member of ENTSO-E RG CE.

A-D6.3 Non-TSO. Legal entities not dealing with Operational TSO Business including:

A-D6.3.1 Market Players. Distributors, producers, power exchanges, traders, consumers, etc.

A-D6.3.2 Authorities. Governments, regulators, European institutions, courts and tribunals, etc.

A-D6.3.3 Other Parties. Universities, research institutions, consultants, manufacturers, engineering offices, departments or companies of vertically integrated companies or groups not dealing with Operational TSO Business, etc.

A-D6.4 Disclosing Party. A party delivering data, being either an ENTSO-E RG CE TSO (A-D6.2.1) or the ENTSO-E RG CE (A-D6.1).

A-D6.5 Receiving Party. A party receiving data, being any party as defined in A-D6.1, A-D.6.2 and A-D.6.3.

A-D7. Information. The term includes, but is not limited to, technical, financial, commercial and operational data in whatever form (whether written, electronically or by any other means) related to one specific Operational TSO Business (A-D.1).

A-D7.1 Individual Information. Data belonging to one ENTSO-E RG CE TSO (A-D6.2.1).

A-D7.2 Common Information. Data set resulting from merging or aggregating shared individual information and all derived data.

A-D7.3 Confidential Information. Any individual and/or common information falling into one of the following categories:

A-D7.3.1 Business and market information. Any information pertaining to the interests of any party developed or acquired by any party and that is proprietarily or competitively sensitive.

A-D7.3.2 Critical energy infrastructure information. Any information about proposed or existing assets, 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.

A-D7.3.3 Investigation reports. Reports and any records produced for or during an investigation of disturbance in the system in the framework of the Multilateral Agreement (MLA), i.e. the agreement between all ENTSO-E RG CE TSO rendering some policies of the Operation Handbook binding upon them.

A-D7.3.4 Cybersecurity information. Information that could damage cybersecurity.

A-D7.3.5 Other. All other information recognised as “confidential” (e.g. under other policies of the Operation Handbook) however not falling into any of the categories above.

A-D7.4 Data excluded from Confidential Information. Confidentiality does not apply to the following data:

A-D7.4.1 Data in the public domain other than by reason of breach of this Policy; or any other relevant bi- and/or multilateral agreement on confidentiality protection;

A-D7.4.2 Data already lawfully in the possession of the Receiving Party prior to its receipt from the Disclosing Party;

Standards

A-S1. Technical Infrastructure. The availability of technical infrastructure needed to exchange the requisite data has to be ensured by TSOs (A-D6.2), as provided for in Policy 6 of the Operation Handbook.

A-S2. Data Quality. The availability, reliability, validity and accuracy of the exchanged data have to be ensured by TSOs (A-D6.2) so as to fulfil the requirements provided for in the related policies of the Operation Handbook. If nothing is specified, best effort has to be applied for the specific Data Exchange.

A-S3. Data Handling. The TSOs (A-D6.2) have to exchange different kinds of data for Operational TSO Business, as described in the relevant policies of the Operation Handbook or stipulated by bilateral or multilateral agreements among TSOs. They are required to organise handling of their Operational TSO Business’ data to fulfil this Code of Conduct.

A-S4. National Data Coordinator. Each TSO has to designate or delegate a National Data Coordinator, who is an interface between TSOs, the ENTSO-E RG CE and external stakeholders for all issues related to data. National Data Coordinators do not intervene into regular data activities, but intervene in cases that cannot be settled via the correspondents’ networks.. Whenever exceptional data delivery is requested, National Data Coordinators decide e.g. on the submission of Confidential Information on the basis of national laws as well as of existing contracts between their TSO (A-D6.2) among themselves and their TSOs and any Non-TSO (A-D6.3).

A-S5. Data Correspondents. Each TSO (A-D6.2) has to designate appropriate data correspondents, who are responsible for the quality and delivery of operational data as defined in A-D2.

A-S6. Data Format. Each TSO (A-D6.2) shall use the standardised format for Data Exchange as agreed within ENTSO-E RG CE. In case of no standardised format, the format shall be agreed among the TSOs concerned.

A-S7. Data Access. An ENTSO-E RG CE TSO (A-D6.2.1) participating in creation of Common Information (A-D7.2) related to a specific Operational TSO Business (A-D1) based on the data provided by other ENTSO-E RG CE TSOs has to share this Common Information or the data derived from it with other contributing ENTSO-E RG CE TSOs. The contributing ENTSO-E RG CE 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.

