Article 13a State of Play 2015

Article 13a implementation in the Member States

JULY 2015

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013
Reproduction is authorised provided the source is acknowledged.

Table of Contents

1. Introduction

This document summarises the implementation in the Member States of Article 13a in the Telecom Package Framework Directive[1].

Article 13a states the following:

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.

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.

4. The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements. These technical implementing measures shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraphs 1 and 2.

   These implementing measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 22(3).

[1] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation.

1.1 Goal

The goal of this document is to provide an overview of the implementation of Article 13a of the Telecom Package Framework Directive in the Member States.

1.2 Target audience

The target audience for this document is the NRAs and relevant Ministries in the European Union Member States as well as experts working in EU's electronic communications sector.

1.3 Structure of this document

The document presents the implementation of Article 13a per Member State and is for each Member State divided in three sub sections, in accordance with the following parts of the first three paragraphs of Article 13a:

- Ensuring provider measures to manage risks for networks and services;
- Ensuring integrity of networks for continuity of supply of services;
- Measures in place to ensure incident reporting by provider to NRA.

2. Austria

The competent authorities for the implementation of Article 13a are primarily the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) and the Telecom-Control Commission (TKK).

Austrian Telecommunications Act (TKG) - unofficial English translation:

Security and integrity

Article 16a.

(1) Operators of public communications networks are to take appropriate steps to guarantee the integrity of their networks and to ensure the continuous availability of the services provided over those networks.

(2) Operators of public communications networks or services are to take reasonable technical and organisational measures with due attention to the technological state of the art in order to ensure a level of security appropriate for controlling risks to network security. In particular, these measures must be suitable for the purpose of preventing and minimising the impact of security incidents on users and interconnected networks.

(3) Upon request, operators of public communications networks or services are obliged to provide the regulatory authority (acting within the scope of its legally assigned duties) with the information necessary to assess the security or integrity of their services and networks, including documented security policies.

(4) In performing its legally assigned duties, the regulatory authority may, in cases where specific indications of a violation of this provision are identified, require operators of public communications networks and services to submit to a security audit by the regulatory authority or by a qualified, independent body commissioned by the regulatory authority at the operator's expense.

(5) Operators of public communications networks or services are to notify the regulatory authority of security breaches or losses of integrity in the form prescribed by the regulatory authority in cases where the incident has a significant impact on the operation of networks or services.

(6) The regulatory authority may inform the regulatory authorities of other EU member states or the European Network and Information Security Agency (ENISA) about notifications received pursuant to Par. 5 where required for the purpose of performing their assigned duties.

(7) In cases where disclosing the breach is in the public interest, the regulatory authority may itself inform the public in an appropriate manner or require the operator in question to do so.

(8) Each year, the regulatory authority shall submit to the European Commission and to ENISA a summary report of all notifications received pursuant to Par. 5 and of the actions taken. The report for a given year is to be submitted by 31 March of the following year.

(9) After consultation with the regulatory authority and with due attention to the relevant international regulations, to the type of network or service, to the technical possibilities, to the protection of personal data and to other user interests worth protecting, the Austrian Federal Minister of Transport, Innovation and Technology may issue an ordinance implementing Articles 16 and 16a and stipulating provisions on:

1. the security of network operation;
2. the maintenance of network integrity;

3. the interoperability of services;
4. preventive security measures;
5. the specification of security policies, especially identity and access administration; and
6. procedures for operators of public communications networks or services in the case of security breaches.

(10) With regard to broadcasting networks and the transmission of broadcasting signals, an ordinance pursuant to Par. 9 is to be issued by KommAustria.

(11) In cases which lie within the competence of the Austrian Data Protection Commission, the regulatory authority shall coordinate and exchange any collected information with the Data Protection Commission.

(12) These provisions are without prejudice to Article 95a and of the Data Protection Act (Federal Law Gazette I No. 165/1999).

2.1 Ensuring Provider measures to manage risks for networks and services

- Legal obligation §16a (2) TKG,
- NRA powers §16a (3) (4) TKG,
- Administrative penal law sanctions §109 (3) 1 + 1a TKG (up to 37.000 €)

2.2 Ensuring integrity of networks for continuity of supply of services

- Legal obligation §16a (1) TKG,
- NRA powers §16a (3) (4) TKG,
- Administrative penal law sanctions §109 (3) 1 + 1a TKG (up to 37.000 €)

2.3 Measures in place to ensure incident reporting by Provider to NRA

- Legal obligation §16a (5) TKG,
- NRA powers §16a (5) TKG,
- Administrative penal law sanctions §109 (3) 1b TKG (up to 37.000 €)

(§16a (9) TKG – overall power for secondary legislation, if necessary – ministerial regulation)

3. Belgium

The competent regulatory authority for the implementation of Article13a provisions is the Belgian Institute for Postal Services and Telecommunications (BIPT).

3.1 Ensuring Provider measures to manage risks for networks and services

The obligation on operators to ensure that they take the measures to appropriately manage the risks is transposed via paragraph 1 of article 114 of the Belgian Electronic Communications Act.

The BIPT (Belgian institute for postal services and telecommunications) is entitled to check whether operators comply with this provision.

According article 114/2 the BIPT can issue binding instructions in relation with paragraph 1 of article 114.

3.2 Ensuring integrity of networks for continuity of supply of services

The obligation on operators to guarantee the integrity of the networks and to ensure continuity of services is in Belgian legislation transposed via paragraph 3 of article 114 of the Electronic Communications Act. Concrete implementation measures can be taken by a Royal Decree after the opinion of the BIPT (today these measures do not exist).

The BIPT is entitled to check whether operators comply with this provision.

Also according article 114/2 the BIPT can issue binding instructions in relation with paragraph 3 of article 114.

3.3 Measures in place to ensure incident reporting by Provider to NRA

In paragraph 2 of article 114/1 of the Electronic Communications Act it is foreseen that operators have to notify the BIPT when a breach of security or loss of integrity occurs which has a significant impact. In the same article it is stated that “significant impact” has to be defined in a Decision of the BIPT. Such a Decision which contains the detailed thresholds which are an indicator of the significance of the impact was adopted by the BIPT on 1st April 2014.

4. Bulgaria

The competent authority for the implementation of Article 13a amendments is the Communications Regulation Commission (CRC).

4.1 Ensuring Provider measures to manage risks for networks and services

The requirements of Art. 13a of the Framework directive are introduced in the Bulgarian Electronic Communications Act:

Article 243. (Amended, SG No. 105/2011, effective 29.12.2011) (1) The undertakings providing public electronic communications networks and/or services shall take appropriate technical and organisational measures to manage the risk posed to security of networks and services. The measures shall ensure a level of security appropriate to the risk presented, taking account of the nature of the problems and the costs of implementing the said measures.

(2) The measures referred to in Paragraph (1) shall be taken to prevent and minimize the impact of security incidents on users and interconnected networks.

4.2 Ensuring integrity of networks for continuity of supply of services

Electronic Communications Act:

Article 243a. *(New, SG No. 105/2011, effective 29.12.2011) The undertakings providing public electronic communications networks shall take all steps necessary to guarantee the integrity of the networks thereof and thus to ensure the continuity of supply of services provided over those networks.*

4.3 Measures in place to ensure incident reporting by Provider to NRA

A3: Electronic Communications Act:

Article 243b. *(New, SG No. 105/2011, effective 29.12.2011)*

(1) The undertakings providing public electronic communications networks and/or services shall immediately notify the Commission[2] of any breach of security or impairment of integrity that has had a significant impact on the operation of networks or services.

(2) The Commission may inform the public or require the undertakings to do so, where the Commission determines that disclosure of the breach is in the public interest.

(3) The Commission may, at its own discretion, inform the competent national regulatory authorities of the affected Member States of the European Union and the European Network and Information Security Agency of the cases referred to in Paragraph (1).

(4) The Commission shall inform the Minister of Transport, Information Technology and Communications of the cases referred to in Paragraph (1).

(5) Once a year, the Commission shall submit a summary report on the notifications received under Paragraph (1) and on the action taken to the European Commission and to the European Network and Information Security Agency.

[2] Communications Regulation Commission

5. Croatia

The competent authority for the implementation of Article 13a is the Croatian Regulatory Authority for Network Industries (HAKOM).

Relevant provisions regarding security and integrity of networks and services, as required by the Framework directive, are prescribed in Electronic Communications Act and more detailed in the Ordinance on the manner and deadlines for the implementation of measures for protecting safety and integrity of networks and services (hereinafter: the Ordinance).

5.1 Ensuring Provider measures to manage risks for networks and services and ensuring integrity of networks for continuity of supply of services

According to the Electronic Communications Act and the Ordinance, electronic communication undertakings are obligated to implement appropriate technical and organizational measures to ensure security and integrity of their networks and services. These measures have to ensure continuity of supply of services as well as a level of security appropriate to the risks and prevent security incidents or mitigate their impact on the operation of a network, network interconnection and user of a public communications services.

These minimum measures have to include risk management procedures, security requirements for staff, security of systems and premises, procedures management, security incidents management, business continuity management, monitoring and testing of security.

The Ordinance also prescribes the list of these minimum measures and associated standards for their enforcement.

Electronic communication undertakings are obligated to submit to the Agency by electronic means once a year, at the latest by the end of January, a documented security policy for the previous year including the undertaken measures and associated standards.

5.2 Measures in place to ensure incident reporting by Provider to NRA

According to the Electronic Communications Act and the Ordinance, operators are obligated to notify the Agency, in the case of unauthorized connection to a public communication network or part of the network and in case of breach of security or integrity of public communications services, which had a significant impact on the provision of networks and services. Also operators are obligated to notify the Agency, in case of Internet-related security incidents, bearing in mind that they refer to servers of operators providing hosting services, own public services and user systems for which the operator received a security incident report. The notification has to be sent using security protocol or encrypted form without delay.

The Electronic Communications Act considers a severe violation of its provisions if the operator does not take the appropriate measures to protect the security and integrity of electronic communications networks or electronic communications services, or does not notify users on threats to network security, or specifies a responsible person, or to notify the Agency or the public about the breach of security or loss of integrity of a significant impact on the operation or performance of services. For these violations the Electronic Communications Act prescribes a fine ranging from 100,000.00 to 1,000,000.00 HRK. These fines are a part of the procedure before Misdemeanour court.

6. Cyprus

The competent authority for the implementation of Article 13a is the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR).

6.1 Ensuring Provider measures to manage risks for networks and services

According to Order 253/2011 (issued by OCECPR), electronic communication undertakings are obliged to take measures so as to ensure their network and information security. Providers are obliged to conduct a Risk Assessment on a yearly basis and to update their Business Continuity Plan (BCP) and Contingency Plan accordingly.

6.2 Ensuring integrity of networks for continuity of supply of services

Providers have an obligation under Order 253/2011 to take a set of security measures e.g redundancy of core network components. OCECPR checks their written procedures with regard to their BCPs annually and has the power to perform audits so as to confirm that the measures described in the written procedures are indeed being actively enforced.

6.3 Measures in place to ensure incident reporting by Provider to NRA

OCECPR has issued Order 371/2013 with regard to notification of security incidents and has conducted a series of meetings with providers, with the intent of clarifying the scope of Article13a and ensuring that the providers have understood and comply with the relevant obligations concerning the notification of certain incidents. ENISA has supported this action by attending one of the meetings with the providers and by presenting the European perspective of the notifications process. In addition OCECPR has the power to perform audits. It should also be mentioned that when OCECPR comes across news from the media, complaints or other sources that network disturbances (such as outages) have occurred, it has the power to contact the provider and ask whether the national thresholds for reporting have been met. The capabilities of the security team of OCECPR will be reinforced within 2015 provided that the CERT is fully functional.

7. Czech Republic

The competent authorities for the implementation of Article 13a are the Ministry of Industry and Trade and the Czech Telecommunications Office.

7.1 Ensuring Provider measures to manage risks for networks and services

Article 13a was implemented to the § 98 of act n. 127/2005 collection on electronic communication. All undertakings are obligated to ensure security and integrity of public networks and public services of electronic communications. The Czech Telecommunication Office (CTO) can impose a fine up to the amount of 20 million CZK when this obligation is not complied.

7.2 Ensuring integrity of networks for continuity of supply of services

According § 98 and § 99 act of electronic communication the undertakings are obligated to process their technical and organizational rules of security and integrity of their networks. CTO determined the content of these technical and organizational rules through an implementing legislation (Decree). The decree sets out general requirements which parts have to contain technical and organizational rules (organizational structure of crisis management, measures to control and maintain the integrity and network security, logistical support, principles for external and internal communications, etc).

7.3 Measures in place to ensure incident reporting by Provider to NRA

According § 98 act of electronic communication the telcos are obligated to notify to CTO a breach of security or loss integrity that has had a significant impact on the operation of electronic communication networks or services. CTO has determined the way and form of notification by means of decree. The CTO can impose a fine up to the amount of 20 million CZK when this obligation is not complied with.

8. Denmark

The competent authority for the implementation of Article 13a is Project Office for Cyber Security within the Ministry of Defence.

8.1 Ensuring Provider measures to manage risks for networks and services

According to the Danish executive order no. 445 of 11 May 2011 (the executive order) electronic communications undertakings are obliged to take measures to appropriately manage the risks posed to security of network and services.

As NRA for Telecom, Centre for Cybersecurity (CFCS) conducts auditing of the telecom sector in order to assure the implementation of appropriate security measures. The auditing for 2014 is based on ENISA's "Technical Guidelines for Minimum Security Measures".

Based on the audit feedback, CFCS can recommend or mandate existing measures to be strengthened or further measures to be implemented.

8.2 Ensuring integrity of networks for continuity of supply of services

According to the executive order, electronic communications undertakings are obliged to develop security plans containing measures to protect networks, services and data. Furthermore, electronic communication undertakings are obliged to do emergency planning, for emergency situations which could significantly impact their own infrastructure and services, or other parts of the national telecom infrastructure. Electronic communication undertakings are also obliged to conduct tests and exercises in order to check their emergency plans. As NRA for telecom, CFCS is auditing the telecom sector to assure that such security and emergency plans have been developed, and tests and exercises are being conducted.

8.3 Measures in place to ensure incident reporting by Provider to NRA

According to the executive order electronic communications undertakings are obliged to immediately report to CFCS any breach of security or loss of integrity that is having a significant impact on the operations of networks or services. CFCS has published guidance for the principles and content of this reporting.

Based on the reporting CFCS can mandate the electronic communications undertakings to provide a final report on the incidents leading to the reporting.

Based on the level of impact, CFCS further provides the incident information to ENISA under the Incident Reporting scheme defined within the Article 13a expert group.

9. Estonia

The competent authorities for the implementation of Article 13a is the Ministry of Economic Affairs and Communication together with the Estonian Information System Authority (EISA).

Ensuring Provider measures to manage risks for networks and services

Article 13a of framework directive has been implemented into Estonian law by Electronic Communications Act § 87^2 .

Please see § 87^2.

(1) A communications undertaking is required to take appropriate technical and organisational measures to manage the risks related to security and integrity of the communications services and network. The measures must be proportionate to the potential emergency situation and ensure minimum impact of incidents endangering the ensuring of security and integrity on users of communications services and related networks and ensure continuity of the provided services.

(2) A communications undertaking is required to notify the Estonian Information System Authority immediately of all incidents endangering the ensuring of security and integrity of the communications network and services which to a significant extent affect the functioning of the communications services or network and of measures taken to eliminate such incidents.

…….

(5) The Estonian Information System Authority is entitled to require a communications undertaking to:

- provide information needed to assess the security and integrity of their communications services and networks, including security policies;
- order a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the Estonian Information System Authority. The cost of the audit shall be covered by the communications undertaking.

9.1 Ensuring integrity of networks for continuity of supply of services

Please see § 87^2 section 1.

(1) A communications undertaking is required to take appropriate technical and organisational measures to manage the risks related to security and integrity of the communications services and network. The measures must be proportionate to the potential emergency situation and ensure minimum impact of incidents endangering the ensuring of security and integrity on users of communications services and related networks and ensure continuity of the provided services.

9.2 Measures in place to ensure incident reporting by Provider to NRA

Please see § 87^2 sections 2, 3, 4 and 5.

(2) A communications undertaking is required to notify the Estonian Information System Authority immediately of all incidents endangering the ensuring of security and integrity of the communications network and services which to a significant extent affect the functioning of the communications services or network and of measures taken to eliminate such incidents.

(3) If necessary, the Estonian Information System Authority shall notify the cases specified in subsection (2) of this section to foreign supervision authorities and the European Network and Information Security Agency (ENISA). If the Estonian Information System Authority finds that due to public interest it is justified to make the violation public, it may inform the public thereof or require the communications undertaking to do it.

(4) The Estonian Information System Authority shall submit a summary report on the notices submitted pursuant to subsection (2) of this section and on measures applied to the European Commission and ENISA once per calendar year.

(5) The Estonian Information System Authority is entitled to require a communications undertaking to:

- provide information needed to assess the security and integrity of their communications services and networks, including security policies;
- order a security audit carried out by a qualified independent body or a competent national authority and make the results thereof available to the Estonian Information System Authority. The cost of the audit shall be covered by the communications undertaking.

10. Finland

The competent authority for the implementation of Article 13a is the Finnish Communications Regulatory Authority (FICORA).

10.1 Ensuring Provider measures to manage risks for networks and services

The Telecom Framework directive and the Directive on privacy and electronic communications have been implemented mainly into one Finnish act: the Information Society Code (917/2014) (http://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf).

Quality requirements for a communications network and services are given in section 243 of the Information Society Code. For example according to section 243(1) paragraph 4, telecommunications operators have to plan, build and maintain public communications networks and communications services in such a manner that among other things significant information security violations and threats against them and other defects and disruptions that significantly interrupt their functionality can be detected. According to section 247(1) when transmitting messages, communications providers must maintain the information security of their services, messages, traffic data and location data. According to section 243(3), maintaining information security means measures to ensure the security of operations, communications, equipment and programmes, as well as the security of information material. According to sections 243(3) and 247(3) these measures shall be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures.

In section 272, telecommunications operators have been granted additional measures for ensuring information security. In section 274, provisions have been given about telecommunications operators' obligations to notify subscribers and users without undue delay of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes communication services. Section 275 includes provisions on telecommunications operators' obligation to give disturbance notifications to the Finnish Communications Regulatory Authority.

10.2 Ensuring integrity of networks for continuity of supply of services

In section 243 on the Information Society Code, certain quality requirements have been set for communications networks and communications services. For example, according to section 243(1) paragraph 1, the technical quality of telecommunications must be of a high standard and information security ensured. In section 243(1) paragraph 2 there is another requirement of the networks and services withstanding normal, foreseeable climatic, mechanical, electromagnetic and other external interference as well as information security threats. Section 243(1) paragraph 14 requires that public communications networks and communications services and the communications networks and communications services connected to them shall function as reliably as possible even in the exceptional circumstances referred to in the Emergency Powers Act (1551/2011) and in disruptive situations under normal circumstances. Sections 243(1) paragraph 6 to 243(1) paragraph 7 further require that the data protection, information security and other rights of users and other persons are not endangered, and that the health and assets of users or other persons are not put at risk. In section 243(1) paragraph 9, it is stated that the networks and services must not cause unreasonable electromagnetic or other interference or information security threats.

In accordance with section 244 on the Information Society Code, The Finnish Communications Regulatory Authority may issue regulations on the quality requirements, information security and interoperability of communications networks and communications services as referred to in section 243. The Finnish

Communication Regulatory Authority actively uses this right and has given a number of technical regulations concerning quality and interoperability requirements. For example:

- Regulation 28 on the interoperability of communications networks and services (https://www.viestintavirasto.fi/en/steeringandsupervision/actsregulationsdecisions/regulations/regulation28ontheinteroperabilityofcommunicationsnetworksandservices.html) concerns the interconnectivity and interoperability of public communications networks and public authority networks, including the communications services provided therein, as well as the information security of interconnection and customer interfaces.
- Regulation 58 on the quality and universal service of communications networks and services (https://www.viestintavirasto.fi/en/steeringandsupervision/actsregulationsdecisions/regulations/regulation58onthequalityanduniversalserviceofcommunicationsnetworksandservices.html) contains general obligations that apply to all general communications networks and services and public authority networks as well as special requirements for telephone services, Internet access services and television services.
- Regulation 67 on information security of telecommunications services (https://www.viestintavirasto.fi/en/steeringandsupervision/actsregulationsdecisions/regulations/regulation67oninformationsecurityoftelecommunicationsservices.html) lays down for example provisions on information security governance and risk management, security measures in interconnectivity interfaces, and minimum security measures in providing internet access services or e-mail services.

10.3 Measures in place to ensure incident reporting by Provider to NRA

According to section 275 on the Information Society Code, a telecommunications operator shall notify the Finnish Communications Regulatory Authority without undue delay of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes communication services. A notification shall also be made of the estimated duration and consequences of information security violations and threats, corrective measures taken as well as of measures undertaken to prevent the reoccurrence of such violations.

Notifying users about different kinds of disturbances has been addressed in the section 274 of the Information Society Code. Section 274(1) states that the telecommunications operator shall notify subscribers and users without undue delay of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes communication services. According to section 275(1), if notifying of information security violation is in the public interest, the Finnish Communications Regulatory Authority may also order the telecommunications operator to provide information regarding the matter.

According to section 274(4) FICORA may issue further regulations on the content and form of the notifications to users. Regarding telecoms operator's obligations to notify FICORA, according to section 275(2) FICORA may also issue further regulations on the significance of a violation as well as the content, form, and delivery of the notification.

The Finnish Communications Regulatory Authority has issued a regulation 66 on disturbances in telecommunications services

(https://www.viestintavirasto.fi/en/steeringandsupervision/actsregulationsdecisions/regulations/regulation66ondisturbancesintelecommunicationsservices.html) which specifies the procedures and contents of notifications about different kinds of disturbances: significant faults or violation of information security.

11. France

The competent authority for the implementation of Article 13a is The Ministry of Industry.

11.1 Ensuring Provider measures to manage risks for networks and services

The Post and electronic communications code creates obligations regarding availability and security of electronic communications networks and services. It was completed by the transposition of the relevant European directive, including reporting of incidents that was previously done without any regulatory obligation. Furthermore the Defence code introduces the concept of vital operator and points of vital importance (comparable to the critical infrastructure and operator) and amplifies these obligations with regard to large operators of electronic communications.

11.2 Ensuring integrity of networks for continuity of supply of services

Two mechanisms exist: the obligation to report significant incidents (technical failure or security breach) and the ability for the State to enforce controls on the integrity and security of networks. The biggest telcos (including MVNO) apply that reporting obligation (smaller telcos hardly reach the reporting thresholds) and have already been concerned by a control (ex: HLR system or IP network). Major operators also undertake to consider a list of potential threats and feared events, to do their risk assessment facing these hazards, to identify their critical systems, their vital sites and to apply the various devices for defence: VigiPirate plans, cyber security and business continuity plans. The State services also have informal knowledge of the architecture of the networks of major operators: these networks have a good level of redundancy therefore no distortion of competition by lack on this point.

11.3 Measures in place to ensure incident reporting by Provider to NRA

Incident reporting is subject to a consensual procedure described in a “guide” describing the severity levels triggering the reporting obligation. These severity levels are consistent with the annual return by the French NRA to ENISA (the thresholds for internal French reporting are usually lower than ENISA’s ones). Two separate but complementary channels exist: the declaration of technical dysfunction (loss of integrity, technical failure) and the declaration of IS attack or presumption of attack. The notifications are made to an H24 operational centre which concentrates such information and possibly associates incidents together, for example malfunctioning of emergency calls reported by call centres. Furthermore, an incident is rarely invisible in social networks (which often amplify it), some web sites are dedicated to this type of incidents. We take into account the sensitivity of the information regarding the incident reporting. These notifications are collected first for statistical purposes but also to inform the services in charge of official communication to the public. Sometimes, the information conveyed by the social networks about the incidents need to be rectified. Personal data breaches (private data) are notified to a dedicated authority (CNIL).

12. Germany

The competent authority for the implementation of Article 13a is the Bundesnetzagentur.

12.1 Ensuring Provider measures to manage risks for networks and services and ensuring integrity of networks for continuity of supply of services

Mandatory obligations for service providers and network operators are regulated in the German telecommunications act, moreover the Federal Network Agency has a supervisory function to ensure that the rules are complied with. The Federal Network Agency has published a "Catalogue on security requirements" in the national gazette which is however not mandatory. It explains, amongst other things, how to compile a security concept.

Below some important excerpts from the **telecommunications act**:

§109

Technical safeguards

Clause 1:

Every service provider shall make appropriate technical arrangements or take other measures in order to protect:

1. the privacy of telecommunications and personal data; and

2. telecommunication and data processing systems against unauthorized access.

Clause 2:

Any person operating a public telecommunications network or publicly available telecommunications services provides, shall take appropriate technical measures and other safeguards for the telecommunications and data processing systems being operated

First

to protect against disruptions that lead to significant impairment of telecommunications networks and services, including those which may be caused by external attack and the effects of disasters and

Second

to control the risks to the security of telecommunications networks and services.

In particular, measures must be taken to secure telecommunications and data processing systems against unauthorized access and to maintain the impact of security incidents on users and interconnected networks for as low as possible. Anyone who operates a public telecommunication network, shall take measures to ensure the proper operation of its networks and thus ensure the continuity of supply of services provided over those networks.

…

Clause 4:

Any person operating a public telecommunication network or who is providing publicly available telecommunication services, shall appoint a security commissioner and file a security concept stipulating:

First

Which public telecommunication network(s) are being operated and which publicly available telecommunication services are provided,

Second

Which hazards have to be assumed and

Third

Which technical safeguards or other protective measures to fulfil the obligations of clause 1 and 2 have been taken or are being planned.

Anyone who operates a public telecommunication network, shall submit the security concept to the Federal Network Agency immediately after the start of operation of the network. Anyone providing publicly available telecommunications services may be required to submit the security concept to the Federal Network Agency after the beginning of provision of the telecommunication services. The security concept has to be submitted along with a declaration that the technical arrangements and other safeguards specified there, have been, or will be, implemented without undue delay. Where the Regulatory Authority establishes shortcomings in the security concept itself or in the course of its implementation, it may require the operator to eliminate them without undue delay. Provided that the underlying conditions for the security concept change, the obligated party (clause 2 or 3) shall adapt the security concept and furnish it again providing the Federal Network Agency with information pertaining to the changes. The Federal Network Agency may review the implementation of the security concept.

12.2 Measures in place to ensure incident reporting by Provider to NRA

Clause 5

Any person operating a public telecommunications network or providing publicly available telecommunications services has to notify the Federal Network Agency about a security breach, including disorders of telecommunications networks or services, having a significant impact on the operation of telecommunication networks or the provision of telecommunication services. The Agency may require a detailed report on the security breach and the remedial action taken from parties obligated under clause (1). If necessary, the Agency may inform the Federal Office for Security in Information Technology (BSI), the national regulatory authorities of the other Member States or the European Union and the European Agency for Network and Information Security (ENISA) on the security breach. The Federal Network Agency may inform the public or require the undertakings (obliged under clause 1) to do so, when it comes to the conclusion that disclosure of the breach is in the public interest. Once a year the Agency shall submit a summary report on the notifications received and the corrective action taken - to the Commission, the European Agency for Network and Information Security (ENISA) and the Federal Office for Security in Information Technology (BSI).

13. Greece

The competent authorities for the implementation of Article 13a are the Hellenic Authority for Communication Security and Privacy (ADAE) and the Hellenic Telecommunications and Post Commission (EETT) which share the mandate of the implementation of Article 37 that transposes Article 13a of Regulation 140/2009.

13.1 Ensuring Provider measures to manage risks for networks and services

The Hellenic Authority for Communication Security and Privacy (ADAE) has issued Regulation 205/2013 (GG B' 1742/15.07.2013) "for the security and integrity of networks and electronic communication services". Article 5 of the Regulation, entitled "Risk assessment", aims at motivating the undertakings to initially analyze, recognize and evaluate their network threats, either internal or external, regarding network integrity and the availability of their services. Based on this analysis undertakings are expected to take specific measures which respond to the evaluated threats and vulnerabilities.

13.2 Ensuring integrity of networks for continuity of supply of services

Undertakings should comply with the requirements imposed with Regulation 205/2013 by implementing a group of appropriate security measures. The content of Regulation 205/2013 is adapted to the national needs but it also covers the requirements of the "Technical Guideline on Security Measures" which was issued by ENISA. ADAE is authorized by Law 4070/2012, which transposes Directive 2009/140/EC into the national legal order, to perform audits on undertakings providing public communications networks or services, in order to monitor the implementation of the security measures taken. These onsite audits may be either scheduled (periodical) or ad hoc. Currently ADAE is in the process of auditing ten major providers of public communications networks and services in Greece.

13.3 Measures in place to ensure incident reporting by Provider to NRA

According to Law 4070/2012, electronic communications undertakings are obliged to notify EETT of any breach of security or loss of integrity that has had a significant impact on the operation of networks or services. In the frame of its competences, EETT has issued Regulation 675/7 "Incident Reporting in relation to the uninterrupted operation of electronic communications' networks and services" (Official Gazette 107/B/24-1-13).

Regulation 675/7:

- defines the incidents having significant impact on the operation of networks or services, by setting specific thresholds based on a combination of duration and the number of users of a service affected
- requires that electronic communications' providers submit an initial report to EETT, within two working days of the occurrence of an incident of a significant impact and a detailed report 15 days after the incident
- defines the procedure for the reporting and the information to be provided by the electronic communications undertakings
- provides an incident report template to be used by the providers. Incident report template is based on ENISAS's «Technical Guideline on Reporting Incident».

Moreover, as prescribed by the same law, EETT forwards also to ADAE this information. This notification mechanism towards ADAE is necessary because it produces feedback information necessary in order to evaluate and to improve, should that be required, the security requirements set out in Regulation 205/2013.

14. Hungary

The competent authority for the implementation of Article 13a is the National Media and Infocommunications Authority (NMHH).

14.1 Ensuring Provider measures to manage risks for networks and services

According to Section 156. (1) of Act C. of 2003 on Electronic Communications (Section 51 of Act CVII. of 2011):

(1) Service providers shall take appropriate technical and organizational measures - jointly with other service providers if necessary - in order to safeguard security of their services, and for the protection of personal data of subscribers obtained in the process of supplying electronic communications services.

Furthermore:

According to Section 156. (9) of Act C. of 2003 on Electronic Communications (Section 51 of Act CVII. of 2011):

(9) The technical and organizational measures shall be sufficient - with regard to best practices and the costs of the proposed measures - to afford a level of security appropriate to the risk presented in connection with network integrity and the services provided.

14.2 Ensuring integrity of networks for continuity of supply of services

According to Section 156. (9) of Act C. of 2003 on Electronic Communications (Section 51 of Act CVII. of 2011):

(9) The technical and organizational measures shall be sufficient - with regard to best practices and the costs of the proposed measures - to afford a level of security appropriate to the risk presented in connection with network integrity and the services provided.

14.3 Measures in place to ensure incident reporting by Provider to NRA

According to Section 156. (1) of Act C. of 2003 on Electronic Communications (Section 51 of Act CVII. of 2011):

(1) Service providers shall take appropriate technical and organizational measures - jointly with other service providers if necessary - in order to safeguard security of their services, and for the protection of personal data of subscribers obtained in the process of supplying electronic communications services.

According to Section 6 (1) of NMHH Decree 4/2012 (I.24.)

(1) Service providers shall at short notice inform the 24/7 Duty Service of NMHH about each case in connection with breach of security or loss of network integrity (hereinafter: incident) that has had a significant impact on the operation of networks or services. (This involves each and every incident, the consequence of which would hamper or make impossible network operations and service provision undertaken in contract.)

NOTE: The 24/7 Duty Service of NMHH is the central duty service of the IT, electronic communications and postal services sectors. Its main task is to provide technical supervision over the duty services of service providers of IT, electronic communications and postal services involved in the duty service system of the

sector; monitoring of network operation and – based on the notifications - facilitating conditions of timely reaction to incurred or potential incidents by informing pre-determined organizations and personnel.

According to Section 6 (2)-(3) of NMHH Decree 4/2012 (I.24)

(2) The 24/7 Duty Service informs by means of the National Media and Infocommunications Authority the regulatory authorities of Member States and the European Network and Information Security Agency (hereinafter: ENISA)

(3) The National Regulatory Authority (NMHH) informs the public and via its decisions it may impose an obligation of information upon service providers, if the lack of disclosure of the incident would seriously risk or damage public interest.

15. Ireland

The competent authority for the implementation of Article 13a is the Commission for Communications Regulation (ComReg).

15.1 Ensuring Provider measures to manage risks for networks and services

Article 13a (1) of the Framework Directive has been transposed in Ireland by a domestic legislative act imposing appropriate obligations on undertakings affected by the Directive and by providing the necessary statutory authority to the appointed national regulatory authority (NRA) to monitor and direct compliance.

The NRA assesses compliance with Regulation 23(1) of the domestic legislative act predominantly through analysis of incident reports (as per Art. 13a (3)) and incident trends. It is likely that the independent NRA will also consider having an audit undertaken where it is considered possible that an undertaking may not be compliant with its obligations in this area.

Statutory provisions.

The domestic legislative act is "The EUROPEAN COMMUNITIES (ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES) (FRAMEWORK) REGULATIONS 2011.

Regulation 23(1) requires that Undertakings providing public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

The NRA can monitor any undertakings compliance with this obligation and issue directions in relation to the obligation if required. Regulation 24(1) provides that: For the purpose of ensuring compliance with Regulation 23 (1), ….+. the Regulator may issue directions to an undertaking providing public communications networks or publicly available electronic communications services, including directions in relation to time limits for implementation.

In addition, in order to ensure the NRA has access to information necessary to monitor an undertaking's compliance, Regulation 24(2) states that: The Regulator may require an undertaking providing public communications networks or publicly available electronic communications services to—

(a) provide information needed to assess the security or integrity of their services and networks, including documented security policies, and

(b) submit to a security audit to be carried out by a qualified independent body nominated by the Regulator and make the results of the audit available to the Regulator ……."

It is an offence for an undertaking to fail to comply with a requirement of Regulation 24.

15.2 Ensuring integrity of networks for continuity of supply of services

Article 13a (2) of the Framework Directive has been transposed by the domestic legislative act referenced above. It imposes appropriate obligations on undertakings affected by the Directive and provides the statutory authority to the NRA to monitor and direct compliance.

The NRA assesses compliance predominantly through analysis of incident reports (as per Art. 13a (3)) and incident trends. It is likely that the independent NRA will also consider having an audit undertaken where it is considered possible that an undertaking may not be compliant with its obligations in this area.

Statutory provisions.

Regulation 23(3) of the legislative act requires that: Undertakings providing public communications networks shall take all appropriate steps to guarantee the integrity of their networks, thereby ensuring the continuity of supply of services provided over those networks.

The NRA can monitor any undertaking's compliance with this obligation and issue directions in relation to the obligation if required. Regulation 24(1) provides that: "For the purpose of ensuring compliance with Regulation 23 .... (3), the Regulator may issue directions to an undertaking providing public communications networks or publicly available electronic communications services, including directions in relation to time limits for implementation"

In addition, in order to ensure the NRA has access to information necessary to monitor an undertaking's compliance Regulation 24(2) states that: The Regulator may require an undertaking providing public communications networks or publicly available electronic communications services to—

(a) provide information needed to assess the security or integrity of their services and networks, including documented security policies, and

(b) submit to a security audit to be carried out by a qualified independent body nominated by the Regulator and make the results of the audit available to the Regulator ……".

It is an offence for an undertaking to fail to comply with a requirement of Regulation 24.

15.3 Measures in place to ensure incident reporting by Provider to NRA

Regulation 23(4) (a) of the domestic legislative act provides that: An undertaking providing public communications networks or publicly available electronic communications services shall notify the Regulator in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks or services. An undertaking that fails to comply with the reporting requirement commits an offence.

The NRA has consulted on the reporting requirement and has advised undertakings of the scope of the reporting requirements in terms of the duration and scale of associated service outages. This reporting requirement is set out in a publication which can be accessed at
http://www.comreg.ie/_fileupload/publications/ComReg1402.pdf

16. Italy

The competent authority for the implementation of Article 13a is the Ministry for Economic Development.

16.1 Ensuring Provider measures to manage risks for networks and services

A proposal of decree has been drafted, but not officially issued yet, on the base of the outcomes of a WG with the relevant TELCOs and Associations. That proposal defines the measures whose electronic communication undertakings must implement in order to manage the risks posed to security of networks and services. The measures refer to those laid down in the dedicated technical guideline defined in the working group established by ENISA.

16.2 Ensuring integrity of networks for continuity of supply of services

The proposal envisages that the TELCOs must implement the measures for their critical assets. The technical annex of the above cited decree contains a procedure for the definition of the conditions under which an asset could be considered critical. TELCOs must provide the Ministry of Economic Development with the documentation related to the implemented measures; the Ministry could decide to make audit in order to verify that the measures are effectively in place and that they are working properly.

16.3 Measures in place to ensure incident reporting by Provider to NRA

The proposal envisages that the TELCOs are obliged to notify the Ministry of Economic Development of incident having a significant impact.

Thresholds have been settled in order to define an incident as significant. Those thresholds are the same as defined in the dedicated technical guideline developed by the working group established by the ENISA.

In case an incident occurs, the TELCOs will send a brief report within three days. A detailed report must be sent within fifteen days.

17. Latvia

The competent authority for the implementation of Article 13a is the Information Technologies Security Incident Response Institution (CERT.LV).

17.1 Ensuring Provider measures to manage risks for networks and services

According to the Information Technologies Security Law (in force as of February 1, 2011), electronic communications undertakings are obliged to ensure integrity of the network, thus ensuring continuity of services, as well as to issue an action plan for a continuous operation of electronic communication network with technical and management measures with aim to overcome network and services security.

According to the Regulation of the Cabinet of Ministers No.327, adopted in April 26, 2011 "Content of action plan of electronic communications undertakings, its control procedures and procedure of temporary disconnection of end-users from electronic communications networks" (in force as of May 1, 2011) electronic communication undertakings have to establish an action plan with information regarding the person (or unit) ensuring the implementation of security measures of an electronic communications network and contact information thereof. Information Technologies Security Incidents Response Institution (CERT.LV) shall evaluate the action plan and, if it establishes a non-conformity with the requirements of Regulation, request the relevant merchant of electronic communications to make corrections according to instructions within the time period specified thereby, which is not less than one month.

CERT.LV has established a good working relationship with all major internet service providers (merchants of electronic communications) to ensure information exchange on regular basis as well as help in the case of crisis.

17.2 Ensuring integrity of networks for continuity of supply of services

According to the Regulation of the Cabinet of Ministers No.327, adopted in April 26, 2011 "Content of action plan of electronic communications undertakings, its control procedures and procedure of temporary disconnection of end-users from electronic communications networks" electronic communication undertakings in action plans have to include a general description and scheme of the structure of an electronic communications network, a risk analysis of an electronic communications network, the procedures for response to security incidents and damages and offences of other types, which endanger the operation of an electronic communications network (technical and organisational measures), a description of measures for restoration of operation of an electronic communications network (technical and organisational measures).

17.3 Measures in place to ensure incident reporting by Provider to NRA

The aforementioned norm in the Republic of Latvia has been transposed by the Information Technologies Security Law and Regulation of the Cabinet of Ministers No.327, "Content of action plan of electronic communications undertakings, its control procedures and procedure of temporary disconnection of end-users from electronic communications networks". Electronic communications undertakings have to report on security or integrity violations that have had a significant impact on electronic communications networks operation or on services provided.

CERT.LV maintains a unified representation of activities in progress in the electronic information space as well as has a good practical cooperation with electronic communications undertakings. Electronic communications undertakings apply CERT.LV provided support for the prevention of an information technologies security incident.

Good working relationship between the CERT.LV and electronic communications undertakings ensures the information exchange regarding serious security incidents, especially in cases when the electronic communications undertaking needs help from the CERT.LV to coordinate incident response.

High competition among electronic communications undertakings is another factor ensuring a high level of availability. The same factor however works against willingness to disclose incidents in order to save the public image of the undertaking.

18. Lithuania

The competent authority for the implementation of Article 13a is the Communications Regulatory Authority.

18.1 Ensuring Provider measures to manage risks for networks and services

According to the requirements of Paragraph 1 of Article 421 of Republic of Lithuania Law on Electronic Communications (hereinafter - Law), undertakings providing public communications networks or publicly available electronic communications services (hereinafter - Providers) must take appropriate technical and organisational measures to appropriately manage the risks posed to security of their networks and services.

More detailed security requirements for Providers are set in Rules for security and integrity of public communications networks and publicly available electronic communications services, approved by order No. 1V-122 of 25 January 2013 of the Director of the Communications Regulatory Authority of the Republic of Lithuania

Communications Regulatory Authority of the Republic of Lithuania (hereinafter – RRT) has the power to issue binding instructions to Providers, including requirement to conduct and independent security audit on their own costs and provide results to RRT.

In case Providers fail to comply with the requirements, RRT has the right to issue binding instructions or impose economic sanctions.

18.2 Ensuring integrity of networks for continuity of supply of services

According to the requirements of Paragraph 2 of Article 421 of Law, undertakings providing public communications networks must implement appropriate technical and organisational measures to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.

In case Providers fail to comply with the requirements, RRT has the right to issue binding instructions or impose economic sanctions.

18.3 Measures in place to ensure incident reporting by Provider to NRA

According to the requirements of Paragraph 5 of Article 421 of Law, Providers must notify RRT of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

In case Providers fail to comply with the requirements, RRT has the right to issue binding instructions or impose economic sanctions.

19. Luxembourg

The competent authority for the implementation of Article 13a is the Institut Luxembourgeois de Régulation (ILR).

19.1 Ensuring Provider measures to manage risks for networks and services

In Luxembourg the Public Research Centre Henri Tudor together with the Institut luxembourgeois de regulation (ILR) and in close collaboration with a selected group of electronic communication providers has developed a risk assessment software tool (named TISRIM Telco) designed specifically to ensure the security and integrity of public telecommunications networks. Based on models of the telecommunications services through business processes and an information system architecture, TISRIM Telco allows fast, simple and robust risk assessment. This results in ongoing improvement of communication security, protecting networks and users against service interruptions and security breaches and enabling compliance with a new Telecom Framework Directive on the security and integrity provisions. This tool has been made available, without charges, to the electronic communication undertakings in order to perform their own risk assessment to comply with the requirements of the aforementioned directive.

19.2 Ensuring integrity of networks for continuity of supply of services

No obligations are in place to force undertakings which provide public communications networks to take appropriate steps to improve technical and organisational measures to guarantee the integrity of their networks and thus ensure the continuity of supply of services provided over those networks. The TISRIM Telco tool proposes a list of measures for implementation and improvement of the public communications network under the responsibility of the undertakings.

19.3 Measures in place to ensure incident reporting by Provider to NRA

The ILR has fixed the criteria and the significant impact for notification of a breach of security or loss of integrity to the NRA via a regulation. An interactive template has been developed by the ILR in order to ensure that the notifications are harmonized and in line with the information required from ENISA according to the technical guideline on incident reporting.

20. Malta

The competent authority for the implementation of Article 13a is the Malta Communications Authority (MCA).

20.1 Ensuring Provider measures to manage risks for networks and services

In Malta, undertakings are legally obliged to take appropriate technical and organisational measures to manage the risks posed to, and safeguard the security of, the networks and services.

20.2 Ensuring integrity of networks for continuity of supply of services

Undertakings are legally obliged to take all necessary measures to ensure the fullest possible availability of service in the event of catastrophic network breakdown, or in the cases of force majeure. Specifically, with regards to international connectivity, operators are legally obliged to secure adequate capacity or alternative measures at all times to ensure an adequate level of uninterrupted connectivity.

A number of incidents have occurred that did not result in catastrophic outages due to the measures adopted by the undertakings, indicating that current measures have been adequate.

20.3 Measures in place to ensure incident reporting by Provider to NRA

Services providers are required by law to report major outages to the Malta Communications Authority (MCA) and to provide a written report to the MCA once service has been restored. The report must include the root cause analysis and the actions taken to restore service. The MCA developed and published reporting guidelines which are in line with the ENISA guidelines.

These reports serve to indicate weaknesses in networks and guide the MCA as to additional measures it may need to take to ensure appropriate network security and integrity.

21. The Netherlands

The competent authorities for the implementation of Article 13a are the Dutch Ministry of Economic Affairs, which is responsible for telecommunications, and the Radiocommunications Agency Netherlands (RAN), which acts as the watchdog, implementer and expert across the entire domain of electronic communication.

Article 13a of the Directive was transposed into Dutch law on June 5 2012. The new requirements were introduced in the Dutch Telecommunications Act (Telecommunicatiewet) in Chapter 11A and comprises of two articles:

Article 11a1 describes measures for public network and/or service providers to manage risks and to ensure integrity of networks for continuity of supply of services (cf. Q1-2).

Article 11a2 describes measures for public network and/or service providers to ensure incident reporting to the competent authority (cf. Q3)

Secondary legislation came into force on 1 January 2013. This piece of regulation describes ways in which the providers, or undertakings, should implement the above mentioned security measures and incident reporting scheme.

21.1 Ensuring Provider measures to manage risks for networks and services

In relation to security measures, article 11a 1 of the Dutch Telecommunications Act includes (inter alia) the following:

Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.

Notwithstanding the provisions of paragraph 1, network and service providers that offer pubic telephone services must take all necessary measures to maintain the availability of public telephony via electronic communications networks in the event of a technical failure or power outage.

Additional rules for the technical implementation of measures can, in future, be laid down by a ministerial set of regulations.

Technical and organizational measures as referred to in this article can, in future, be designated in or pursuant to a general administrative order.

The measures indicated above are intended to create a level of security that, taking into account available technology and the costs of implementing the measures, is appropriate to the risk for disturbances and outages. An important exception however, is made for public telephony for which providers are to take all necessary measures[3].

The entry into force of the secondary regulation obliges all public electronic communications network and service providers to have a continuity plan in place. Radiocommunications Agency Netherlands has issued a set of minimum requirements for such a continuity plan[4]. In addition, RAN is currently consulting providers

[3] Cf. point 2

[4] http://www.agentschaptelecom.nl/sites/default/files/minimale-eisen-continuiteitsplan.pdf

with view of further enhancing, clarifying or modifying the requirements on the appropriate and necessary technical and organisational measures to manage the risks to the security of networks and services.

RAN regularly performs supervisory activities to ensure that network and service providers comply with the regulation regarding security measures.

21.2 Ensuring integrity of networks for continuity of supply of services

The requirements of Chapter 11A article 1 of the Dutch Telecommunications Act apply to both public electronic communications network and service providers and aims to transpose both paragraphs (1 and 2) of Article 13a.

21.3 Measures in place to ensure incident reporting by Provider to NRA

According to Chapter 11A article 2 undertakings providing public communications networks and/or services must notify the Radiocommunications Agency the Netherlands at once about breaches of security and integrity of networks and services, if they had 'significant impact' on operation of networks or services.

Secondary legislation was issued on 1 January 2013[5]. This document describes additional rules for notifying incidents that impact security and/or integrity of public electronic communications networks and services, inter alia which information about the incidents that should be included in the reports, as well as the timeframe for reporting.

All regulation was implemented in accordance with the ENISA document „Technical Guideline on Incidents Reporting".

The Dutch Telecommunications Act works with the notion of 'open norms' and is, in essence, technology-neutral[6]. As a result the Dutch legislation does not specify what incidents should be notified in terms of thresholds, instead it is preferred to use the ENISA guideline as an indication. In addition on-going talks with the undertakings are key in establishing and maintaining a proper incident reporting scheme.

The significance of a notifiable breach is estimated by the undertaking. Incidents are reported at once via a designated telephone line and a secure web portal (www.meldplichttelecomwet.nl), that are both available 24/7. Additional information on the (cause, the impact etc.) incidents is collected by e-mail and telephone.

The Dutch incident reporting scheme was evaluated by the Radiocommunications Agency in 2013, one year upon implementation and the outcomes were shared with the Ministry of Economic Affairs and the relevant undertakings. Based on that, some minor adjustments were made to the reporting scheme but not to the underlying regulation.

From 2014 onwards an annual report is made and shared with the above mentioned parties so that all can learn and benefit from lessons learned.

[5] Besluit Continuiteit
[6] Cf. security measures

22. Poland

The competent authorities for the implementation of Article 13a are the ministry responsible for telecommunication (Ministry of Administration and Digitization), the President of Office of Electronic Communications.

22.1 Ensuring Provider measures to manage risks for networks and services and ensuring integrity of networks for continuity of supply of services

Art. 13a (1) and (2) FR are implemented into Polish legal system in art. 175(1) and 175(2) of the Telecommunication Law.

Article 175(1) A provider of publicly available telecommunications services, and if necessary also an operator of a public telecommunications network shall take technical and organisational measures in order to ensure the security and integrity of the network, services and transmission of communication in relation to the services provided by them. The undertaken measures should ensure security levels adequate to the involved risk, taking account of the recent technological advances and the associated implementation costs.

Article 175(2) A service provider shall inform users of a specific risk of breach to network security requiring measures which go beyond the technical and organizational measures taken by the service provider, as well as of the existing possibilities to ensure security and related costs.

22.2 Ensuring integrity of networks for continuity of supply of services

Art. 13a (2) FR are implemented into Polish legal system in art. 175c and art. 175d of Telecommunication Law.

Article 175c (1) A telecommunications undertaking, subject to Article 160 (2), shall take proportional and reasonable measures in order to ensure security and integrity of the network, services and transmission of communication related to the services provided, including:

- elimination of transmission of communication which poses a risk to network or service security;
- interruption or limitation in the provision of a telecommunications service at the network termination point where communication posing risk to network or service security originates.

Article 175c (2) A telecommunications undertaking shall inform the President of UKE of taking measures referred to in paragraph 1, without delay, but not later than within 24 hours these measures are taken. The information shall include data necessary to identify the risks to network or service security and transmission of communication related to the services provided, indicating the remedies taken.

Article 175c (3) The President of UKE may, by means of a decision, prohibit the application of measures referred to in paragraph 1, if he/she finds that they are not proportionate or reasonable or fail to fulfil the objectives referred to in that provision.

Article 175c (4) If the measures referred to in paragraph 1 are taken, a telecommunications undertaking shall not be liable for non-performance or inadequate performance of telecommunications services within the scope resulting from the measures taken. The provision shall not apply if a decision referred to in paragraph 3 is issued.

Article 175c (5) A telecommunications undertaking may inform other telecommunications undertakings and entities active in IT security about the identified risks referred to in paragraph 1. Such information may contain the data required for identifying and limiting such risk.

Article 175d. The Minister competent for communications may specify, by means of an ordinance, minimum technical and organizational measures and the methods of preventing risks which should be applied by telecommunications undertakings in order to ensure security or integrity of the network or services, taking into account the guidelines of the European Commission and the European Network and Information Security Agency within this scope (ordinance is not issued).

Additionally there is a set of older regulation (prepared before implementation of art 13a FR) referring to security and integrity of network and services:

As stated in art. 176a(1) of Telecommunication Law undertakings providing public communications networks or publicly available electronic communications services should bear in mind in order to ensure continuity of services and networks provision, possibility of occurring crisis situations, states of emergency and direct threats to the telecommunications infrastructure. Those emergency situations are actually the cases of security and network integrity breach.

According to art. 176a(2) of Telecommunication Law undertakings providing public communications networks or publicly available electronic communications services are obliged to have valid and accepted by President of UKE action plans for emergency situations. In those plans there are envisaged procedures and measures aimed at:

- protection of the infrastructure against damage and unauthorised access,
- ensuring continuity of networks and services,
- in the cases of loss of continuity of networks and service – reconstruction of networks and services provision,
- cooperation with equipment and service maintenance suppliers.

According to secondary legislation delegated by art. 176a(5) of Telecommunication Law the process of action plans preparation is precluded by analyse of potential risks and threats in area where the undertaking is operating and the assessment of these risks and threats impact on its infrastructure and ability to continue service and network provision. These analyses and assessments should be undertaken on the basis of data received from the public administration (local governments, provincial governors) and – in the case of the biggest companies – from the state authorities responsible for state security and crisis management.

The undertaking describes in the plan also measures and procedures applicable in the case of emergency (which, as noted above, is identical with measures and procedures protecting against breaches of security and integrity of networks and services).

22.3 Measures in place to ensure incident reporting by Provider to NRA

Art. 13a(3) of DR was transposed into Polish legal system by in. art. 175a of telecommunication Law.

According to art. 175a(1) of Telecommunication Law telecommunications undertakings are obliged to immediately inform the President of UKE about cases of breaches of security and integrity of networks and services, if they had remarkable impact on operation of networks or services. They are obliged also to inform about preventive measures that had been taken by the undertaking.

On the basis of authorization stated in art. 175a(2) there is issued secondary legislation on the form of notification of breaches. The secondary legislation also precises which cases should be notified to the

President of UKE. Above mentioned regulations were implemented in accordance with ENISA document "Technical Guideline on Incidents Reporting".

The system encompasses network of contact points established by telecommunication undertakings and the contact point established by President of UKE.

The significance of the breach that occurred is estimated by the undertaking. The system is functioning efficiently and it allows President of UKE to collect information about most significant breaches if safety and networks and services integrity, enabling next preparation (in line with DR, ENISA recommendations and national Telecommunication Law) incidental reports and yearly report for European Commission.

23. Portugal

The competent authority for the implementation of Article 13a is the Autoridade Nacional de Comunicações (ANACOM).

23.1 Ensuring Provider measures to manage risks for networks and services

As stated in

Article 54-A, 1: - Undertakings providing public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to appropriately prevent, manage and reduce the risks posed to security of networks and services, aiming in particular to prevent or minimise the impact of security incidents on interconnected networks, at national and international level, and users

23.2 Ensuring integrity of networks for continuity of supply of services

As stated in,

Article 54-A, 2: - Undertakings providing public communications networks shall take all appropriate steps to guarantee the integrity of their networks, ensuring the continuity of supply of services provided over those networks.

Article 54-C:, 1 - For the purposes of article 54-A, the NRA is entitled to approve and impose technical implementing measures on undertakings that provide public communications networks or publicly available electronic communications services. (…) 3 - Implementing measures provided for in the preceding paragraphs shall comply with decisions of the European Commission adopted pursuant to the procedure provided for in article 13-A of Directive 2002/21/EC, of the European Parliament and of the Council of 7 March, as amended by Directive 2009/140/EC of the European Parliament and of the Council, of 25 November, and, in their absence, such measures shall be based on European and international standards governing the matter.

Article 54-D Additional requirements - In addition to the technical implementing measures provided for in the preceding article, the NRA, for the purposes of article 54-A, is entitled to impose more demanding requirements on undertakings providing public communications networks or publicly available electronic communications services, in particular determining the following:

- The indication of a permanent contact point, for the purposes of the present chapter;
- The drawing up of an up-to-date plan covering all technical and organizational measures adopted;
- The performance of assessment and improvement exercises of technical and organizational measures adopted, as well as the participation in joint exercises;
- The drawing up and presentation to the NRA of an annual report under terms to be set out, including in particular, the experience obtained at the level of security incidents.

23.3 Measures in place to ensure incident reporting by Provider to NRA

As stated in,

Article 54-B: Undertakings providing public communications networks or publicly available electronic communications services shall notify the NRA of a breach of security or loss of integrity with a significant impact on the operation of networks or services.

-Article 54-C 2: - For the purposes of article 54-B, it is incumbent on the NRA to approve measures defining the circumstances, format and procedures applicable to notification requirements concerning breach of security or loss of integrity of networks.

-Article 54-E: It is incumbent on the NRA: b) To inform the public, by the most appropriate means, of any breach of security or loss of integrity or to require undertakings that provide public communications networks or publicly available electronic communications services to do so, where it determines that disclosure of the breach is in the public interest.

-Determination of 12 December 2013, ANACOM has approved the final decision on the circumstances, format and procedures applicable to the requirements of reporting security breaches or losses of integrity with significant impact on the functioning of public communications networks and publicly available electronic communication services; the decision also governs respective public disclosure, by companies offering public communications networks or publicly available electronic communication services, of security breaches or losses of integrity as may occur on their networks and as part of their services. (http://www.anacom.pt/streaming/decision_12Dec2013integritySecurityEC.pdf?contentId=1186408&field=ATTACHED_FILE)

24. Romania

The competent authority for the implementation of Article 13a is the National Authority for Management and Regulation in Communications (ANCOM).

24.1 Ensuring Provider measures to manage risks for networks and services and ensuring integrity of networks for continuity of supply of services

According to Decision 512/2013,

1) the providers of public electronic communications networks or of publicly available electronic communications services shall take all appropriate security measures to appropriately manage the risks posed to the security of electronic communications networks and services in order to ensure a level of security appropriate to the identified risk and to prevent or minimise the impact of security incidents on users and interconnected networks, considering the newest technologies and, where applicable, shall collaborate in order to implement these measures. (Art. 3 (1))

2) the providers of public electronic communications networks shall take all appropriate security measures to appropriately manage the risks posed to the integrity of electronic communications networks and services in order to guarantee the integrity of these networks and to ensure the continuity of the provision of services over these networks and, where applicable, shall collaborate in order to implement these measures. (Art. 3 (2))

3) The minimum security measures that the providers should establish and implement in order to comply with the obligations under paragraph (1) and, as applicable, under paragraph (2) shall cover at least the domains identified in annex no. 1. (Art. 3 (3))

The providers shall assess and, if necessary, update these measures whenever required, but at least once every 12 months. (Art.3 (4))

ANCOM chose to treat together the two concepts of security and integrity.

According to Decision 512/2013, security and integrity of electronic communications networks and services means the ability of an electronic communications network or service to resist accidental events or malicious actions which can compromise or affect the continuity of the provision of networks and services at a performance level equivalent to that preceding the occurrence of the event. (Art. 2)

In Decision 512/2013, security measures are defined as follows: means of risk management (of administrative, managerial, technical or legal nature), including policies, actions, plans, equipment, facilities, procedures, techniques etc. meant to remove or reduce the risks posed to the security and integrity of electronic communications networks or services.

This Decision also establish the domains concerned by the minimum security measures. These refer to:

I. Security policy and risk management
II. Human resources security
III. Security and integrity of networks, associated facilities and information
IV. Operations management
V. Incident management
VI. Business continuity management
VII. Monitoring, testing and auditing

The domains are in line with ENISA's Technical Guideline on Security Measures.

In order to monitor the implementation of the provisions of Decision 512/2013 on security measures implemented by providers of electronic communications networks and services, ANCOM conducts periodical surveys.

24.2 Measures in place to ensure incident reporting by Provider to NRA

According to Decision 512/2013, *the providers of public electronic communications networks or of publicly available electronic communications services shall submit to ANCOM, a notification on the existence of an incident with significant impact on the security and integrity of electronic communications networks and services. (**Art. 4**)*

In Decision 512/2013, an incident with significant impact is defined as an incident which affects more than 5,000 connections for at least 60 minutes.

The providers of public electronic communications networks or of publicly available electronic communications services shall submit to ANCOM:

- an **initial notification** on the existence of an incident with significant impact on the security and integrity of electronic communications networks and services (no later than 1 p.m. of the working day following the day when the incident with significant impact on the security and integrity of electronic communications networks and services was detected).
- a **final notification** on the existence of an incident with significant impact on the security and integrity of electronic communications networks and services, within two weeks from its detection.

The initial notification shall be transmitted electronically to a dedicated e-mail address and the final notification shall be transmitted by means of an application available on the ANCOM website as an electronic document having included, attached or logically associated an extended electronic signature based upon a qualified certificate.

Following the centralization, cataloguing and analyzing incidents reported by the providers of public electronic communications networks or of publicly available electronic communications services, ANCOM elaborates an annual report available on its website[7].

Having analyzed the incidents with significant impact on the electronic communications networks and services, ANCOM may identify the incident cause, monitor the steps taken by the respective provider for the purpose of restoring the networks and services to an adequate level and may evaluate the security level of the electronic communications networks and services. The statistical analysis of the incidents is, as well, an effective instrument of tracking the trends.

[7] The reports are available at the following address: http://www.ancom.org.ro/en/rapoarte-si-studii-privind-securitatea-si-integritatea-retelelor-si-serviciilor-de-comunicatii-electronice-_4958

25. Slovak Republic

The competent authority for the implementation of Article 13a in Slovak Republic is the Regulatory authority for electronic communications and postal services (RU).

25.1 Ensuring Provider measures to manage risks for networks and services

Act on electronic communications, section 64:

(1) The undertaking that provides public networks or public services shall be obliged to take appropriate technical and organizational measures to protect security of its networks and services which with regard to the technology state shall ensure such a level of security that is adequate to the risk posed. Measures shall be taken in particular to prevent and minimize impact of security incidents on users and interconnected networks.

(6) The undertaking that provides public networks or services shall be obliged:

a) Upon the request of the Office, to provide the relevant information necessary to assess security and integrity of its services and networks, including the documented security policies,…

Measure on integrity and security of electronic communications (O-30/2012) imposes an obligation to the undertakings to prepare and maintain a security policy in accordance with the minimum set of 7 security domains stipulated in the measure.

RU can impose a fine to an undertaking up to the amount of 1,5 mil. euro in case it does not comply with the obligation in point (1) and up to the amount of 300k euro in case it does not comply with the obligation in point (6).

25.2 Ensuring integrity of networks for continuity of supply of services

Act on electronic communications, section 64:

(2) The undertaking that provides public networks shall be obliged to maintain integrity of its networks in order to ensure the continuity of provisioning services over those networks.

(6) The undertaking that provides public networks or services shall be obliged:

...

b) To enable a security audit carried out by a qualified independent person selected by the Office or the Office itself, while the cost of the audit shall be covered by the undertaking.

c) To provide the results of the audit to the Office and, upon the request, the Office for protection of personal data,…

Obligations stipulated by the above mentioned Measure on integrity and security of electronic communications include obligations, which shall also ensure a high level of continuity of supply of services.

RU can impose a fine to an undertaking up to the amount of 1,5 mil. euro in case it does not comply with the obligation in point (2) and up to the amount of 300k euro in case it does not comply with the obligation in point (6).

25.3 Measures in place to ensure incident reporting by Provider to NRA

Act on electronic communications, section 64:

(3) The undertaking that provides public networks or services shall be obliged, without delay, to inform the Office about a breach of security or integrity that has had a significant impact on the operation of networks or services.

(6) The undertaking that provides public networks or services shall be obliged:

...

d) To cooperate with the Office in investigation of cases of non-compliance with regulations and their impact on network security and integrity and, upon the request, to provide the Office with relating relevant information.

The above mentioned Measure on integrity and security of electronic communications includes sections stipulating details on incident reporting. The annex of the measure includes conditions and thresholds for determination of incidents with significant impact.

RU can impose a fine to an undertaking up to the amount of 300k euro in case it does not comply with the obligations in points (3) or (6).

26. Slovenia

The competent authority for the implementation of Article 13a is the Agency for Communication Networks and Services of the Republic of Slovenia (AKOS).

26.1 Ensuring Provider measures to manage risks for networks and services

The Republic of Slovenia transposed the provisions on security of networks and services and operation under exceptional circumstances through the provisions of the Chapter VII of the Electronic Communications Act (Official Gazette of RS, Nr.109/12, 110/13, 40/14- ZIN-B and 54/14- decision of the Constitutional Court, hereinafter: ECA). Provisions of Article 13a (1) of the Framework Directive are transposed by Article 79 of ECA that establishes obligations for operators who must adopt appropriate technical and organisational measures to appropriately manage network and service security risks, in particular to prevent and reduce the impact of security incidents on users and interconnected networks. Having regard to the state of the art, such measures shall ensure a level of security appropriate to the risk presented. This measures shall also include the adoption and implementation of a security plan, which the operators shall designate a business secret. According to the paragraph 3 of Article 79 the security plan shall at least:

- identify all security risks from within or outside the operator's domain that may threaten operation of the public communications network and/or interfere with the functioning of publicly available electronic communications services provided by the operator;
- identify the likelihood of an event for all security risks referred to in the preceding indent;
- determine the level of negative effects and consequences for the operation of the public communications network and publicly available communications services for all the security risks referred to in the first indent;
- specify measures to reduce the likelihood of a security incident occurring;
- specify measures to reduce the negative impacts and mitigate the consequences of the security incident;
- determine the appropriate method for organising security within the operator domain, an integral part of which shall be security of the network and information system, and physical protection of facilities and installations;
- identify an appropriate method of ensuring that key posts dealing professionally with security at the operator are filled;
- determine the method of regular verification that measures and procedures undertaken match those specified in the security plan.

According to Article 86 of ECA The Electronic Communications Networks and Services Agency of the Republic of Slovenia (hereinafter: the Agency) shall, by means of a general act, specify the manner of implementation of the provisions of the chapter VII of the ECA (including the provision of Article 79).

On the basis of Article 86 of ECA the Agency has adopted the General act on the security of networks and services (Official Gazette of RS, Nr. 75/13), which specifies organizational measures, which must be taken by operators, in order to adequately ensure the security of networks, services and network integrity.

According to Article 87 of ECA, the Agency also has to supervise the implementation of the above mentioned provisions of the Chapter VII of ECA.

According to Articles 228 and 233 of ECA the Agency can also impose fine in case of violations of above mentioned provisions.

26.2 Ensuring integrity of networks for continuity of supply of services

Provisions of Article 13a (2) of the Framework directive are transposed by Article 80 of ECA. According to Article 80 of ECA network operators shall take all appropriate measures to ensure the integrity of their networks, in order to ensure the uninterrupted provision of services over such networks.

According to Article 86 of ECA the Agency shall, by means of a general act, specify the manner of implementation of the provisions of the chapter VII of the ECA (including the provision of Article 80).

On the basis of Article 86 of ECA, the Agency has adopted the General act on the security of networks and services (Official Gazette of RS, Nr. 75/13), which specifies organizational measures, which must be taken by operators, in order to adequately ensure the security of networks, services and network integrity.

According to Article 87 of ECA, the Agency also has to supervise the implementation of the above mentioned provisions of the Chapter VII of ECA.

According to Articles 228 and 233 of ECA the Agency can also impose fine in case of violations of above mentioned provisions.

26.3 Measures in place to ensure incident reporting by Provider to NRA

Provisions of Article 13a (3) of the Framework directive are transposed by Article 81 of ECA. According to Article 81 of ECA there is an obligation for operators to notify and report network security or integrity breaches. Operators must, immediately upon detection, notify the Agency of any breach of security or integrity that has had a significant impact on the operation of public communications networks or the provision of the public communications services. Where necessary and with regard to the degree of the breach, the Agency shall notify the national contact point for dealing with security incidents (SI-CERT) of individual network and service security breaches and network integrity breaches. Where necessary and with regard to the degree of breach, the Agency shall notify national regulatory authorities in other EU Member States and the European Network and Information Security Agency (ENISA) of individual network and service security breaches and network integrity breaches. The Agency may inform the public or require the operator affected by the security or integrity breach to do so if it believes that disclosure of the breach is in the public interest. Once a year, and not later than by the end of February for the previous year, the Agency shall submit a summary report to the European Commission and ENISA on notifications received and actions taken in accordance with the first, second and/or third paragraphs of Article 81.

According to Article 86 of ECA the Agency shall, by means of a general act, specify the manner of implementation of the provisions of the chapter VII of the ECA (including the provision of Article 81).

On the basis of Article 86 of ECA, the Agency has adopted the General act on the security of networks and services (Official Gazette of RS, Nr. 75/13), which specifies organizational measures, which must be taken by operators, in order to adequately ensure the security of networks, services and network integrity.

According to Article 87 of ECA, the Agency also has to supervise the implementation of the above mentioned provisions of the Chapter VII of ECA.

According to Articles 228 and 233 of ECA the Agency can also impose fine in case of violations of above mentioned provisions.

27. Spain

The competent authority for the implementation of Article 13a is the Ministry of Industry, Energy and Tourism (MINETUR).

27.1 Ensuring Provider measures to manage risks for networks and services

The new General Telecommunications Law, approved on 8th March 2014, states the following:

"1. Operators of networks and electronic communications services available to the public, properly manage security risks that may affect their networks and services to ensure an adequate level of safety and prevent or minimize the impact of incidents safety on users and interconnected networks."

27.2 Ensuring integrity of networks for continuity of supply of services

The new General Telecommunications Law, approved on 8th March 2014, states the following:

"2. Also, operators of public electronic communications networks guarantee the completeness thereof to ensure the continued provision of services using these networks."

(…)

4. The Ministry of Industry shall establish mechanisms to monitor compliance with the above requirements and, where appropriate, shall issue instructions, which shall be binding for operators, including those relating to application deadlines, to adopt measures concerning the integrity and security of networks and electronic communications services. Among them, impose:

a) The obligation to provide the information necessary to evaluate the safety and integrity of their services and networks, including documented security policies.

b) The obligation to submit to a security audit by an independent body or a competent authority, and put the result available to the Ministry of Industry. The cost of the audit shall be borne by the operator.

5. In particular, operators shall ensure the widest possible availability of publicly available telephone services through public communications networks in the event of catastrophic network breakdown or in cases of force majeure, and shall take all measures necessary to ensure access uninterrupted emergency services."

27.3 Measures in place to ensure incident reporting by Provider to NRA

The new General Telecommunications Law, approved on 8th March 2014, states the following:

"3. Operators that operate networks or provide electronic communications services available to the public shall notify the Ministry of Industry breaches of security or loss of integrity that has had a significant impact on the operation of networks or services.

Where appropriate, the Ministry shall notify the competent national authorities of other Member States and the European Agency for Safety and Information Networks (ENISA). It may inform the public or require companies to do so, if it determines that disclosure of the violation interests the public Once a year, the Ministry shall submit to the Commission and ENISA a summary report of the notifications sent and action taken pursuant to this paragraph.

Similarly, the Ministry shall inform the Ministry of Security of the Ministry of Interior those incidents affecting national strategic operators relevant to improving the protection of critical infrastructure in the framework

of Law 8/2011, of April 28, regulating the same. Also the Ministry shall inform the National Commission of Markets and Competition breaches of security or loss of integrity that this section refers affecting or likely to affect the specific obligations imposed by the Committee in the relevant markets."

28. Sweden

The competent authority for the implementation of Article 13a is the Swedish Post and Telecom Authority (PTS).

28.1 Ensuring Provider measures to manage risks for networks and services

Chapter 5 Section 6b of the Electronic Communications Act implements Article 13a(1)-(2). It requires providers of public communications networks and publicly available electronic communications services to take appropriate technical and organisational measures to ensure that reasonable demands for operational reliability are achieved. The measures taken shall be intended to create a level of security that, taking into account available technology and the costs of implementing the measures, is appropriate to the risk for disturbances and outages.

The Swedish Post and Telecom Authority (PTS) has issued general advice which details the requirements. PTS is currently drafting regulations which will replace the general advice and lay down more in-depth and detailed binding requirements on the appropriate technical and organisational measures required to appropriately manage the risks posed to security of networks and services. The Regulations will take into account the ENISA recommendation on security measures under Article 13a(1)-(2).

PTS regularly performs supervisory activities to ensure that providers comply with the obligations laid down in the Electronic Communications Act.

28.2 Ensuring integrity of networks for continuity of supply of services

The requirements of Chapter 5 Section 6b of the Electronic Communications Act apply to both network and service providers and aims to transpose both paragraphs (1) and (2) of Article 13a.

28.3 Measures in place to ensure incident reporting by Provider to NRA

Chapter 5 Section 6c of the Electronic Communications Act implements Article 13a(3). PTS has issued regulations detailing which incidents that are to be reported, which information about the incidents that should be included in the reports, as well as the timeframe for reporting. The Regulations take into account the ENISA recommendation on reporting of incidents under Article 13a(3).

29. United Kingdom

The competent authority for the implementation of Article 13a is the independent regulator and competition authority for the UK communication industries (Ofcom).

29.1 Ensuring Provider measures to manage risks for networks and services

Article 13a/b requirements were introduced into UK law by new measures in Section 105A-D of the Communications Act 2003 which came into force on 25 May 2011, in line with revisions to the Electronic Communications Framework by the European Commission.

In relation to security, the Act includes the following:

105A.—(1) Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.

(2) Measures under subsection (1) must, in particular, include measures to prevent or minimise the impact of security incidents on end-users.

(3) Measures under subsection (1) taken by a network provider must also include measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks.

(5) In this section and sections 105B and 105C—

"network provider" means a provider of a public electronic communications network, and

"service provider" means a provider of a public electronic communications service.

Ofcom has enforcement powers including the power to issue binding instructions, conduct audits at the providers own cost, and levy fines.

In May 2011 Ofcom issued high level guidance on the new requirements for providers of public electronic communication networks and services to maintain security and resilience, and to report significant breaches or outages to Ofcom. The guidance was revised in Feb 2012 and most recently in Aug 2014. The revisions reflect the developments which have occurred since the new rules came into force, such as:

Member State coordination activity facilitated by ENISA has led to a series of increasingly mature documents which provide guidance on assessing compliance with various elements of Art 13a. The updates to Ofcom's own guidance reflect the output of this work and reference these documents extensively.

- Changes in Ofcom's and the industry's maturity and understanding of these issues since the new obligations and powers came into force.
- Changes in the threat landscape and the technology used by communications companies since 2011.
- Some specific examples of changes in the most recent version of the guidance include:
- Rewriting and restructuring to simplify the document and highlight key points
- Revised reporting arrangements and revised thresholds for "significant incidents"
- Guidance on new specific security issues, such as outsourcing of key network functions to third parties.
- Ofcom expects to keep the guidance under regular review and continue to update it as required.

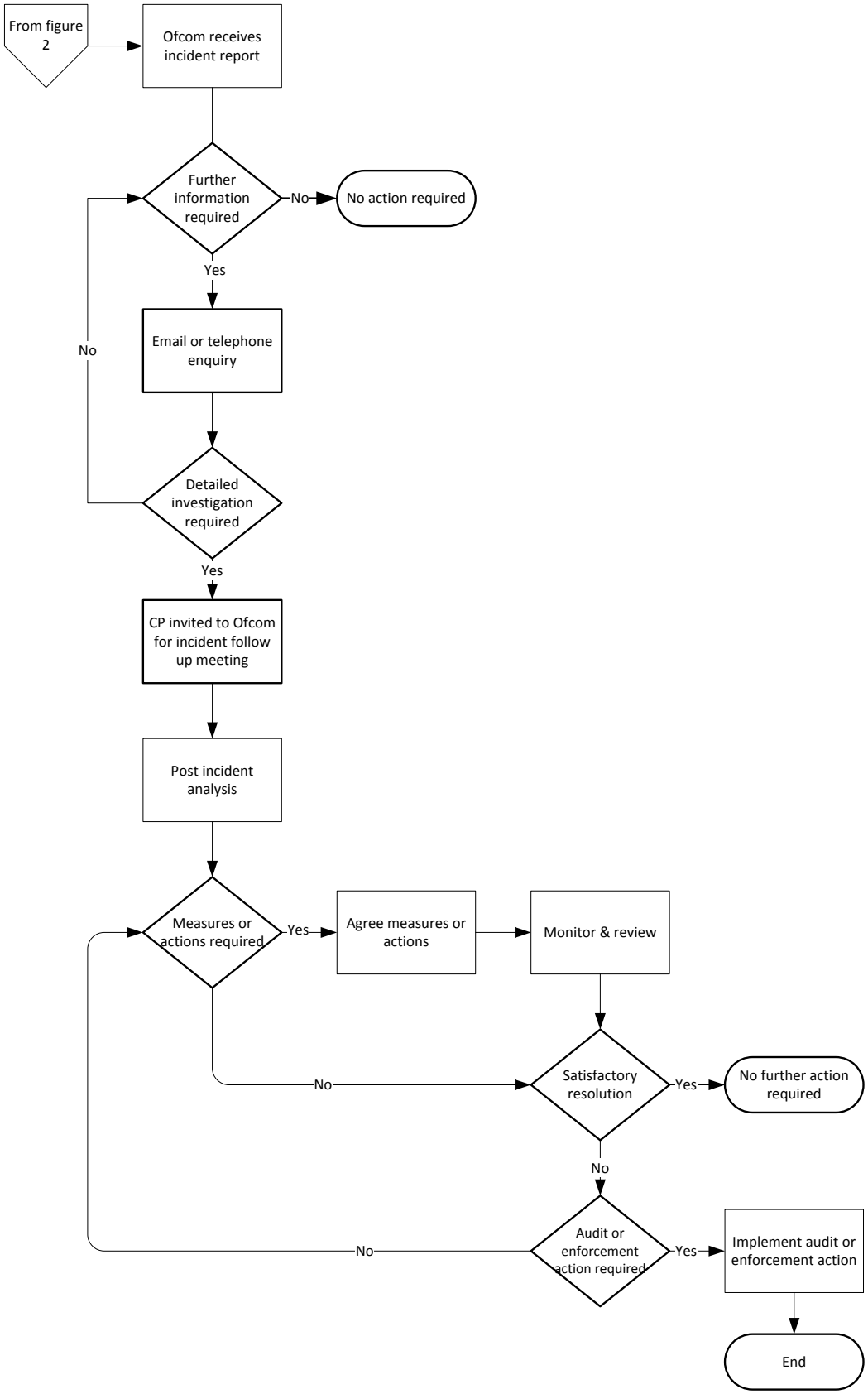
As indicated in Article 13a itself, risk management is a key tool in managing security and this is reflected in our guidance to providers and our dealings with them. When investigating a potential security concern we will typically ask the provider involved for evidence of a suitable risk assessment and risk mitigation plan at an early stage. If we are not satisfied with the response this would be a possible trigger for undertaking a security audit using our corresponding powers. If an improvement plan is required we will monitor the execution of this, for example to ensure any further risk mitigation is undertaken.

Investigations can be triggered by a range of events such as:

- A “significant incident” report submitted by the provider in question
- A “significant incident” report submitted by another provider
- An incident that comes to our attention through another route, such as a customer complaint directly to us, media reporting and so on
- A security concern that comes to our attention even though it has not yet resulted in an incident
- A cross-industry investigation of a specific security issue or concern. In this case we may not have any particular concern about a given provider but would instead be looking across a number of providers to understand how they each manage a particular security risk.

The incident follow-up process is illustrated in the Ofcom guidance by the following figure.

Figure 1: Incident follow-up process



Beyond the specific actions taken in relation to Art 13a, many CPs already have plans in place to ensure that their networks and services operate with an appropriate degree of resilience. In some cases, customers may have service level agreements with their providers, setting out the minimum level of service they expect, including security measures. For many companies, this focus on security represents a very significant investment. It may culminate, for example, in certification against key security standards. Ofcom will look for evidence of external audit of security arrangements, such as those represented by security standard certification.

29.2 Ensuring integrity of networks for continuity of supply of services

Much of the commentary in 28.1 applies here also as we deal with all parts of Art 13a/b under one umbrella within Ofcom. This includes issuing a single guidance document covering all three aspects.

In relation to integrity and supply, the Act includes the following:

(4) A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network. (5) In this section and sections 105B and 105C—

"network provider" means a provider of a public electronic communications network, and

"service provider" means a provider of a public electronic communications service.

Ofcom has enforcement powers including the power to issue binding instructions, conduct audits at the providers own cost, and levy fines.

Beyond the specific actions taken in relation to Article 13a, many CPs already have plans in place to ensure that their networks and services operate with an appropriate degree of resilience. In some cases, customers may have service level agreements with their providers, setting out the minimum level of service they expect, including availability measures. For many companies, this focus on resilience represents a very significant investment. It may culminate, for example, in certification against key security standards. In addition to this individual activity, there already exists cross-industry collaboration, such as through the Electronic Communications Resilience and Response Group (EC-RRG), aimed at continuing to improve performance across these areas.

EC-RRG deals with cross-sector planning for key risks to resilience. For example it coordinates the participation of the telecoms sector in resilience exercises conducted by other sectors. It also studies specific threats such a fuel supply problems.

EC-RRG maintains and operates a process for coordination between communications providers, Government, the regulator and other relevant parties during the response to major incidents which threaten resilience.

29.3 Measures in place to ensure incident reporting by Provider to NRA

Much of the commentary in 28.1 applies here also as we deal with all parts of Art 13a/b under one umbrella within Ofcom. This includes issuing a single guidance document covering all three aspects. Particular, the guidance contains detail on the incident reporting process.

In relation to reporting, the Act includes the following:

105B.—(1) A network provider must notify OFCOM—

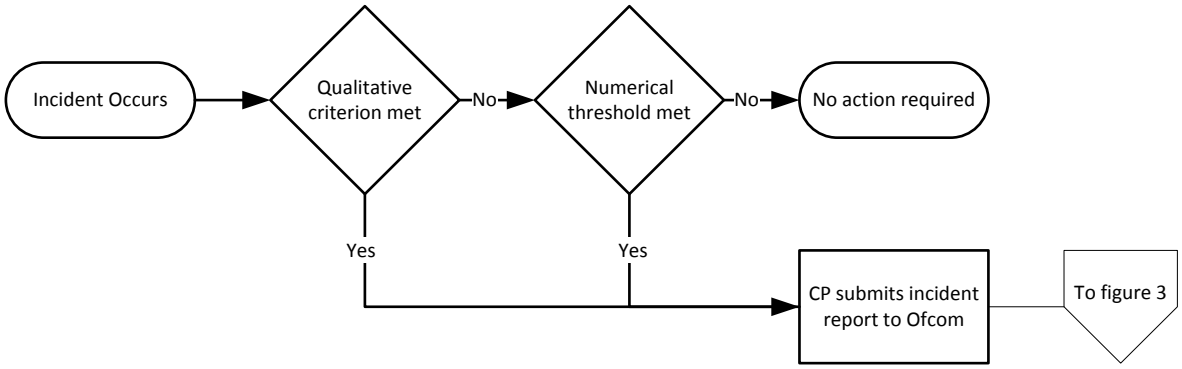
(a) of a breach of security which has a significant impact on the operation of a public electronic communications network, and'

(b) of a reduction in the availability of a public electronic communications network which has a significant impact on the network.

(2) A service provider must notify OFCOM of a breach of security which has a significant impact on the operation of a public electronic communications service.

The overall reporting process is summarised in the following diagram:

Figure 2: Overal reporting process



The qualitative criteria for deciding whether an incident should be reported are:

i) General

- Any incidents reported to other Government agencies or departments.
- Any incidents that CPs are aware of being reported in the media (local, national or trade news sources).

ii) Repeat incidents

- Repeat incidents are considered to be those which reoccur within four weeks, or are separate incidents affecting the same services in the same areas over a four week period.
- For repeat incidents, the CP should combine the impacts of the individual incidents in determining whether they meet the numerical thresholds.

iii) Outages affecting the ability of the customer to contact the emergency services

- Any incident affecting central services involved in connecting emergency calls (e.g. Call Handling Agent platforms, emergency call routing etc.) and leading to a reduction in the usual ability to answer or correctly route calls.
- Any incident that the CP is aware of that has a link to a potential loss of life.

The quantitative thresholds vary by service type, but by way of example for fixed network services:

NETWORK/SERVICE TYPE	MINIMUM NUMBER OF END CUSTOMERS AFFECTED	MINIMUM DURATION OF SERVICE LOSS OR MAJOR DISRUPTION
Fixed network providing access to the emergency services	1,000	1 hour
Fixed network providing access to the emergency services	100,000	Any duration
Fixed voice or data service/network offered to retail customers	10,000 or 25%	8 hours
Fixed voice or data service/network offered to retail customers	100,000	1 hour

The incident follow-up process outlined in 28.1 is used as appropriate in response to incident reports.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu