

Article 13 a implementation: Context and State of Play



Art.13 a: context and scope

- ★ First EU initiative to legally impose security obligations on providers of communication network and services
 - ★ Mandates MS/NRAs to “ensure” that providers implement proper technical and organisational security measures
 - ★ Imposes on MS a national incident reporting scheme
 - ★ Harmonised implementation of article 13 across EU is required

- ★ Calls for ENISA to
 - ★ Facilitate the implementation process among MS and providers
 - ★ Propose, if asked, appropriate technical implementing measures
 - ★ Collect and analyse on annual basis aggregated and anonymised incident reports
 - ★ Be informed on major, cross-country incidents

General Objectives of ENISA

- ★ establish **minimum common denominators** in all MSs to be used as baseline for harmonising the measures referred to in paragraphs 1, 2, and 3

- ★ provide support to Member States in the implementation of
 - ★ par.1 and 2 of article 13 a, and
 - ★ par. 3 of article 13 a

- Define the annual reporting scheme to ENISA and the objectives of the consolidated report

What ENISA is doing?

- ★ Involving all the 27 MSs in a open discussion about Art 13a implementation and facilitating **information sharing**
- ★ Identifying **minimum common denominators** in all MSs to be used as baseline for harmonising the measures referred to in paragraphs 1, 2, and 3
- ★ Planning for **minimum security measures guidelines** for NRAs (with the support of MSs and providers)
- ★ Planning the establishment of a **reporting scheme to ENISA** to collect annual incident reports from MSs

Where are we now?

- ★ 25 MSs actively involved in the common effort for an harmonized implementation of Art 13a:
 - ★ several discussion 1 to 1 between ENISA and MSs
 - ★ Regular phone conferences
 - ★ 4 workshops (Madrid, Stockholm, Vienna and Rotterdam)

- ★ Identified minimum common denominators for:
 - ★ Definitions
 - ★ Scope and context of Art.13 a
 - ★ Reporting parameters and thresholds

- ★ Minimum security measures guidelines for NRAs:
 - ★ Stock taking on existing good practises and standards in MSs launched in the beginning of Dec.2010
 - ★ Providers now gradually involved in discussions

- ★ Reporting scheme to ENISA:
 - ★ Starting simulation with data provided from some MSs

Collected Data: which use?

- ★ Inform Member States and European Union relevant Institutions on:
 - ★ number of security incidents with a significant impact at European level
 - ★ incidents root causes, including the most frequently detected threats and vulnerabilities
 - ★ lessons learned (detection, response and recovery phases)
- ★ Support the knowledge transfer between Member States
- ★ Understand the impact on interdependent critical assets at supra-national level (including the understanding of the impact of weakest link failures).
- ★ Pan European Exercises: develop possible incident scenarios
- ★ Issue recommendations to relevant policy makers of Member States and private sector
- ★ Understand the threat environment (correlate the information with data sources and through information sharing with experts)
- ★ Analyze the suitability of relevant good practices in use
- ★ Understand possible future trends

Minimum security measures guideline for NRAs

- ★ ENISA proposes to prepare a minimum security measures guidelines for national regulatory authorities (NRAs).
- ★ Such a guideline is meant to address and support the implementation of paragraphs 1 and 2 of Art.13 a.
- ★ The minimum security measures guidelines are **not** meant to become a binding measure for MSs, but we cannot exclude a priori that in the future, and if necessary, the EC will impose them as a mandatory minimum standards.
- ★ All the MSs consulted so far, expressed a favourable opinion in the proposal
- ★ All the MSs are aware that it would be a very difficult to achieve a good result and that service communication provider will play a key role in this project.

Why minimum security measures?

- ★ Ally the varying levels of security and resilience of the market operators with a consistent minimum national framework
- ★ Provide a minimum guaranteed level of security and resilience in all MSs, avoiding the creation of weakest links
- ★ Ensure a minimum level of harmonization on security and resilience requirements across Member States and thus reducing compliance and operational costs of multinational operators
- ★ Set the basis for a minimum auditable framework of controls across Europe
- ★ Facilitate the establishment of common preparedness, recovery and response measures and pave the way for mutual aid assistance across operators during crisis
- ★ Achieve an adequate level of transparency in the internal market

Methodology- Approach of ENISA

- ★ Stock taking of:
 - ★ existing minimum security and resilience requirements at national level in Europe and elsewhere
 - ★ good practices in use by operators
 - ★ survey involving experts from NRAs and operators on relevant topics
- ★ Constitution of a working group with representatives from NRAs and Private sector
- ★ Analysis of the findings from the stock taking and the survey
- ★ Definition of the framework's domains, sub-domains & controls
- ★ Dissemination of the minimum security and resilience measures

- ★ A project Steering Committee will provide guidance, and validate all the steps.
- ★ A working group will provide support

Next Steps: minimum security measures guideline for NRAs

- ★ Increase the number of the MSs involved in the process – aiming at 100%
- ★ Facilitate the dialogue and information sharing among MS on open issues
- ★ Enlarge the consensus base
- ★ Provide, upon request, targeted informal implementation guidance
- ★ Develop knowledge, expertise and good practices on
 - ★ Annual reporting scheme to ENISA
 - ★ Minimum security requirements/measures

Contact

Resilience Team - resilience@enisa.europa.eu

European Network and Information Security Agency
Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

www.enisa.europa.eu