A-S8. Data Confidentiality.

A-S8.1 Identification of Confidential Information. The Disclosing Party (A-D6.4) shall mark as confidential any information submitted to the Receiving Party (A-D6.5) that it reasonably believes to be confidential. Any Common Information (A-D7.2) which involves Confidential Information shall be treated as confidential.

A-S8.2 Use of Confidential Information. Only the TSOs may use the Confidential Information for their strict Operational TSO Business needs or otherwise agreed or in the case of request from authorised authorities under national or international law.

This Confidential Information may only be disclosed to the managers, employees, advisers and representatives of the TSOs as long as those persons are bound by an obligation of confidentiality with the same content as in this Policy.

A-S8.3 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-S8.3.1. The explicit consent of the Disclosing Party(ies) and to the conclusion of a non-disclosure agreement (NDA) which provides for, at least, equivalent obligations of confidentiality as provided for in this Policy.

A-S8.3.2. 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 authorised 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 ENTSO-E RG CE. The disclosure of the Confidential Information is made in a proper and discreet manner. The TSO who has to disclose Confidential Information under this paragraph 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 policy.

A-S8.4 Confidential Information handling. The TSO has to organise its data handling in such a way as to minimise the risks of misuse or unauthorised access or disclosure of Confidential Information.

A-S8.5 Any Disclosing and Receiving Party dealing with Confidential Information, has the right to rule its use, protection, etc. in more precise bilateral agreements. In case of contradiction or inconsistency between such agreement and this Policy, this Policy supersedes the bilateral agreement.

A-S9. Duty to mitigate. If an ENTSO-E RG CE TSO is temporarily unable to provide its required information in due time, it has to warn the other ENTSO-E RG CE TSOs involved immediately and shall use all reasonable efforts to mitigate the effects of the event which has caused the failure.

A-S10. Miscellaneous legal provisions

A-S10.1 Property. Common Information derived from the Individual Information of all TSOs is owned by the ENTSO-E RG CE 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 other agreement excepted. Each TSO may process the Common Information for its

individual use. No change in the information limits the restrictions on the use of the data.

A-S10.2 Intellectual property. This Code of Conduct 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.

A-S10.3 Hardship. If there should occur any extraordinary event or circumstance, independent of the will of the TSO, which is unforeseeable (including material legislative changes or positions/practices of authorities) and fundamentally modifies the fulfilment of this Policy, the parties shall, in due time, notify each other and ENTSO-E RG CE of the event and seek to adjust it with bilateral or multilateral agreements, while protecting their respective interests.

A-S10.4 Internal reorganisation. If a TSO loses its responsibility for the system operation, i.e. as a consequence of a restructuring process, this TSO has to inform ENTSO-E RG CE in due time and remains compelled to respect this Code of Conduct for the following twelve months. The succeeding entity shall be compelled to fulfil this Code of Conduct.

A-S10.5 Non-TSO data. This Code of Conduct 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 ENTSO-E RG CE under the condition that there is an agreement between the TSO and the non-TSO allowing such diffusion.

A-S10.6 Responsibility. Each provider is responsible for the availability, reliability and validity of the data he provides, according to the specified requirements.

A-S11. Publication

A-S11.1 Data to be published. ENTSO-E RG CE defines the information (including scope, level of aggregation of data and derived information) dedicated to internal and external publication.

A-S11.2 Language. ENTSO-E RG CE publications are written in English, in accordance with ENTSO-E general rules and practice.

A-S11.3 Role of ENTSO-E. The secretariat of ENTSO-E (the Secretariat) is responsible for the supervision of publication and circulation of documents. The list of documents for external publication is kept by the Secretariat. Regular publications with mainly recurrent statistical content are validated by the providers. All other publications are approved by the Plenary of ENTSO-E RG CE.

A-S11.4 Publications. Data sent by the ENTSO-E RG CE members for periodical publication can be found in monthly, quarterly, half-yearly or yearly publications that can be accessed from the ENTSO-E website.

Guidelines

A-G1. Coordinator. A TSO is appointed in writing as the coordinator for each data collection related to a specific Operational TSO Business. For a collection of data on request, the TSO in charge of performing the analysis or in charge of reporting shall coordinate the data. 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.

A-G2. Use of Individual Information. Each party may make free use of its own Individual and/or Common information for any purpose without constraints.