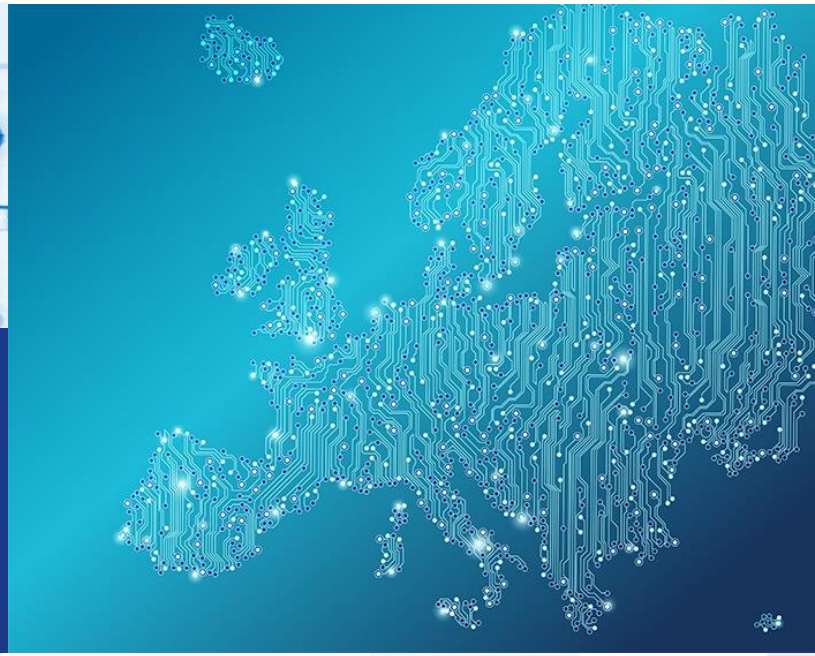


Cyber Security in the EU: the legal framework

Udo Helmbrecht | Executive Director

14 March 2016

European Union Agency for Network and Information Security

Agenda

Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union (NISD) COM(2013) 48 final, 7/02/2013

Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

Directive 2009/140/EC, article 13a on Security and integrity

Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR) COM(2012) 11 final, 25/01/12

Network and Information Security Directive

First EU cyber security initiative

The NIS Directive

enisa

Strategic
Cooperation network

NCSS

cloud computing services

DSPs

ESPs

transport

Online market places

Incident Reporting

Security requirements

energy

Search engines

banking

Tactical /Operational
CSIRT network

NIS directive

Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level)

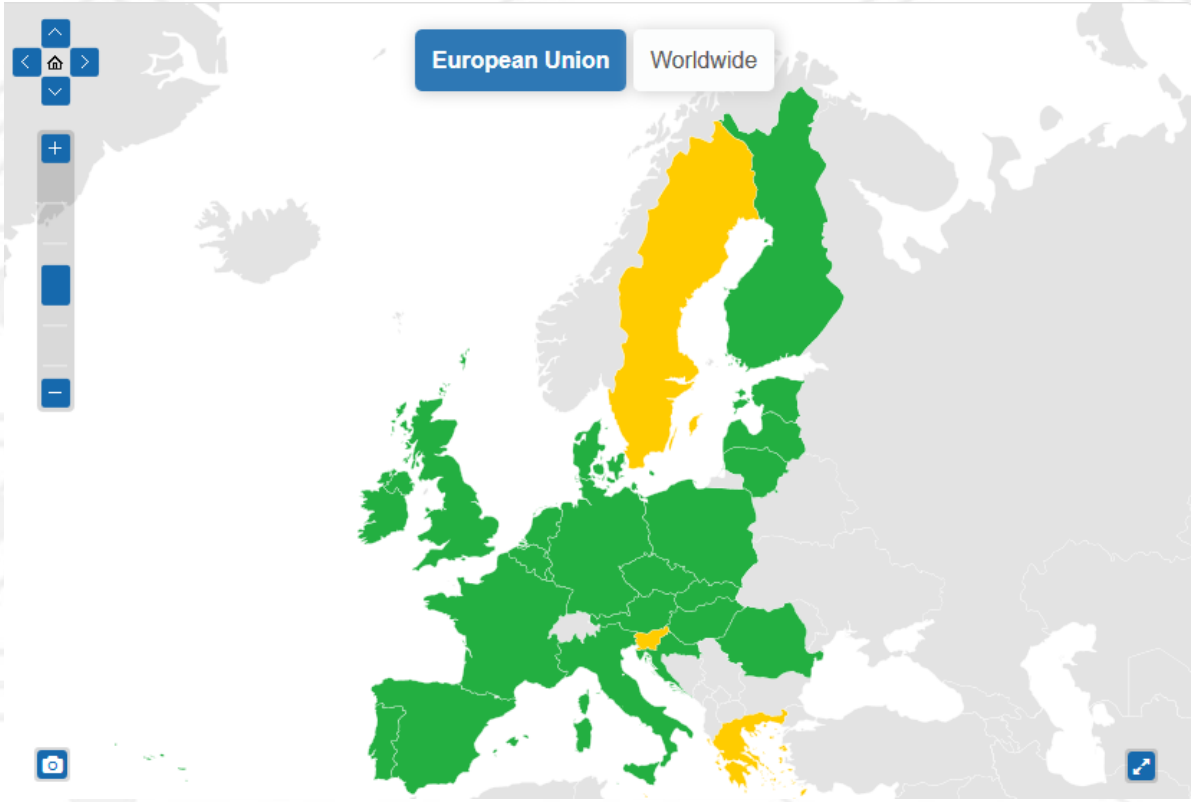
Current stage of promulgation: EU Parliament and EU Council reached an agreement, possible adoption April 2016

