

Reporting of the security breaches under the EU law

*Outage requirements - FCC workshop
8 September 2011
Presentation by
the European Commission DG INFSO and ENISA*



Legal aspects

European Union context

- *The 2009 Telecoms Reform introduced the security breaches reporting obligation at the European level*
- *Before, only 2 out of 27 Member States had a reporting mechanism concerning security breaches (Finland, Sweden)*
 - > *Amendment of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services: new chapter on security and integrity of networks and services*
 - > *Amendment of 'ePrivacy' Directive: new obligation to report personal data breaches*



Legal aspects

Reporting - Legal basis

Art. 13a(3):

*“Member States shall ensure that **undertakings providing public communications networks or publicly available electronic communications services** notify the **competent national regulatory authority** of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.*

*Where appropriate, the **national regulatory authority concerned** shall inform **the national regulatory authorities in other Member States** and the **European Network and Information Security Agency (ENISA)**. The **national regulatory authority concerned** may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.*

*Once a year, **the national regulatory authority concerned** shall submit a summary report to the **Commission and ENISA** on the notifications Received and the action taken in accordance with this paragraph.”*



Legal aspects

Risk management context

Art. 13a (1)and(2):

“1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.”



Reporting obligations under Art. 13a

Three types of reporting:

1. From *undertakings* to the *competent national regulatory authority (NRA)*
2. From the *NRA concerned*, where appropriate, to the *NRA*s in other Member States and to the European Network and Information Security Agency (*ENISA*).

The *NRA concerned* may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest

3. From the *NRA concerned* to the *Commission* and *ENISA*.

Annual summary report about the notifications received and the actions taken (First one due in Q1 2012)



Implementation process of the Directive/ State of play

- *25 May 2011 - **transposition date** of the Telecom Package, incl. Art. 13a*
 - > *Member States have to adopt necessary national measures*
 - > *The **Commission** may adopt technical implementing measures with a view to harmonising the national measures concerning Art. 13a*
- **State of Play**
 - > *bottom up approach: MSs and ENISA are working together on **Technical Guidelines** to boost the harmonised implementation process*
 - > *The **Commission** will base the technical implementing measures on the common baseline and the **Technical Guidelines** elaborated by ENISA and the MSs*



Technical aspects of reporting security breaches under Technical Guidelines



Technical aspects

Content of Reporting Scheme under Technical Guidelines

- *Annual, aggregated and anonymous report of all reported security breaches (without the name of the provider involved)*
- *Fields for describing the breaches*
 - *Date of occurrence*
 - *Date of detection*
 - *Affected asset(s) and services*
 - *Information on the root cause including threats vector(s) and vulnerabilities exploited*
 - *Impact*
 - *Breach handling and response approach*
 - *Measures taken to avoid similar breaches*



Networks and/or services affected by the security breaches

Non-exhaustive list of assets and services affected

*Telephony/ Voice
Fixed Network*

Data Services

Satellite Communication Fixed Network

Wireless broadcast Services



Technical aspects
Parameters Set

Amount of Users Affected

Duration of the Breach

Geographic Spread/ Region

Impact on Emergency Services



Technical aspects

Thresholds

under Technical Guidelines

- *Thresholds are a minimum entry level*
- *NRAs can impose more strict and granular thresholds to trigger the reporting at national level.*
- *The following thresholds are proposed (the red area covers breaches reported to ENISA):*

	1h<...<2h	2h<...<4h	4h<...<6h	6h<...<8h	>8h
1%<...< 2% of users					
2% < ...< 5% of users					
5% <...< 10% of users					
10% <...<15% of users					
> 15% of users					



The objectives of collecting data on security breaches

- *Better access and dissemination of information among the interested parties*
- *Provide information and data relevant to the risk management activity*
- *Learning process for policy makers and providers*



THE END

Contacts:

European Commission: Joanna.Borzecka@ec.europa.eu

ENISA: Lionel.Dupre@enisa.europa.eu

web sites:

http://ec.europa.eu/dgs/information_society/index_en.htm

<http://www.enisa.europa.eu/>

