POSITION PAPER

Brussels, 20 January 2020

Accelerating Smart Grids Deployment: Implementing the latest EU Smart Grids Task Force Recommendations in support of the Clean Energy Package

A decade ago, the EU Smart Grids Task Force was set up to advise the European Commission on issues related to the development and deployment of smart grids. It is supported by several expert groups that focus on energy value chain debates on specific smart grids topics. In 2017, three new expert groups started their work to advise the Commission on preparing the grounds for potential secondary legislation on data exchange, cybersecurity for the electricity sector and demand response, for implementing the Clean Energy Package and the revised Electricity Regulation EU 2019/943 and Electricity Directive 2019/944 in particular. Their intensive work resulted in three recently published reports with specific recommendations. Orgalim was actively engaged in the three working groups and endorses the final reports.

For a successful implementation of the Clean Energy Package and the EU's 2030 energy and climate framework, it is now important to carry these reports forward to the next level and proceed with the development of the respective network codes and implementing measures as foreseen in article 59 of the Electricity Regulation 2019/943. We call on the incoming European Commission to secure the timely implementation of this provision as the next step and to progress with the implementation of the final EU SG TF reports as follows:

1. EXPERT GROUP 1 REPORT ON DATA FORMAT AND PROCEDURES

Customers are entitled to receive their electricity and gas consumption data and allow access to it to any third party of their choice. To facilitate this, standardised national arrangements covering a semantic model of the data to be exchanged, the content of the data, potentially the format in which data is provided to parties, and the systems and procedures, including communications protocols, need to be in place. To facilitate the interoperability of national and cross-border services and products, convergence of such arrangements across the EU is needed.

Orgalim
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438

EG1 delivered a set of recommendations on the scope and coverage of a potential specific EU secondary legislation that will set up the requirements and the procedures for such arrangements on data access and exchange and facilitate achieving and maintaining full interoperability of energy services within the EU.

In our view, the following principles enshrined in the recommendations are particularly important for implementing article 59 of the Electricity Regulation:

- Building on available reference models, a **common European role model**[1], **common information model**[2] and a **core process model**[3] should be adopted and used.
- High-level **business requirements**, formulated in a technology-and technical-architecture-neutral way, should be the basis for interoperability.
- Regarding the **emerging services**, existing role models need to be extended to take into account new roles; new business use cases should be described using the same methodology.
- To improve interoperability, available **European standards** should be adopted and used.
- A **roadmap** is required to achieve and maintain interoperability, and all relevant stakeholders must be involved in the process.

Orgalim also particularly underlines the conclusion drawn regarding emerging services that 'download my data' or 'share my data' services do not yet exist in the majority of member states. This opens the opportunity to harmonise the processes and data format in Europe, so that tools developed based on this data can enter an open European market. To allow for the fast growth of emerging services, data formats based on a common 'reference ontology' must be in place.

We specify our detailed opinion on all EG1 recommendations in Annex I.

2. EXPERT GROUP 2 REPORT ON CYBERSECURITY

The energy infrastructure is one of the most critical assets for a modern society and a backbone for its economic activities, welfare and stability. Making the European energy grid smarter is necessary for improving efficiency and managing the complexity in a future system with increased variable renewable energy sources. It also enables citizens to become active consumers ("prosumers") and better manage their consumption or produce, store and ultimately trade and sell their own energy. Digitalisation is key to optimise the energy systems, ensure safety and security of supply and offer more affordable energy services. Therefore, it is in the interest of the EU, its member states and industry, to secure its energy infrastructure against cyber risks and threats. By doing so, we can also set global leadership standards in managing the challenge.

[1] A model representing core functions/responsibilities in the energy sector and their interdependence.
[2] A representation of concepts and the relationships, constraints, rules, and operations to specify data semantics for the energy sector for semantics.
[3] A representation of harmonised processes for information exchange within the energy sector so that these processes may be implemented as such or as the basis for a customised version according to regional/national business needs.