Provisions:

- Obligation for MS to adopt national NIS strategies and designate national authorities
- Creates first EU cooperation group on NIS, from all MS
- Creates an EU national CSIRTs network
- Establishes security and notification requirements for operators of essential services (ESP) and digital service providers (DSP)

ENISA's role in NIS strategies

- Work already done in this area, aims at rendering further support as need be to improve NIS strategies



National CSIRTs

- **Article 7** of the Directive gives the framework for CSIRTs
- **Article 8b** of the Directive covers the CSIRT Network
- **Annex 1**. Requirements and tasks of the CSIRT. This Annex gives a list of tasks that a MS' CSIRT has to perform
- **Annex 2**. Sectors and entities. This Annex lists the sectors and subsectors that need to be covered by each country's Information Security Strategy and CSIRTs

NB: (For ease of reading we refer to national CSIRTs in this presentation simply as "CSIRT" or "dedicated CSIRT")

eIDAS Article 19

The role of ENISA in Art. 19 of eIDAS

Art. 19 expert group:

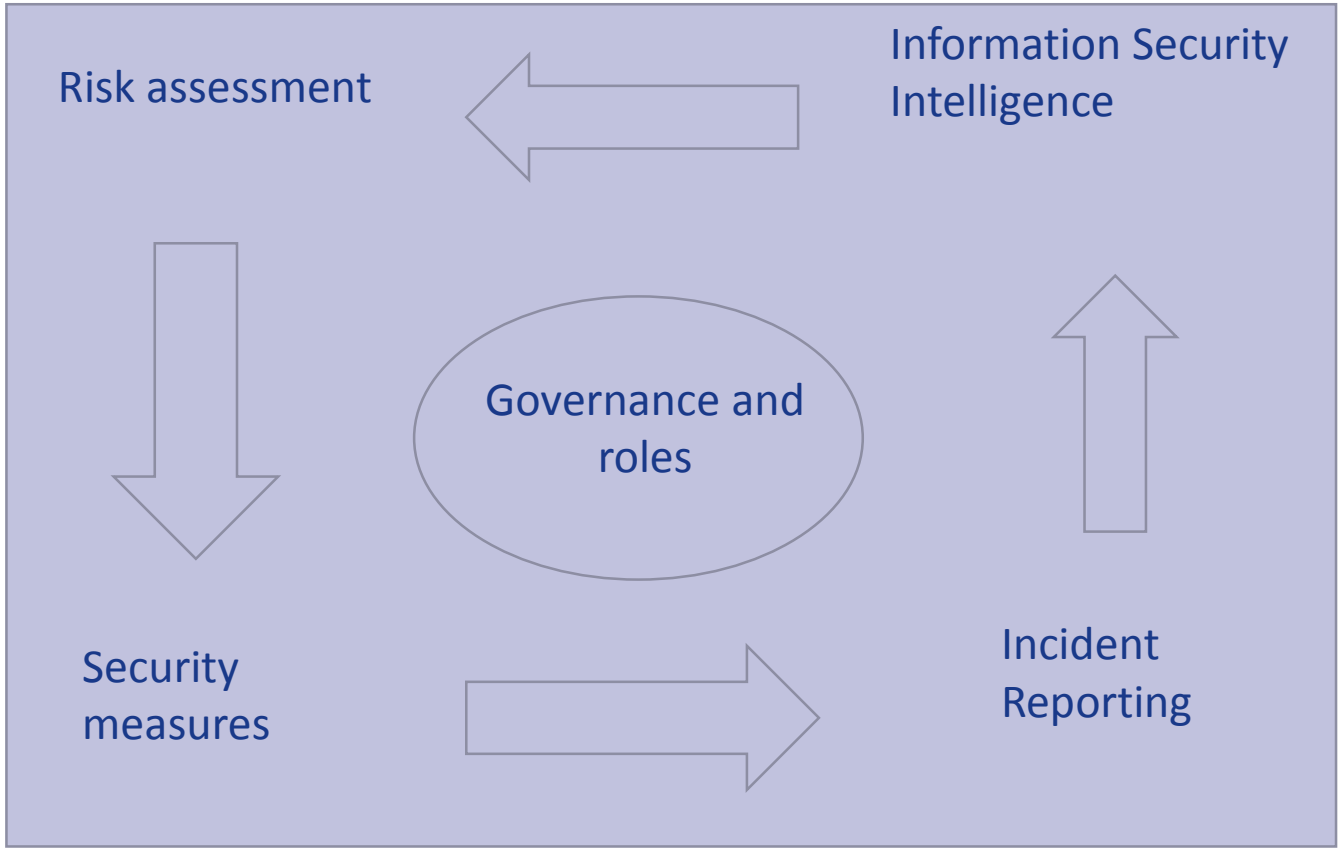
- Composed of public authorities
- Scope is Article 19 – eTrust services providers
- Group is run by ENISA, that will liaise with relevant industry groups
- EC supports this group and will liaise with other/existing groups or legislation (such as NIS directive).
- Simple, streamlined, harmonized, fitting existing national structures/authorities

Goal is to develop non-binding technical guidelines for SB on article 19 (to support their work).

Working with experts from these bodies.

Most of the MSs have not nominated their SB.

