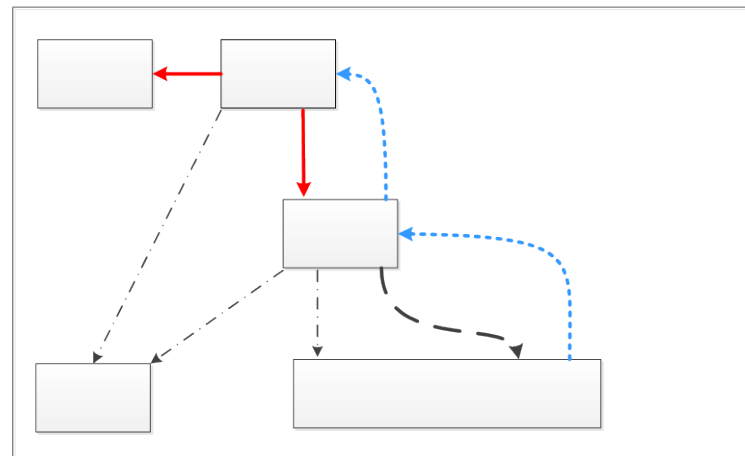




enisa

Implementing EU Legislation



Christoffer Karsberg

Secure Infrastructure and Services Unit

ENISA

NLO meeting 17 Feb 2014



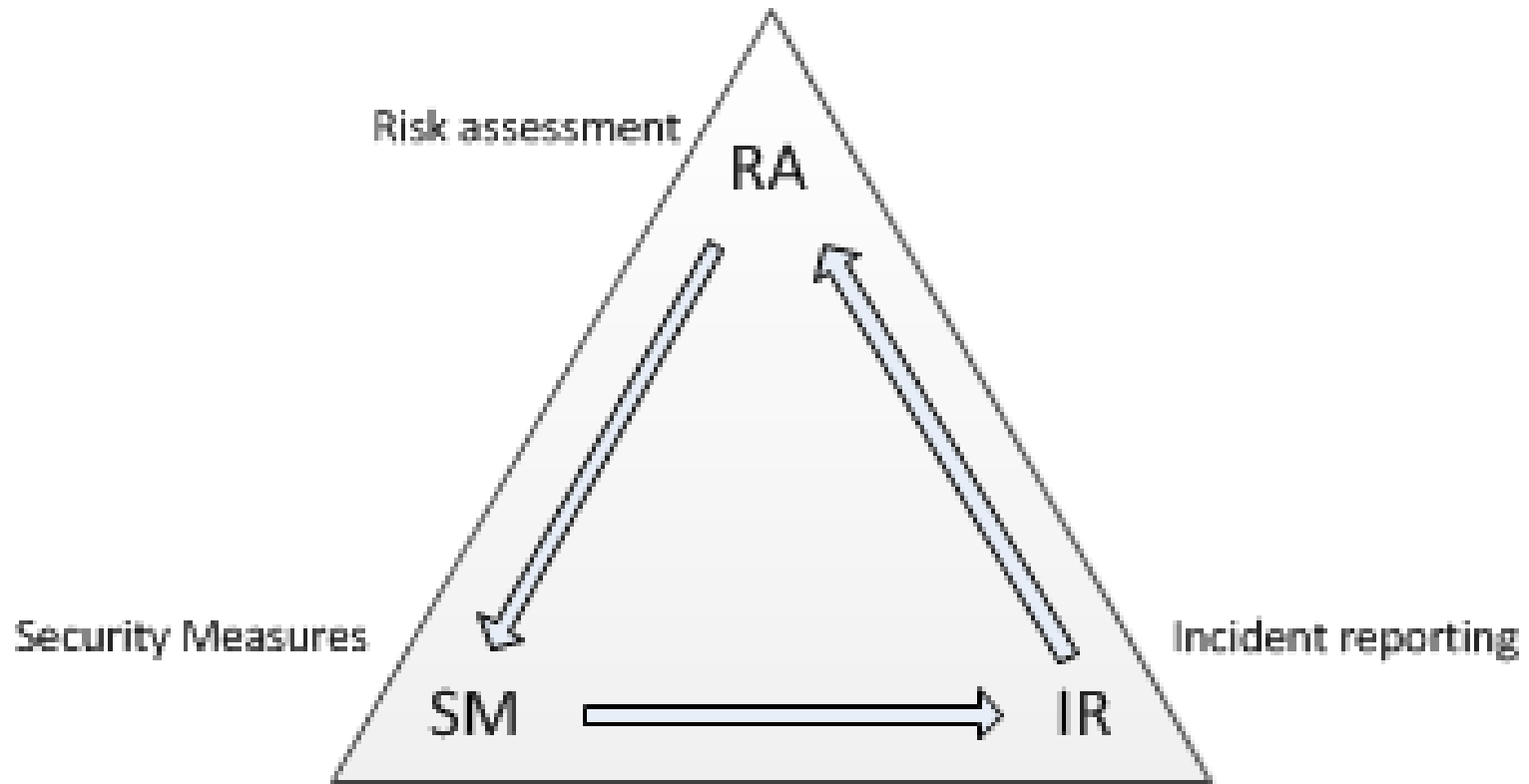


Article 13a Principles



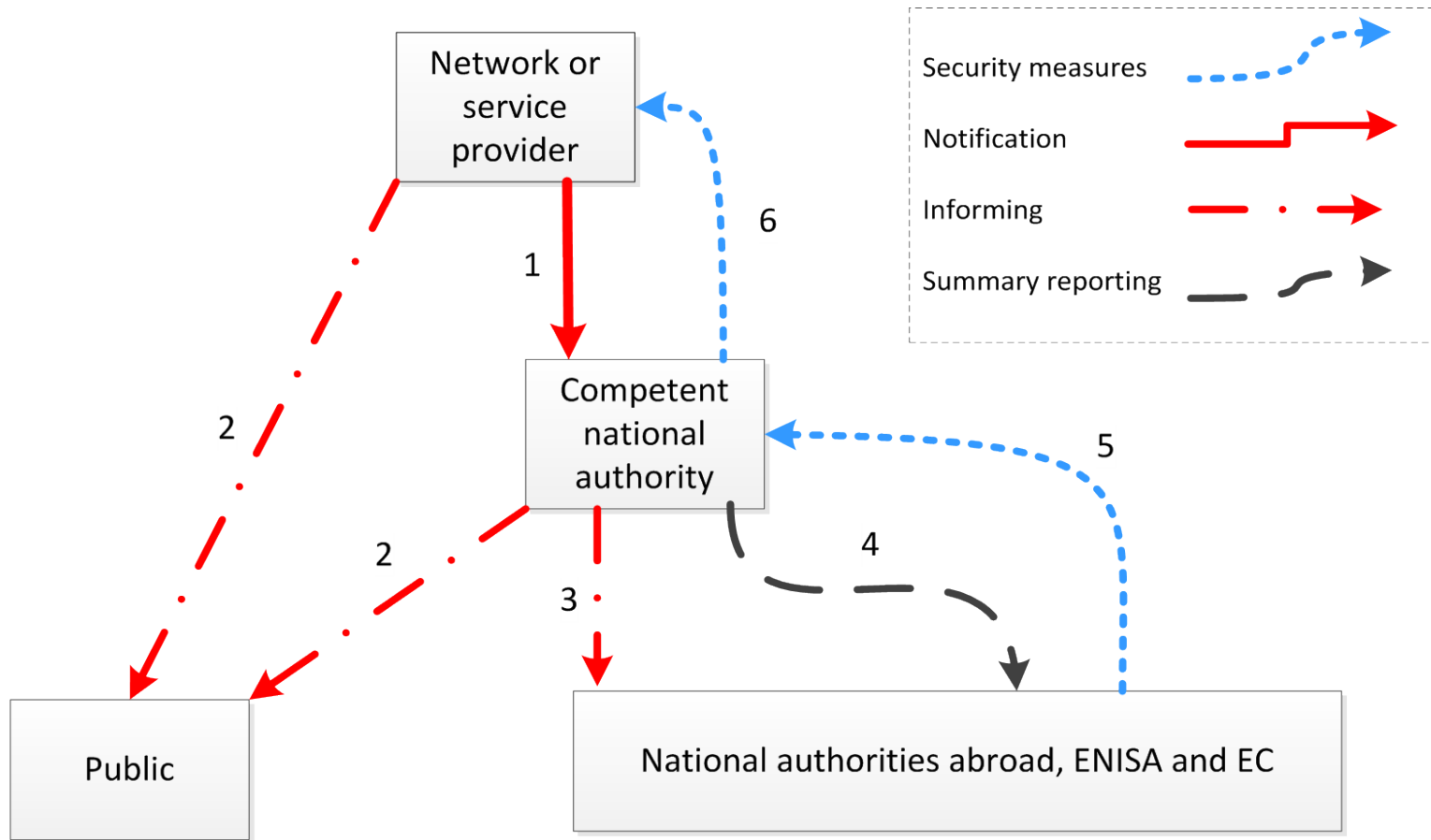
- EU Directive
 - allows MS to adapt to national circumstances
 - Implementing measures by the EC are an option
- Harmonization is achieved
 - ENISA convenes NRAs on a voluntary basis
 - ENISA drafts non-binding guidelines for NRAs, with NRAs
 - NRAs share about national legislative processes, past incidents, supervision experiences.
- Countries, markets and regulators are different
 - National thresholds for reporting are different
 - ENISA sets EU reporting threshold, in consensus with NRAs
- National incident reporting drives supervision of the sector
- Pan-EU sharing (summaries of) incident reports drives collaboration and harmonization.

Security processes mandated by Art13a



- Goal: Security of e-communication networks and services
- Supervised by a national regulator
(in collaboration with regulators abroad – the 'single market')

Information flows in Article 13a





Article 13a Expert group

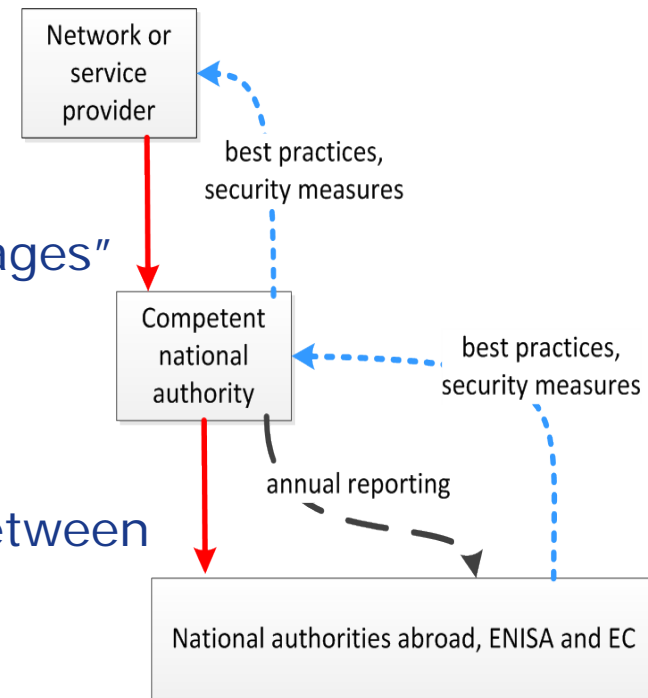


- Informal, voluntary group of experts
- Chaired by ENISA, EC is observer
- The NRAs in the EU + EFTA countries
- 3 F2F meetings per year – next meeting is the 12th meeting – in Malta 25-26 Feb. The 13th meeting is in Helsinki 11-12 June.
- Tele-meetings when needed
- Discussion topics
 - Implementation of the EU directive
 - Supervision activities
 - **Past incidents, stories, sharing experiences**
- Tools
 - Guideline on incident reporting
 - Guideline on security measures
 - Mailing list, portal, issue tracker, reporting tool
 - Agreement on sharing (Traffic Light Protocol)
 - Contact list for cross border notification
 - State of play (status, issues per member state)



Incident reporting as a means to improve

- Understand and discuss specific security issues
 - Not 'cyber' security in general
- Make recommendations about specific security measures
- Based on the reported incidents we address the most pressing issues:
 - In 2013:
 - "National roaming for mobile outages"
 - "Power supply dependencies"
 - In 2014 we are addressing
 - "Telecoms meet ICT vendors"
 - Interconnection dependencies between critical services and the internet



Article 13a Expert group members



Austria	RTR
Belgium	BIPT
Bulgaria	CRC
Croatia	HAKOM
Cyprus	OCEPR
Czech republic	CTO
Denmark	MINDEF
Estonia	TJA
Finland	FICORA
France	MinFin
Germany	BNetzA
Greece	ADAE, EETT
Hungary	NMHH
Ireland	COMREG
Italy	MISE
Latvia	CERT.LV
Lithuania	RRT
Luxembourg	ILR
Malta	MCA
Netherlands	Ag Telecom/ACM
Poland	UKE
Portugal	ANACOM
Romania	ANCOM
Slovakia	TELEOFF
Slovenia	AKOS
Spain	Minetur
Sweden	PTS
UK	OFCOM



Article 13a Expert group members



Austria	RTR
Belgium	BIPT
Bulgaria	CRC
Croatia	HAKOM
Cyprus	OCEPR
Czech republic	CTO
Denmark	MINDEF
Estonia	TJA
Finland	FICORA
France	MinFin
Germany	BNetzA
Greece	ADAE, EETT
Hungary	NMHH
Ireland	COMREG
Italy	MISE
Latvia	CERT.LV
Lithuania	RRT
Luxembourg	ILR
Malta	MCA
Netherlands	Ag Telecom/ACM
Poland	UKE
Portugal	ANACOM
Romania	ANCOM
Slovakia	TELEOFF
Slovenia	AKOS
Spain	Minetur
Sweden	PTS
UK	OFCOM