This expert group focused on the scope for the potential network code on cybersecurity rules in the electricity subsector, building on the existing legislation (Network Information Security Directive EU 2016/1148 and General Data Protection Regulation 2016/679) and identifying the gaps.

Orgalim also welcomes the recommendations of EG2 and supports the recommendation for a harmonised certification approach across the European digital single market. We recognise the importance of a **holistic approach** for cybersecurity, as it combines baseline cybersecurity requirements for the electricity subsector with the needs of the electricity subsector stakeholders. The application of **ISO/IEC 27001** and **IEC 62443** allows addressing cybersecurity in the electricity subsector while supporting energy-specific, established and proven standards such as IEC 62351 and providing the flexibility to meet individual system requirements and use cases. The application of IEC 62443 offers the opportunity to have a single standard for Operational Technology (OT) to certify the vertically integrated transmission and distribution domain in a consistent cybersecurity approach across the energy value chain that will provide clarity for suppliers, integrators and operators that ultimately eventually support the objective of a baseline security in the electricity subsector.

In a holistic cybersecurity approach, specific risks can be mitigated by a defence-in-depth approach while considering not only the product but also the overall system with the different stakeholders such as suppliers, integrators and operators with appropriate cybersecurity measures in place.

Should the scope of the future network code not stop "before the meter", the following aspects should be taken into account regarding smart meters:

- Considering that a smart meter is an edge device for the electrical grid and the home application area, and considering that the EG2 report is addressing the electrical grid domain only, Orgalim expresses its support for a holistic cybersecurity approach.
- For countries where common criteria are already applied by legislation for smart meters, Orgalim could agree with safeguarding the existing implementation. For the limited, domain specific home application area of smart meters, common criteria could be considered as an alternative and equivalent approach to IECEE for the certification of smart meters, however not beyond.

We specify our detailed opinion on the EG2 recommendations in Annex II.

3. EXPERT GROUP 3 REPORT ON DEMAND SIDE FLEXIBILITY

Demand-side flexibility refers to enabling the final customer to become active in the market, and to provide services to system operators to ensure efficient system operation on a regional level. It can play a key role in reducing overall system costs.

This expert group has identified the main barriers and proposed recommendations to advance the development of demand-side response. These barriers and recommendations have been clustered around the following main topics: customer perspective; market access; flexibility product design; market processes and coordination; measurement, validation and settlement; technical solutions and platforms to fulfil system and grid needs; privacy and security; market and technology readiness.

We highlight the following recommendations that require urgent action:

- National regulatory authorities should ensure that Transmission System Operators (TSO) and Distribution System Operators (DSO) revenue regulation and network tariffs structures take the **costs and benefits of flexibility for the system** into account and that they are non-discriminatory.
- As to market access, we agree on the need for **standardisation, or at least interoperability, of hardware** (EMS, smart meters, charging stations etc.), and stress that this should apply only to the new generation of products. We also support the harmonisation of market rules and energy products.
- Concerning the flexibility product design, we should allow for the market to define the suitable products. However, providing **locational information** should be a requirement for flexibility products offered for congestion management. Also, it is necessary to define **data requirements** that flexibility service providers must deliver to the relevant system operator or responsible market operator.
- As regards market processes and flexibility, it is necessary to develop an **EU framework to ensure an equal and transparent level playing field**.
- The **Harmonised Electricity Market Role Model** should include common terminology for demand-side flexibility, and develop roles and responsibilities for all relevant roles. In addition, a **market monitoring** system to provide a view on how much flexibility is active in the market needs to be developed.
- With respect to technical solutions and platforms to fulfil system and grid needs, **observability in low voltage grids** should be increased and **load and generation forecasting** at distribution level need to be improved. In addition, it is important to address large scale simultaneous behaviour of demand response technologies.
- In relation to data security, EU safety, security and liability policies and regulations should be updated to address the new risks. In addition, to address the new complexities that flexible electricity services will bring, **regulators across sectors should collaborate** more.

We specify our detailed opinion on the EG3 recommendations in Annex III.