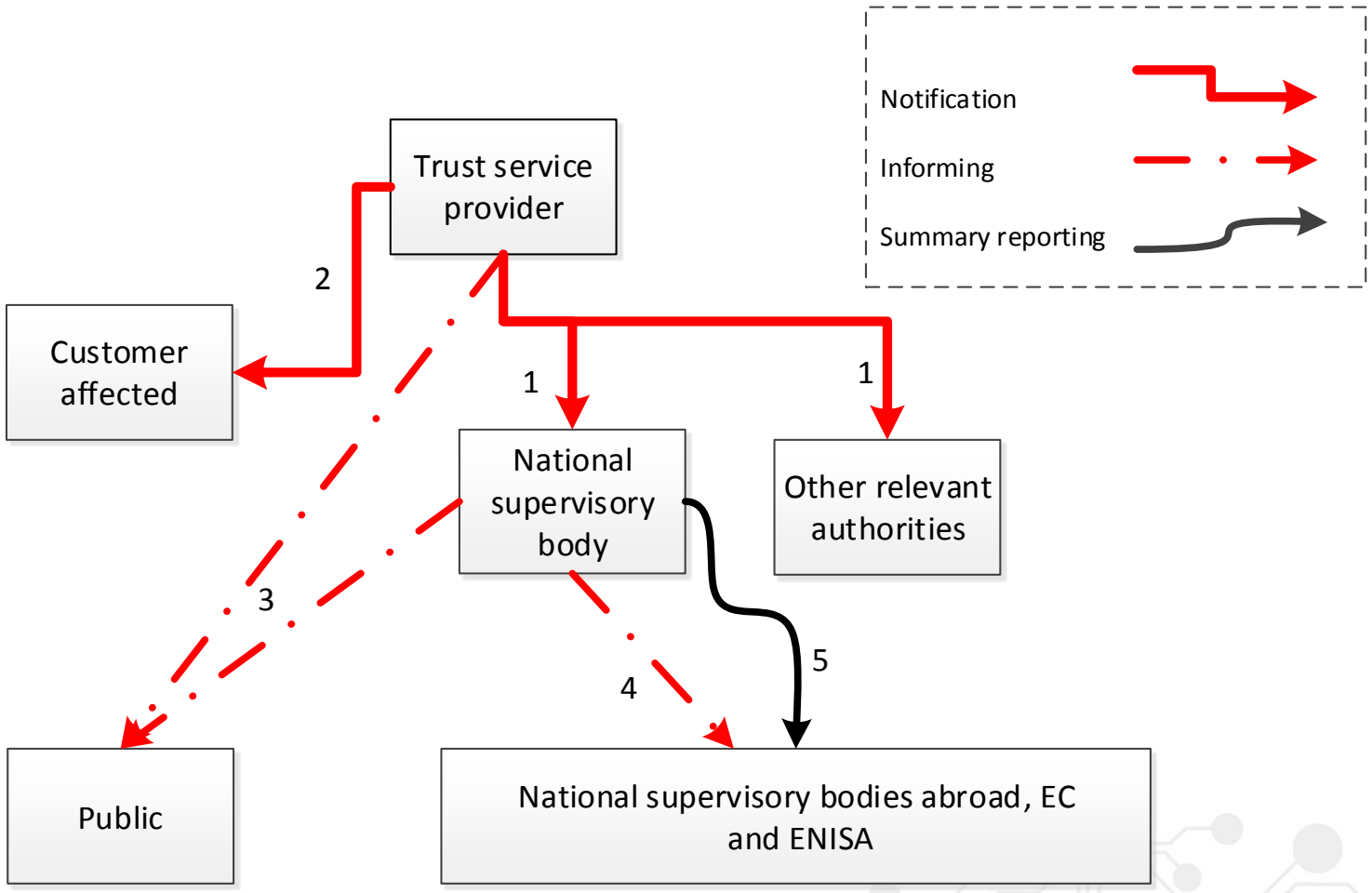
The importance of incident reporting



Supervised by a supervisory body

in collaboration with supervisory bodies abroad (single market)