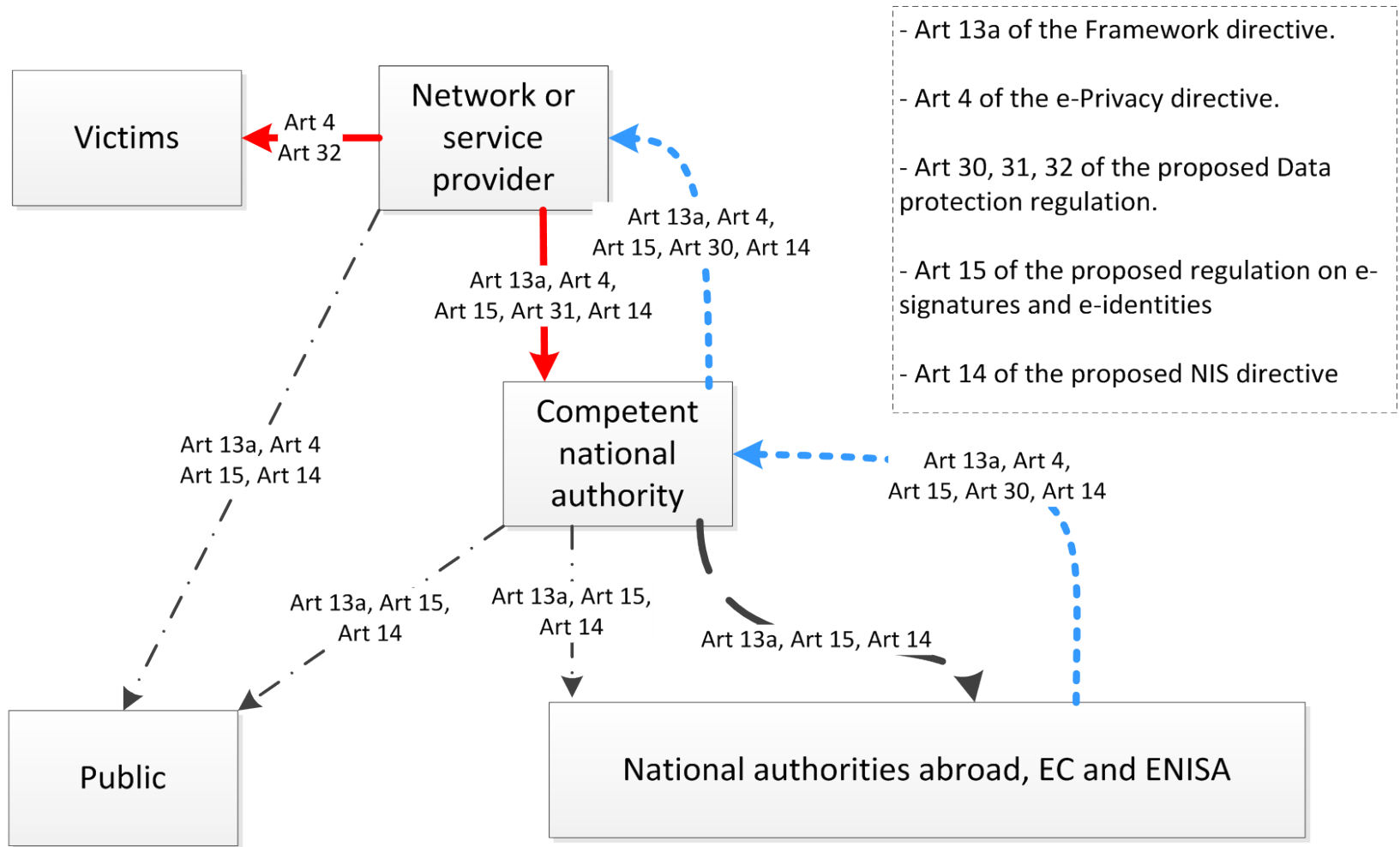




Reference Groups on infrastructure resilience

- Electronic Communications Reference Group
 - CISOs at electronic communications service providers
- This spring we will create the ENISA's infrastructure security and resilience reference group
 - Subject matter experts from the internet operators' community, Cybersecurity agencies, NRAs and infrastructure security and resilience experts

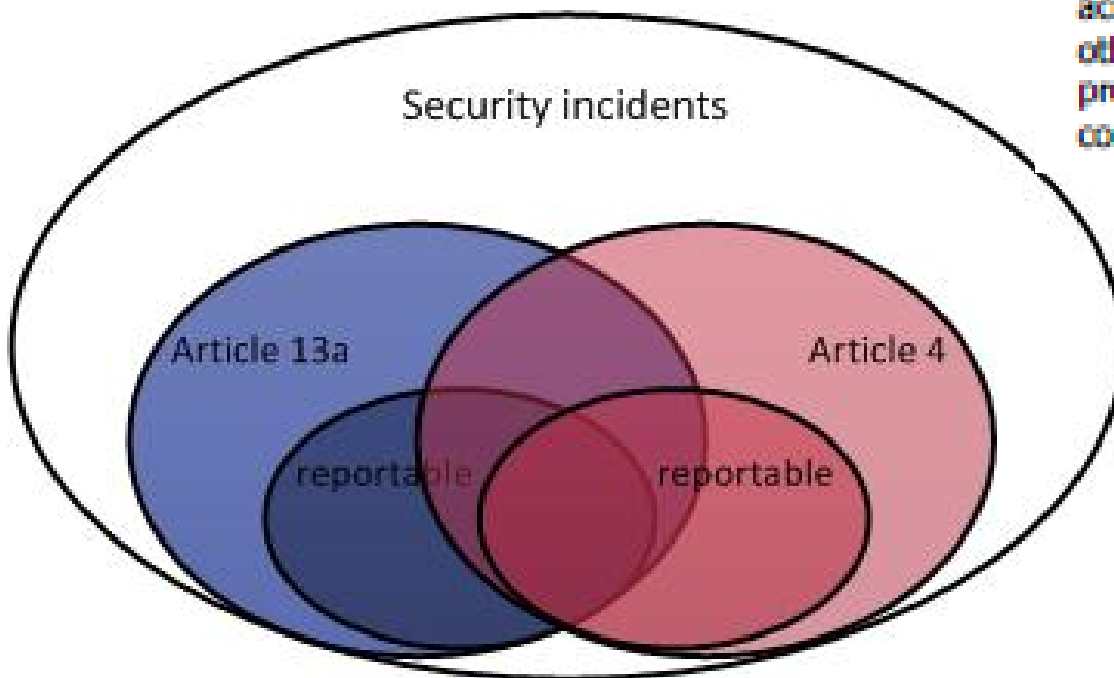
Multiple security articles in EU legislation



Challenges: patchwork

- Article 13a: Security of services and networks
- Article 4: Security of personal data processing
- Often the same security measures.

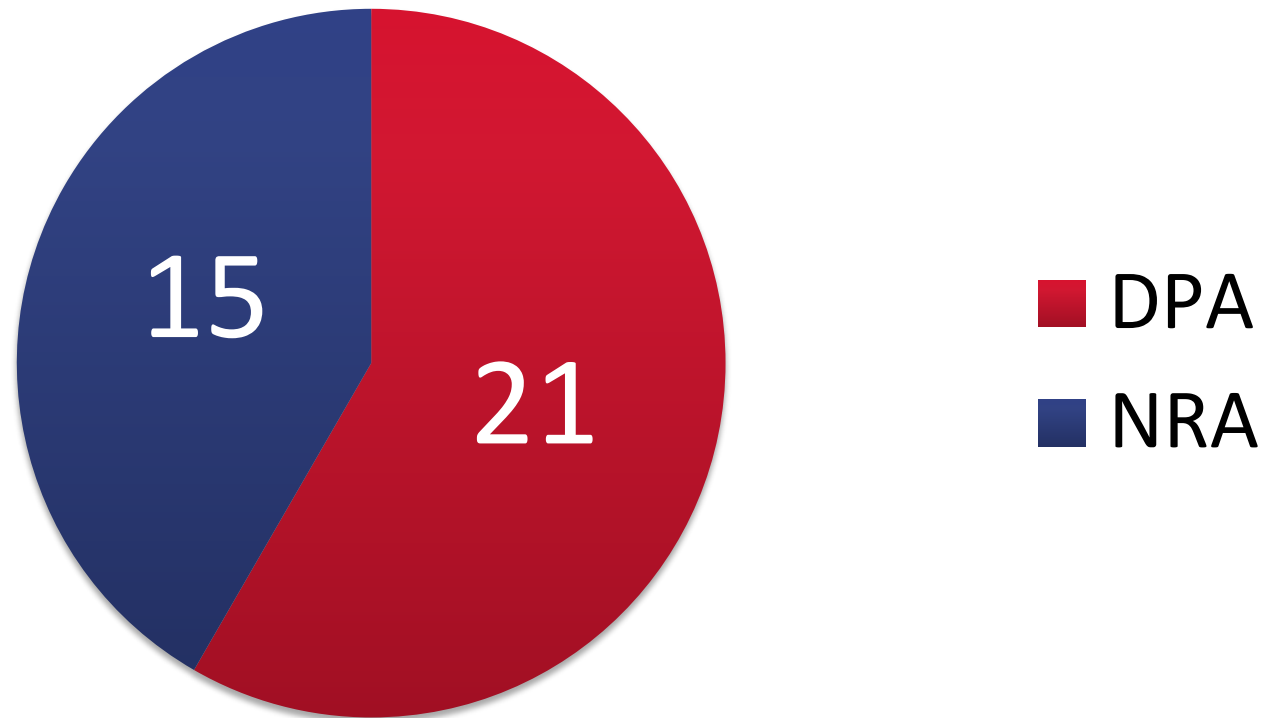
'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.





Personal data breaches: a joint responsibility

Authorities on Article 4 of the e-Privacy directive across the EU



*) DPA – Data protection authority, NRA - telecom regulator

***) In some countries NRAs and DPAs share or split responsibility

Details about Article 4 competences

Country	Art13a Incident Reporting	Art13a Security Measures	Art 4 Incident Reporting	Art4 Security Measures
Austria	RTR	RTR	DPC	DPC/RTR
Belgium	BIPT	BIPT	BIPT	BIPT
Bulgaria	CRC	CRC	PDP	PDP
Croatia	HAKOM	HAKOM	HAKOM	HAKOM
Cyprus	OCEPR	OCEPR	OCEPR	OCEPR/CPDP
Czech republic	CTO	CTO	OPDP/CTO	OPDP/CTO
Denmark	MINDEF	MINDEF	ERST	ERST
Estonia	TJA	TJA	AKI	AKI
Finland	FICORA	FICORA	FICORA	FICORA
France	MinFin	MinFin	CNIL	CNIL
Germany	BNetzA	Bnetza	Bnetza/BfDI	Bnetza/BfDI
Greece	ADAE	ADAE	ADAE/DPA	ADAE/DPA
Hungary	NMHH	NMHH	NMHH	NMHH
Ireland	COMREG	COMREG	DPC	DPC
Italy	MISE	MISE	GPDP	GPDP
Latvia	CERT.LV	CERT.LV	Data Inspector	Data Inspector
Lithuania	RRT	RRT	ADA	ADA
Luxembourg	ILR	ILR	CNPD	CNPD
Malta	MCA	MCA	OIDPC	OIDPC
Netherlands	Ag Telecom/ACM	Ag Telecom/ACM	ACM/CPB	ACM
Poland	UKE	UKE	GIODO	GIODO
Portugal	ANACOM	ANACOM	CNPD	ANACOM
Romania	ANCOM	ANCOM	ANSPDCP	ANSPDCP
Slovakia	TELEOFF	TELEOFF	TELEOFF	TELEOFF
Slovenia	AKOS	AKOS	AKOS/IP-SR	AKOS/IP-SR
Spain	Minetur	Minetur	AGPD	AGPD
Sweden	PTS	PTS	PTS	PTS
UK	OFCOM	OFCOM	ICO	ICO



COM sets up group on Art 4

- COM has set up a group of experts with Art 4 competent national authorities
 - ENISA is supporting this work
 - First meeting was in September 2013
 - Next meeting 11 March in Brussels
 - 2014 we are issuing technical guidelines on security measures
- We want to involve more DPAs from those MS where the DPA is responsible/share responsibility with the NRA.



Art 15 in proposed reg on e-sign/eID

- Art 15 is very similar to Art 13a – targeting Trust Services Providers
 - The regulation is being negotiated
 - ENISA will form an expert group with the competent national authorities
 - Building on FESA (Forum of European Supervisory Authorities for Electronic Signatures)
 - Take stock of the state of play in the Member States
 - Together with the expert group*:
 - Produce incident reporting guidelines
 - Share experiences on potential and past incidents
 - Pilot with incident reporting online tool
- **Eventually we will ask for your support in engaging competent authorities**

*provided that the Regulation has been passed.



Thank you!
Questions?

Christoffer.karsberg@enisa.europa.eu