In terms of procedural next steps, Orgalim calls for an inclusive and transparent process for the development of the network codes foreseeing continuous stakeholder involvement, including European technology providers, as established by the Electricity Regulation.

***

Annex I: EG 1 Report - Towards Interoperability within the EU for Electricity and Gas Data Access & Exchange

Annex II: EG2 Report Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management

Annex III: EG3 Report on Demand Side Flexibility - Perceived barriers and proposed recommendations

ANNEX I:

EG 1 Report - Towards Interoperability within the EU for Electricity and Gas Data Access & Exchange

RECOMMENDATIONS for follow-up work towards convergence of national practices and the potential achievement of full interoperability at European level

Recommendation	High importance and highly urgent	Important and urgent	Less important and less urgent	Not a priority
0) On the way to interoperability of national practices for accessing and exchanging data, all relevant stakeholders must get involved, discuss and negotiate.	x			
1) Building on available role models, adopt and use a common European role model.	x			
2) To facilitate interoperability, adopt and use a common information model for semantics, for example consider building on the available IEC CIM model.	x			
3) Adopt and use a core process model, which should allow for national specificities and stay open for further interoperability over time.		x		
4) Business requirements shall be the basis for interoperability and must remain technology-neutral.	x			
5) Adopt and use available European standards as a basis to improve interoperability.	x			
6) Monitor the gap between each national practice and the reference core model. Consider means for maintaining this at European level.				x
7) Specify information exchange in terms of exchange between harmonised roles.				x
8) Bear in mind that legal aspects in national markets can be a limiting factor to full interoperability.				x
9) Aiming for interoperability should not be conditional to a cost/benefit analysis. However, how to reach it and maintain it (in terms of context and timing) could be analysed and optimised through Cost/Benefit Analyses and Risks/Opportunities Assessments.		x		
10) Bear in mind that reaching and maintaining interoperability is a step-by-step exercise requiring a roadmap that needs to be duly monitored and accordingly adapted.	x			

PROCESS-SPECIFIC RECOMMENDATIONS – a non-exhaustive list based of the findings of this investigation; their description can be found in the related processes' sections in this report along with some proposals for role models and Business Use Cases.

On Emerging Services

Recommendation	High importance and highly urgent	Important and urgent	Less important and less urgent	Not a priority
11) New emerging business use cases related to emerging services should be described using the methodology followed in the report. Four business use cases have already been described and are available in the accompanying document as a basis for implementation: "download my data", "share my data", "revoke consent" and "terminate service".	x			
12) Existing role models should be extended to take into account new roles and the diversity of implementations enabling new services.	x			
13) If an external service is cancelled, the Consent Registry responsible needs to be informed to handle future activities. Service termination must propagate termination of consent previously given by the consumer.	x			
14) If a consent is revoked by the consumer, all concerned service providers and third parties must be informed immediately to handle future activities.	x			

On Billing – referring to data exchanged between actors in the energy sector and not the end bill

Recommendation	High importance and highly urgent	Important and urgent	Less important and less urgent	Not a priority
15) As billing is closely related to the legal aspects of the national markets, convergence - to the extent possible - of legal aspects is important for furthering interoperability.		x		
16) The reference model should encompass different models for billing taking into account significant national characteristics.		x		
17) Building billing interoperability should not restrain an organisation's competitive communication possibilities nor undermine the dynamic innovative trends (digitalisation / new service developments).		x		

ANNEX II:

EG2 Report Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management

RECOMMENDATIONS on **Conformity to ISO/IEC 27001:2013** and **Minimum Security Requirements**

Area	Requirements	Owner	High importance and highly urgent	Imp. and urgent	Less imp. and less urgent	Not a priority
ISO/IEC 27001	Conformity to ISO/IEC 27001:2013 and any subsequent version applicable at the national level.	Operator	x			
Scope	System Operation Critical includes assets, which are directly related to the availability and reliability of power generation and distribution infrastructure. It defines the productive environment of an energy system operator, i.e. the Operational Technology (OT) domain.	Operator	x			
Risk Management	Record known incidents, attacks and vulnerabilities.	Operator		x		
Risk Management	Known basic risks for cyber incidents and attacks should be record.	ENTSO-E and EU-DSO	x			
Risk Management	Regular update on major threats and risks relevant for transmission and distribution operators	ENISA	x			

Risk Management	ENTSO-E and EU-DSO to provide a risk-impact matrix as a template for operators.	ENTSO-E and EU-DSO	x			
Asset Management	ACER to align the approach on categorisation of assets with the respective regulators, ENTSO-E and EU-DSO in order to derive a proper approach on asset management.	ACER	x			
Asset Management	Categorise assets and to have an infrastructure network plan available.	Operator		x		
Certified Components	Operators to use products, processes and services conform to EU cybersecurity certification schemes as soon as respective schemes and components are available from at least two suppliers or service providers.	Operator		x		
Migration of legacy	Use of an infrastructure network plan to classify systems according to a risk-impact matrix in order to derive a migration plan depending on an agreed level of CapEx and OpEx.	Operator		x		
Migration of legacy	Agee with respective stakeholders on the level that should be used for CapEx and OpEx with the objective to migrate	NRA		x		

	existing infrastructure towards a baseline protection.					
Categorisation	Split into domains of OT products, OT systems and IT Services.	ENTSO-E and EU-DSO	x			
Methodology	Methodology based on ISO/IEC 27005:2018 with additional requirements: • Identify and evaluate existing countermeasures • Re-evaluate likelihood and impact • Determine residual risks • Compare residual risks with tolerable risks • Identify additional cybersecurity measures.	ENTSO-E and EU-DSO	x			
Methodology - Context establishment	Context establishment shall cover: - System outline - Categorisation of products, systems and services - Risk-impact matrix - Target protection level; EU reference architecture should consider architectures available in international standards. ENTSO-E and EU-DSO should align on respective architecture.	ENTSO-E and EU-DSO		x		
Methodology - Risk Assessment	Known basic risks for cyber incidents and attacks should be recorded.	ENTSO-E and EU-DSO	x			

Methodology - Risk Assessment	Regular update on major threats and risks relevant for transmission and distribution operator.	ENISA		x		
Methodology - Risk Treatment	Set-up of expert group with relevant stakeholders and final review with respective associations.	ENTSO-E and EU-DSO	x			
Methodology - Risk Treatment	Use of international standards: OT products: IEC 62443-4-1/-4-2 OT systems: IEC 62443-2-4/-3-3 IT Services: Domain specific; advice by ENISA should be considered.	ENTSO-E and EU-DSO	x			
Methodology - Risk Treatment	Residual risks are to be documented.	ENTSO-E and EU-DSO		x		
Methodology - Risk Acceptance	An alignment on classification, minimum security requirements and residual risks.	ENTSO-E and EU-DSO		x		
Methodology - Regular Review	A regular review (at least every five years) to consider changes in technology, threats and risks.	ENTSO-E and EU-DSO		x		
Application of Certification Scheme	SGTF EG2 recommends ENTSO-E and EU–DSO to discuss with the European Cybersecurity Certification Group (ECCG) as to where a certification scheme should be applied and where minimum security requirements without certification are sufficient.	ENTSO-E and EU-DSO	x			

Certification Scheme	Use of profile (mapping of objectives to requirements from standard) as provided by SGTF EG2. ENISA to facilitate the update of profiles in case of new standard releases or updates in regulation.	ENISA	x			
Security Requirements	Use of the profile for security requirements defined independent from the EU Cybersecurity Act approach to meet the same objectives as defined in the EU Cybersecurity Act.	ENTSO-E and EU-DSO	x			
Certification Scheme	Use of IECEE for respective profile for OT products and OT systems including OT services	ENISA	x			
Certification Scheme	ISO/IEC 27001:2013 instead of IEC 62443-2-1/-2-2 within the used parts of IEC 62443, i.e. IEC62443-4-1/-4-2 and IEC 62443-2-4/-3-3.	ENTSO-E and EU-DSO and ENISA		x		
Certification Scheme	Request International and European Standardisation Organisation to review and further develop IEC 62443 into the direction of a horizontal standard by including the flexibility to base relevant parts of IEC 62443 directly on ISO/IEC 27001.	European Commission		x		

Certification Scheme	Assessment criteria to be provided by standardisation groups.	European Commission	x			
Certification Scheme	Analysis of the need for additional sector-specific assessment criteria. In such cases, ENTSO-E and EU-DSO should develop such criteria in alignment with industry stakeholders, ENISA and the standardisation bodies.	ENTSO-E and EU-DSO		x		
Certification Scheme	Use of Annex II of 768/2008/EC for Conformity Assessment Procedures which should be based on ISO/IEC27001:2013 instead of ISO 9001:2015.	ENISA	x			
Certification Scheme	SGTF EG2 proposes to support safeguarding existing national certification implementations for smart meters. A possible harmonisation towards a European approach in regards of smart metering as outlined in this report should anyway take into consideration already established national certification schemes for smart meters.	ENTSO-E and EU-DSO		x		

RECOMMENDATIONS on **Advanced cybersecurity for operators of essential services**

Area	Requirements	Owner	High imp. and highly urgent	Imp. and urgent	Less imp. and less urgent	Not a priority
Risk Assessment	Operators of essential services are recommended to use a risk-based approach by performing cybersecurity risk assessments on their current infrastructure.	Operator	x			
Baseline Security for OES	Operators of essential services follow the obligation as defined in chapter 7 for all operators, with the adjustment that the risk management is based on the current infrastructure and that operators of essential services have the choice to deviate from the usage of products, systems and services that are conform to EU cybersecurity certification schemes that are available in case they can provide evidence that the achieved target protection level is equal or higher than the one defined with the approach defined in chapter 7.2 for minimum security requirements.	Operator	x			
Baseline Security for non-OES	National regulatory authorities (NRA) might consider providing a choice for energy system operators who are not identified as operators of essential services, to follow the risk-based approach.	NCA	x			
Risk Management	SGTF EG2 recommends to follow ISO/IEC 27001:2013 for the supply chain cybersecurity risk management by analysing general risks as described in the standard ISO/IEC 27036-1:2014 chapter 5.3 and by performing a regular review of controls and practices of ISO/IEC 27002:2013 and ISO/IEC 27019:2017. The review on controls and practices should be documented with lists gaps and risks identified and respective mitigation measures.	Operator	x			

Risk Management	SGTF EG2 recommends to limit the risk management to suppliers of products, systems and services that are highly critical for the security of the supply of energy.	Operator	x			
Methodology	Cross-border and cross-organisational cybersecurity risk management to be based on the methodology on the international standards: ISO/IEC 27005:2018 and ISO 55001:2014.	ENTSO-E and EU-DSO	x			
Methodology	Address cyber scenarios that could cause scale 2 or scale 3 emergency situations listed in the ENTSO-E "Incident Classification Scale".	ENTSO-E and EU-DSO	x			
Risk Treatment	Follow the ISO/IEC 27001:2013 principle that each organisation (OES) has to decide on implementation and risk acceptance of residual risks. Consequently, SGTF EG2 recommends that operators of essential services document all risk acceptance with appropriate reasoning.	Operator		x		
Set-Up	Establish a cyber security risk management advisory group for the electricity subsector with the express purpose of identifying and managing common cross-border and cross-organisational Tier 2 and Tier 3 cybersecurity risks.	ENTSO-E and EU-DSO	x			
Methodology	A risk identification and risk evaluation model similar to a functional and logical mapping into the Smart Grid Architecture Model (SGAM) should be specifically defined, harmonised, validated and maintained.	ENTSO-E and EU-DSO		x		
Methodology	A risk impact matrix similar to the NTA8120 risk-impact matrix should be defined, harmonised, validated and maintained.	ENTSO-E and EU-DSO	x			
Methodology	The established cyber security risk management advisory group should identify requirements for key security controls and	ENTSO-E and EU-DSO	x			

	recommended best-practice solutions.					
General	Technology neutrality to be considered as a priority for the Network Code on cybersecurity.	European Commission	x			
Set-Up	ENTSO-E and EU-DSO to initiate the discussion on an early warning system and information sharing in the EU and Member States with ENISA to facilitate a discussion with the Member States in the NIS Cooperation Group on how to best set-up such an early warning system.	ENTSO-E and EU-DSO, ENISA	x			
Code of Conduct	Member States to agree on a Code of Conduct for an early warning system.	ENISA		x		
Participation of non-OES	Offer operators that are not identified as OES the possibility to voluntarily participate in the early warning system.	European Commission		x		
Platform	Use MISP as a platform for the early warning system.	European Commission	x			

RECOMMENDATIONS on **Supportive elements**

Area	**Requirements**	**Owner**	**High imp. and highly urgent**	**Imp. and urgent**	**Less imp. and less urgent**	**Not a priority**
Implementation Guidance	Energy domain-specific guidance for crisis-management of energy system operators should be available without being restrictive for the implementation in order to reflect individual operational needs.	European Commission, ENISA, ENTSO-E and EU-DSO	x			
Guidance on Policies and Agreements	ENTSO-E &EU-DSO to provide guidance on security policies and agreements for suppliers on common security practices. SGTF EG2 recommends to align the guidance with relevant stakeholders.	ENTSO-E and EU-DSO	x			
Guidance on Procurement Requirements	ENTSO-E and EU-DSO to provide guidance on procurement requirements. SGTF EG2 recommends to align the guidance with	ENTSO-E and EU-DSO	x			

	relevant stakeholders representing manufacturers. Furthermore, SGTF EG2 recommends to base this effort on the widely recognized OE-BDEW white paper while to improve the structure by adding a clear separation of roles such as operator, service provider, integrator and manufacturer. Furthermore, minimum security requirements should be considered in such guidance as an option where it might simplify procurement requirements if available.					
Maturity Framework	ENISA to facilitate a mapping of ES-C2M2 to controls of ISO/IEC 27001:2013, ISO/IEC 27002:2013 and ISO/IEC 27019:2017 in order to create an EU cybersecurity maturity model for the electricity subsector that can be further developed independent to ES-C2M2. ENISA might discuss with ENTSO-E and EU-DSO on the value to provide an extended maturity that includes controls not already covered in the existing maturity framework.	ENISA		x		
Maturity Framework	SGTF EG2 recommends operators who intend to use a maturity framework to follow the Plan-Do-Check-Act (PDCA) methodology of ISO 9001:2015 in order to ensure continuous improvement.	Operator		x		

ANNEX III:

EG3 Report on Demand Side Flexibility:

Perceived barriers and proposed recommendations

RECOMMENDATIONS

ID	Recommendation	High importance and highly urgent	Important and urgent	Less important and less urgent	Not a priority
3-2A	Periodically analyse use cases that draw out consumer behaviour requirements, in consultation with the relevant stakeholder groups (see also section 10.3.1).	x (to be done after DSF take-off			
3-2B	Stakeholders should coordinate to create greater awareness of, and trust in, the opportunities of Demand Side Flexibility and the services that customers can participate in.		x		
3-2C	As offers evolve, Member States could consider how to include new offers (new products or new providers) in price comparison tools if this is not available.			x	
3-2D	Member States should monitor developments in consumer offerings, consider the need for changes to consumer protection rules, and empower relevant bodies to take action if required.	x (after DSF take-off)			
3-4	NRAs could ensure that TSO and DSO revenue regulation and network tariffs structures take into account costs and benefits of flexibility for the system, and that they are non-discriminatory.	x			
4-1A	There is a need for standardisation or at least interoperability of hardware (EMS, smart meters, charging stations etc.).	x (should apply only to the new generation of products)			
4-1B	There is a need for harmonisation of market rules and energy products (details in chapter 5).	x			
4-2A	A comprehensive aggregator framework should be implemented, following the CEP and EBGL, and further developing topics like allocation of energy volumes should be addressed.	x			
4-2B	Develop a classification of Transfer of Energy models and a compilation of best		x		

	practices for the ToE, including different compensation/remuneration and perimeter correction mechanisms.				
4-3	Study the integration of Implicit and Explicit DR.		x		
4-4	Define a data access & data sharing framework, including the list of topics in 4.3.4.	x			
5-1	Products should be designed in a dialogue with stakeholders to assess possibilities and needs, at least at national level. Special attention should be given to avoiding too numerous and diverse products, while considering local specificities.				x (market will select suitable products)
5-2A	Locational information in flexibility products should be mandatory for congestion management products, with minimum granularity to the extent necessary.	x			
5-2B	Define the data requirements that flexibility service providers must deliver to the relevant SO or responsible market operator. Study how more locational information could be provided in aggregated flexibility products.	x			
5-3A	The pre-qualification process should be user-friendly, striving to minimise the different steps and standardise them when possible. Proportionality of the process regarding the product type and requirements should be ensured. Transparency of limits applied to bids and their justification should be ensured.	x			
5-3B	Study possible alignment of prequalification process per product, and feasibility of the prequalification process at aggregated level.		x		
5-4	Analyse the need for availability contracts, and their impact on the market liquidity.		x		
5-5	The assets delivering flexibility products should be connected to a smart (sub)meter/gateway to collect data. Telemetry requirements should be established according to capacity thresholds. Other equivalent solutions (where possible) should be implemented for smaller units or aggregators.		x		
6-1	An EU framework shall be developed to ensure an equal and transparent level playing field for all service providers.	x			

6-2	An integrated system approach should be a shared vision. Market processes should have sufficient coordination functions between them for economic efficiency and SoS.	x			
6-3	The appropriate model for the coordination of market processes should be chosen and made transparent. TSOs and DSOs, in coordination with all market actors, should strive for efficient coordination, especially in designing, buying and settling flexibility products.	x			
7-1	The Harmonised Electricity Market Role Model should evolve to include common terminology for DSR, develop roles & responsibilities model for all relevant roles with respect to contracting and activating DSF, especially the Aggregator role. This includes a process model and an information exchange model.	x			
7-2	Share and develop best practices for value stacking.		x		
7-3	Share and develop best practices for sub-metering.			x	
7-4A	Develop a categorisation of best practices for baseline design, and methodology development for selecting and validating baseline methodologies for specific products.	x			
7-4B	Develop market monitoring, at national level or potentially at EU level, to provide a view on how much flexibility is active in the market, and to monitor and prevent strategic behaviour and gaming by market players.	x			
8-1	Increase LV observability with smart meter data.		x		
8-2	Include the digitalisation perspective on achieving DSF.	x			
8-3	Create a smart meter roadmap > 2020.		x		
8-4	Improve forecasting at distribution level.	x			
8-5	Address large scale simultaneous behaviour of DR technologies.	x			
8-6	Develop other options for mitigating grid constraints.	x			
9-1	Further studies should be done to consider and clarify what (and how) information should be made transparent in the energy sector. It may be useful to map categories of energy-related data against how it interacts with data privacy regulations.		x		

9-2	Following above mentioned, a more detailed MS specific study to identify data needs and accessibility is needed (see also 4.2).		x		
9-3	EU safety, security and liability policies and regulations should be reviewed and updated as necessary to address new risks arising from the use of digital technologies in the energy sector.	x			
9-4	Regulators across sectors should collaborate more and consider relevant updates to license conditions in order to address the new complexities that flexible electricity services will bring.	x			
10-1	To improve knowledge sharing through periodic analysis of research projects and proactive feedback.		x		

For further information, please contact:
Sigrid Linher, Director Energy, Climate and Environment: firstname.lastname@orgalim.eu
Toma Mikalauskaité, Adviser: firstname.lastname@orgalim.eu