Overview of reporting flow in Article 19



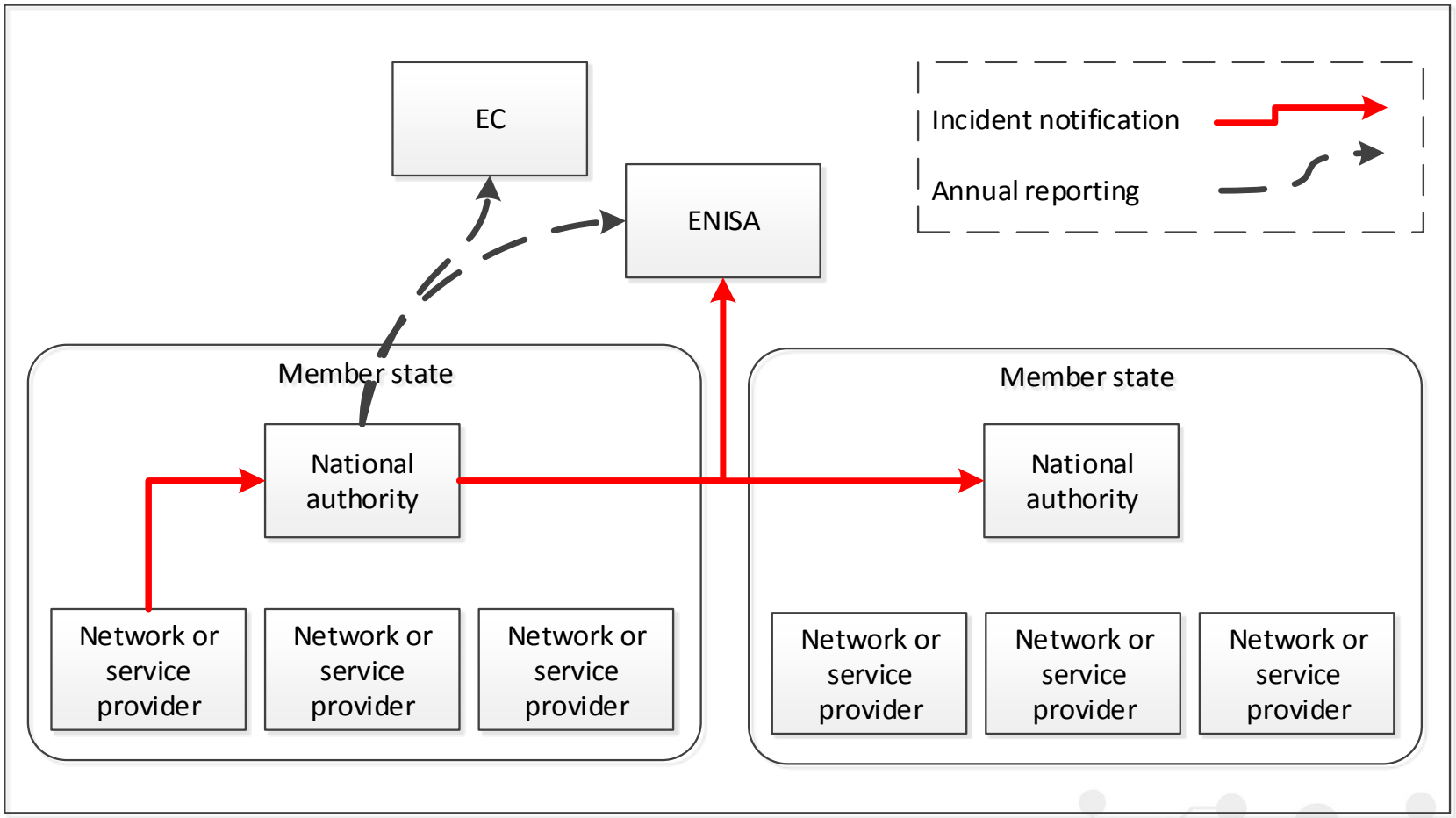
Article 13a

Mandatory incident reporting for the telecom sector

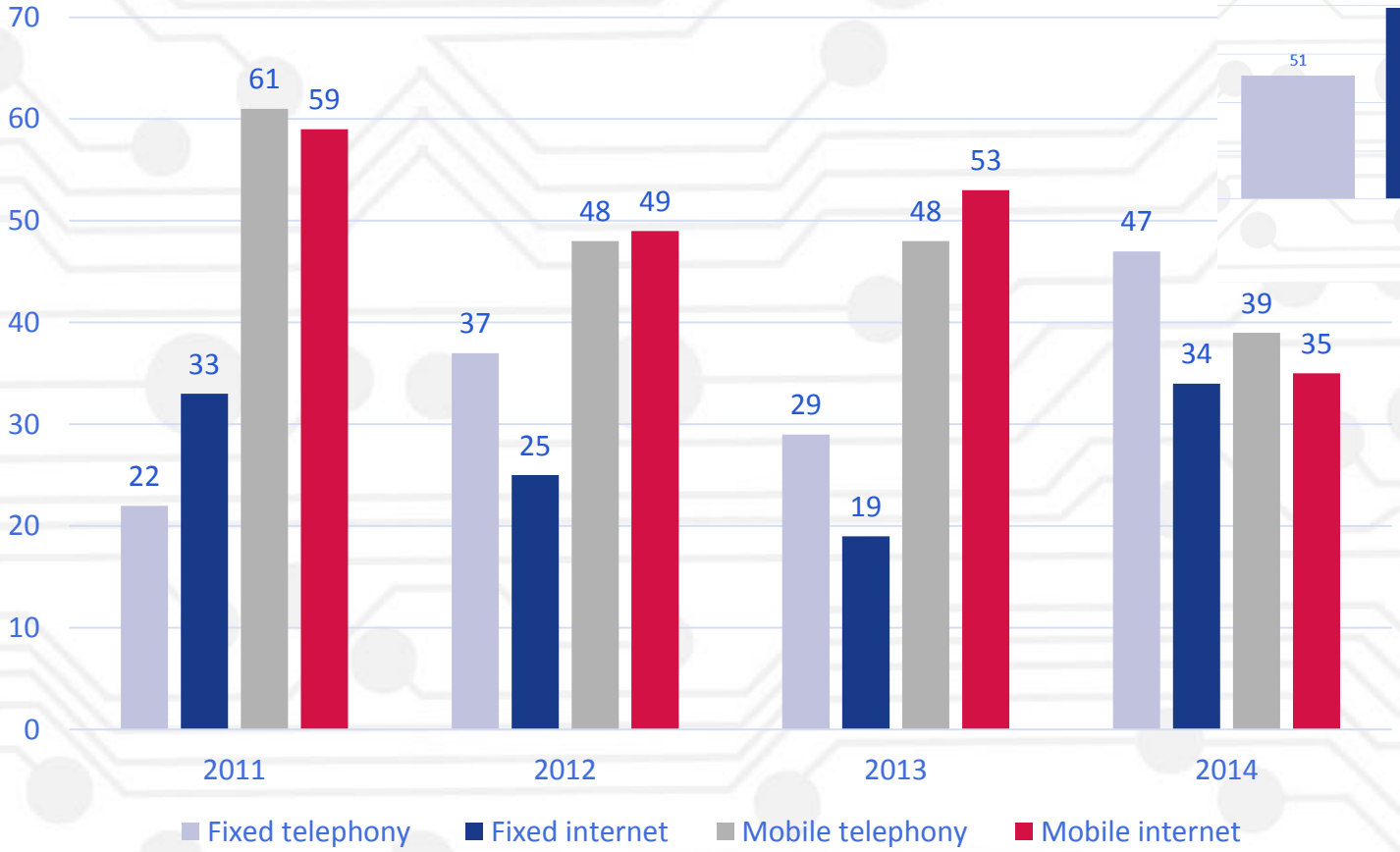
ENISA's role in article 13a

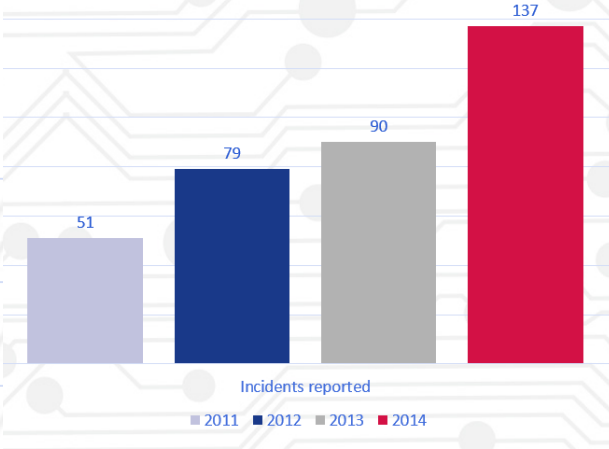
- As requested by the directive, *each MS submits yearly* to Commission *and ENISA* a report with *significant incidents* that had an impact on their networks and services.
- To achieve a harmonised implementation, in 2010, ENISA, Ministries and NRAs initiated a series of meetings (the Article 13a Expert Group).
- Developed an online platform for incident reporting.

Art. 13a incident reporting process



Art. 13a incidents - impact on services (percentage)

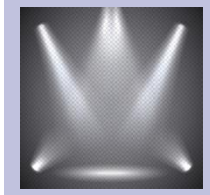


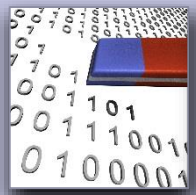


GDPR

General Data Protection Regulation

DATA SUBJECTS






Reinforced user rights

New user rights

EU HARMONISATION

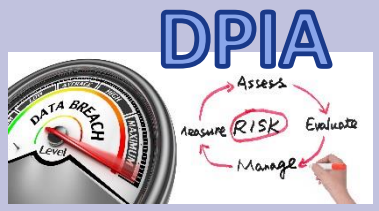
European Data Protection Board

NATIONAL DPAs

Increased powers and fines

DATA CONTROLLERS

Privacy by design



Accountability

ENISA's role in GDPR

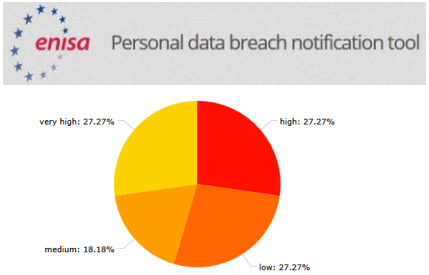
Security of personal data

Crypto

Security measures for controllers

Privacy Enhancing Technologies

Personal data breaches



Transparency, control, new user rights

Personal Data Clouds

Right to be forgotten

Big data privacy

Summary

01 Support to improve cybersecurity strategies in the EU

02 Risk assessment, incident reporting in eIDAS

03 Incident reporting

04 PETs and breach notification in data protection

05 ENISA offers dependable assistance to the MS on NIS

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu