enisa

European Network and Information Security Agency

Implementation of article 15

of the draft regulation on electronic identification and trusted services for electronic transactions in the internal market

Contributors to this report

This study has been written by the team of IDC CEMA under guidance and supervision of ENISA. In particular, the following experts have contributed to the report:

- Joshua Budd – ICD CEMA
- Jachym Homola – IDC CEMA
- Matthew Marden – IDC CEMA
- Clara Galan – ENISA
- Sławomir Górniak – ENISA

Agreements or Acknowledgements

We would like to thank all the stakeholders from EU Member States as well as non-Member States who provided their feedback for this report in the form of returned discussion guides and/or subsequent interviews. We very much appreciate the active involvement of the Forum of European Supervisory Authorities for Electronic Signatures – FESA as well as all the participating national authorities, including:

- Bundesbeaufragte für den Datenschutz und Informationsfreiheit/Federal Commissioner for Data Protection and Freedom of Information (Germany)
- Bundesnetzagentur/Federal Network Agency (Germany)
- Nemzeti Média- és Hírközlési Hatóság/National Media and Infocommunications Authority (Hungary)
- Neytendastofa/Consumer Agency (Iceland)
- Ryšių reguliavimo tarnyba/Communications Regulatory Authority (Lithuania)
- Onafhankelijke Post en Telecom Autoriteit/Independent Post and Telecommunications Authority (the Netherlands)
- Agencia Española de Protección de Datos/Data Protection Authority (Spain)
- Post- och telestyrelsen/Post and Telecom Authority (Sweden)

Last but not least we would like to thank Mr. Jos Dumortier and Mr. Niels Vandezande, legal experts from the Interdisciplinary Centre for Law and ICT of the KU Leuven, Belgium, who were consulted on the feasibility of the implementation of Article 15.

Published: December 2012

About ENISA

The European Network and Information Security Agency (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 details

For contacting ENISA or for general enquiries on the Security Services and Data Protection area in ENISA, please use the following details:

- E-mail: sta@enisa.europa.eu
- Internet: http://www.enisa.europa.eu
- Follow us on Facebook Twitter LinkedIn Youtube & RSS feeds

For questions related to this report, please use the following details:

- E-mail: Slawomir.Gorniak@enisa.europa.eu

Legal notice

Contents

Table of figures

1 Executive Summary

E-Government services have significant potential to make public services more efficient for the benefit of citizens and businesses in terms of time and money. And while these benefits are increasingly being felt nationally, e-Government services still face administrative and legal barriers on a cross-border level, although pan-European projects like STORK have shown that technical issues of interoperability of electronic identifications can be overcome. In order to remove existing barriers for cross-border e-ID based services the European Commission has proposed a **draft regulation on electronic identification and trust services for electronic transactions in the internal market**, which will replace the existing Electronic Signature Directive 1999/93/EC.

Article 15 of the proposed regulation requires that trust service providers have to undertake extensive security measures and notify competent bodies of any breach of security and loss of integrity with significant impact on the trust service provided and on personal data maintained therein.

EU Member States have already largely implemented notification regimes for loss of integrity and breach of security impacting the operation of public telecommunications networks and services (**Article 13a of the revised Framework Directive**) as well as breaches of personal data (**Article 4 of the revised e-Privacy Directive**). The EC has also proposed a comprehensive **reform of general data protection rules**, which will extend the notification obligation to sectors other than telecommunications.

As there are synergies between the existing notification schemes and the regime proposed under Article 15, it is important, when preparing for the implementation of this article, to **make use of existing schemes as a reference.** Analysis of ENISA recommendations and guidelines on the implementation of Article 13a and Article 4 reveals many commonalities that can be applied to implementing Article 15. When drafting Article 15, the EC applied the Article 13a model almost in its entirety. Article 4 may also serve as a model for content-related aspects of breaches.

The similarities between these articles also derive from the fact that a personal data (or e-identification) breach may occur in the context of an information security incident. That is why close cooperation of relevant supervisory authorities is needed. At the same time, supervisory authorities need to consider adequate **media policies** in order to distribute information about serious incidents or to counter rumours and panic.

As the nature of incidents (despite the premise of technology neutrality of the regulation) and their scope notified under Article 15 evolve, it will be important to **manage and update the notification scheme** accordingly. The reviews should be done both nationally (involving all the relevant stakeholders, including trust service providers) and on a European level. **Annual reports on breaches provided to ENISA and the European Commission and their analysis by ENISA could be the main source for reviews of the notification scheme**. The inputs gathered from these reviews should be

further discussed at respective fora, such as FESA, to identify best practices in notifying breaches under Article 15, and address the main problems in its implementation.

2 Introduction

2.1 Background information

EU Member States have long recognised the benefits of new electronic services for citizens and businesses. The main reason for introducing these services was the need to achieve higher efficiency and performance of public administrations, better accessibility and user-friendliness and, most importantly, cost effectiveness. In order for these services to provide the mentioned benefits, it is important that they are based on seamlessly functioning and secure electronic signatures and electronic identification (e-ID) schemes.

The first important step on the European level in this area was taken with the introduction of **eSignatures Directive (1999/93/EC)**[1], which has brought a degree of harmonisation to practices on electronic signatures across Europe. All Member States have transposed the directive into their frameworks for eSignatures. But while there is widespread use of electronic identities[2] for commercial services, such as online shopping, the respective benefits are to a significantly smaller degree achieved with public services, and especially public services involving cross-border interactions.[3]

After having assessed the shortcomings of the directive, the European Commission (EC) came up with a proposal in June 2012 for a **Regulation on electronic identification and trusted services for electronic transactions in the internal market**[4]. The proposed Regulation will ensure citizens and businesses can use their electronic identities to access public services (education, health, tax declarations, notification of a marriage or move in/to another Member State, public tenders etc.) in other Member States. It also creates an internal market for electronic signatures and related online trust services across borders, by ensuring these services will work across borders and have the same legal status as traditional paper-based processes.

In its **Article 15** the EC proposes that trust services providers have to demonstrate due diligence, in relation to the identification of risks and adoption of appropriate security practices, and notify competent bodies of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein (for more details see the box below). When drafting this article, the EC was strongly influenced by notification procedures for **Article 13a** (relating to security and integrity of public electronic networks and services) of the **amended**

[1] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF*

[2] *For details of the concept of electronic identities see the relevant report of ENISA: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/mami*

[3] *The e-Government services based on electronic identification with solid potential for cross-border deployment include for example online education courses and other social services, e-Procurement and e-Health.*

[4] *http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm*

Framework Directive 2002/21/EC[5] and to some degree also by **Article 4** (relating to breaches of personal data) of the **amended e-Privacy Directive (2002/58/EC)**[6]. Similar measures on security and data breach notifications are to be included (**Articles 30, 31 and 32** of the current wording) in the proposed **regulation on data protection**[7], which extends the notification obligations from telecommunications to other sectors as well.

ARTICLE 15 MAIN POINTS: ***Security requirements applicable to trust service providers (main points)***	
1. ... In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents. **2.** Trust service providers shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein. Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in other Member States and the European Network and Information Security Agency (ENISA). The supervisory body concerned may also inform the public or require the trust service provider to do so, where it determines that disclosure of the breach is in the public interest.	**3.** The supervisory body shall provide to ENISA and to the Commission once a year with a summary of breach notifications received from trust service providers. **4.** In order to implement paragraphs 1 and 2, the competent supervisory body shall have the power to issue binding instructions to trust service providers. **5.** The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the further specification of the measures referred to in paragraph 1. **6.** The Commission may, by means of implementing acts, define the circumstances, formats and procedures, including deadlines, applicable for the purpose of paragraphs 1 to 3.

ENISA has been engaged in the area of reporting security breaches for a number of years. It helps Member States with the implementation of Article 13a of the Framework Directive as well as with

[5] *http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf*

[6] *http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf*

[7] *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

implementation of Article 4 of the e-Privacy Directive. For this purpose ENISA has engaged in collaborative working arrangements with national regulatory and data protection authorities, the European Commission and the European Data Protection Supervisor (EDPS) and produced a number of reports with recommendations on modalities of security breaches notifications. For more details see 2.2.1.

2.1.1 Aim of this report

The aim of this report is to produce an analysis including recommendations on how to implement security-related provisions of the draft of the regulation on electronic identification and trusted services for electronic transactions in the internal market, specifically Article 15 (Security requirements applicable to trust service providers) and Article 8 (Coordination). At the same time, an accompanying objective is to assess the feasibility of the implementation of Article 15.

The proposed recommendations take utmost account of and combine existing relevant ENISA studies in the areas of:

- implementation of Article 13a of the Framework Directive;
- advising the competent authorities in EU Member States on the implementation of the Article 4 of the ePrivacy directive[8].

Also, account is taken of the mechanisms proposed in the draft regulation on data protection.

The report is addressed to relevant decision makers and competent authorities in Member States in the area of electronic identification and trusted services.

It should be noted, that apart from this ENISA report, the EC has tendered an extensive study on the topic of electronic identification and trust services in Europe, which will include legal and technical input for secondary legislation (implementing acts) relating to the draft regulation.[9]

---

[8] *Documents relating to the Article 13a can be found at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting, while those relating to the Article 4 at http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn.*

[9] *For more details see http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=8363. The other objectives of the study are to monitor the take-up of electronic identification and trust services in Europe including e-signatures and propose communication and awareness raising activities to promote the uptake of trust services in EU.*

2.1.2 Definitions and the context of trust service providers

2.1.2.1 Definitions

For the purpose of clarity, it is important to specify a number of key definitions in this report. Key definitions are outlined below. They are mainly taken from the EU legislative documents mentioned in 2.1. and Annex I: References.

- ***Electronic identification:*** a process of using person identification data in electronic form unambiguously representing a natural or legal person.
- ***Electronic signature:*** data in electronic form which are attached to or logically associated with other electronic data and which are used by the signatory to sign.
- ***Personal data breach***: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.
- ***Security breach:*** Breaches in (information) security can be defined as a reduction in one or more of the three features of the CIA security concept: confidentiality, integrity, and availability.
- ***Trust service****:* any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.
- ***Trust service provider****:* a natural or a legal person who provides one or more trust services. 'Qualified Trust service provider' means a trust service provider who meets the requirements laid down in the regulation.

2.1.2.2 Context of trust service providers

As the notification requirements under Article 15 will apply to trust service providers (unlike telecom providers and network operators in Articles 13a and 4), it is important to characterize these stakeholders in more detail. The term "trust service provider" has not been formally defined yet in Member States. Currently, only certification service providers (CSP) are defined in the context of the e-Signature Directive 1999/93/EC.

The common feature of the trust service providers is that they provide digital certificates which are used for electronic identification and for other related services aimed to provide authenticity, integrity and non-repudiation to electronic transactions. Apart from electronic (digital) signatures these entities often provide other trust services such as time stamps or electronic seals (for a more comprehensive list of trust services, see the definition for "Trust service" above in the Definitions section).

Qualified trust service providers would roughly correspond to accredited CSPs. For example, qualified trust service providers may issue qualified certificates for qualified electronic signatures, which have the equivalent legal effects of a handwritten signature. Article 19 of the Regulation sets out the requirements the qualified trust service providers issuing qualified certificates must meet in order to be recognised as such by supervisory authorities. It draws on Annex II of Directive 1999/93/EC. The number of these providers varies significantly across the Member States. For example, in Germany, there are 14 accredited CSPs, while in other countries there are fewer or none registered at all.[10] CSPs are not a very homogenous group. They include companies specialized in the subject of certification and electronic signatures, but they also encompass businesses, whose core activities lie elsewhere and with certification and trust services they try to offer value-added services to the benefits of their clients. Examples range from telecoms service providers, to banks and other financial institutions, universities, national postal services or notary chambers to public administration institutions. Apart from qualified trust service providers there are also many providers who issue non-qualified certificates for their organisations and their clients. These providers are not, unlike CSPs, obliged to notify the supervisory authority that they issue digital certificates.

Article 15 makes breach notification compulsory for all trust service providers, both qualified and non-qualified. It is also necessary to specify the character of *breaches* falling *under the scope of Article 15*. One of the more prominent breaches of this nature that has taken place so far involved DigiNotar – a certification authority in the Netherlands. Over the summer of 2011, Diginotar was subject of a large security breach, allowing attackers to generate fake PKI certificates.[11] The fake certificates, the results of the breach, were used to wiretap the online communication of hundreds of thousands of Iranian citizens. Following the breach, many government websites in the Netherlands were offline and declared unsafe to visit. The government took over the operational management of DigiNotar‘s systems and the company itself was declared bankrupt soon afterwards. The example illustrates the nature of one of the most severe types of loss of integrity: a compromise of a certification authority. Also, the compromise of the private key of any type of digital certificate implies immediate revocation of the affected certificate.

Malicious attacks can impact all types of the above-mentioned trust services and involve a number of services, such as electronic signatures, time stamps and website authentication. Website authentication, which allows users to verify the authenticity of the website and link a legal person to the website, is becoming quite common.[12]

---

[10] *See an overview (not updated) in the Member States: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/index_en.htm*

[11] *More information on http://www.enisa.europa.eu/media/news-items/operation-black-tulip.*

[12] *If the website address becomes green in the web browser, it suggests that the website is authenticated with a certificate.*

Beside the malicious hacker attacks, which are featured most in the media, other root causes of breaches affecting trust services and personal data may include:

- Loss of IT equipment (misplaced or stolen equipment) like laptops or USB sticks;
- Technical error – unforseen complication in an IT system exposing data to outside parties, hardware or software failure;
- Human error – internally caused (misconfiguration or erroneous application of procedures)
- Third party failure like faults in the supply chain.

2.2 Methodology

In line with the objectives of the report, an utmost account was taken of ENISA's work related to notifications based on Article 13a of the Framework Directive and Article 4 of the ePrivacy Directive. Additional desk research was carried out on regulatory and voluntary schemes of reporting and notifications to competent national authorities in the EU and other countries. Several aspects of the report were consulted with stakeholders, especially national regulatory and data protection authorities in the EU Member States.

2.2.1 Analysis of existing ENISA documents and status of national reporting schemes in the area of eID and trust services

ENISA has published a number of reports on the implementation of reporting obligations based on above-mentioned Article 13a and Article 4. These reports were analyzed with the aim to identify "common ground" with Article 15 of the draft regulation on electronic identification and trust services, so that previously developed guidelines and recommendations can be utilized to the biggest extent possible.

The following ENISA studies were primarily utilized for this report:

- ***Good Practice on Reporting Security Incidents*** **(December 2009)** – analysis of the situation in Member States regarding Article 13a notifications three years ago, at the moment of which the revised EU directive had not been transposed yet in the majority of Member States. This resembles the current state of notification under the proposed regulation as there is relatively little experience with notifications under the Article 15 of the proposed regulation on electronic identification and trust services.
- ***Technical Guideline on Reporting Incidents*** **(December 2011)** is less theoretical than the previous document and provides concrete recommendations on individual thresholds and their combination for triggering reporting scheme as well as on content of the notifications and reporting template. It is the key document, on which recommendations for implementation of Article 15 can be modelled.

- ***Annual Incident Reports 2011*** **(October 2012)** provides a summary of the first set of annual incident reports under Article 13a delivered from Member States and compiled by ENISA. The report brings details on affected services, root causes or duration of incidents. At the end of the document there are suggestions for revision of some of the existing recommendations (elaborated in the framework of the above-mentioned Technical Guideline), which are further discussed in the Article 13a Working Group.[13]
- ***Data Breach Notifications in the EU (January 2011)*** was an early stock-taking exercise among telecommunication providers and supervisory authorities on the current situation regarding notifications under Article 4. It includes recommendations and best practices on risk assessment, notification thresholds or procedures.

- ***Recommendations on Technical Implementation Guidelines of Article 4*** **(April 2012)** includes a practical and usable description of a data breach, and in particular its relation to the definition of an "information security incident", criteria for determining a data breach, identification and assessment of security controls that affect determination of a breach, identification and assessment of risks of data breaches and procedures of notifications about data breaches in both private and public sector, including online processing of data breaches, definition of "undue delay" etc. The recommendations were developed by an expert group comprising data protection authorities of the Article 29 Working Group, European institutions like EC and EDPS as well industry players.[14] The added value of this document is its complexity as it takes account of the proposed general data protection regulation and addresses all personal data breaches. The proposed recommendations could thus be applied not only by telecommunication service providers but by data controllers in other sectors as well.

- ***Cyber Security Reporting in the EU*** **(August 2012)** provides an overview of existing and planned legislation covering the mandatory incident reporting clauses in Article 13a of the revised Framework Directive and Article 4 of the revised e-Privacy Directive, the proposed e-ID regulation's Article 15, and Articles 30, 31, 32 of the Data Protection reform. The study shows common factors and differences between the articles and looks ahead to the EU cyber security strategy. The paper also identifies areas for improvement.

Specific features of the ENISA documents above, which were utilized for the analysis in this report, are described in more detail in the section 3. Beside these documents, also ENISA and European Commission websites related to the topics of electronic identification and notification of security

---

[13] *The Working Group was established in 2010 and involves ENISA, policy-makers and NRAs from the Member States. Its aim is to facilitate a harmonized implementation of Article 13a. It meets (by means of teleconferences or worksiops) several times a year to share knowledge and exhchange views on addressing incidents.*

[14] *The Article 29 Working Party was set up under the general Data Protection Directive 95/46/EC.*

breaches were utilized as well as websites of supervisory authorities in the Member States grouped in FESA – the Forum of European Supervisory Authorities for Electronic Signatures.[15]

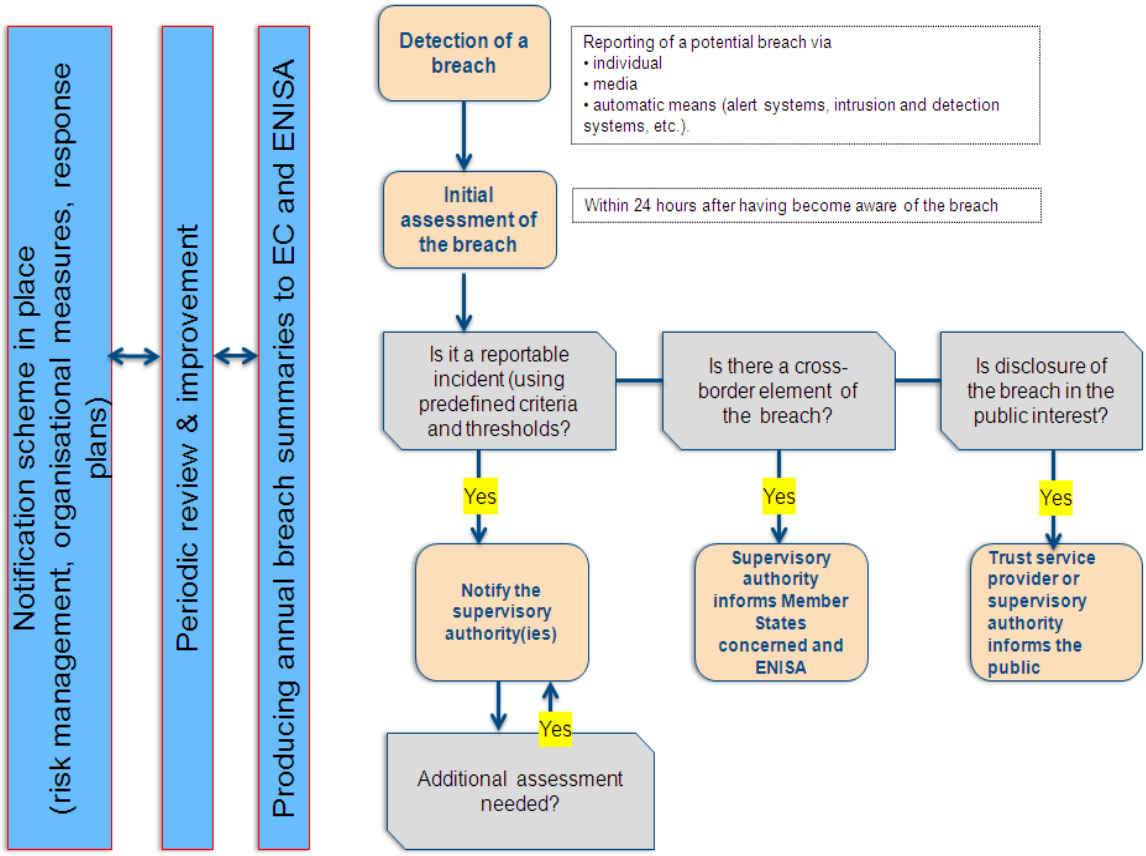
2.2.2 Validation of recommendations by relevant stakeholders

A questionnaire was developed for the collection of views of stakeholders – supervisory authorities - usually grouped in the FESA forum. The questionnaire focused on the following areas:

- existing legislation and schemes in the Member States regarding notifications of eID breaches;
- thresholds, procedures and other aspects of notifications;
- domestic cooperation (involvement of several stakeholders/authorities);
- cross-border cooperation (involvement of authorities from other Member States in case of incidents with cross-border impact and identification of best practices).

For the full version of the questionnaire see Annex IV: Questionnaire for the competent authorities. With a few stakeholders there was a follow-up in the form of a phone call used to elaborate on the inputs from the questionnaire.

[15] *FESA is a forum open to those bodies responsible for the operation of systems of supervision under the current Electronic Signature Directive 1999/93/EC. The objective of FESA is to support cooperation among these bodies and to develop common standpoints.*


Notification scheme in place (risk management, organisational measures, response plans)
Periodic review & improvement
Producing annual breach summaries to EC and ENISA
Detection of a breach
Reporting of a potential breach via
• individual
• media
• automatic means (alert systems, intrusion and detection systems, etc.).
Initial assessment of the breach
Within 24 hours after having become aware of the breach
Is it a reportable incident (using predefined criteria and thresholds?
Is there a cross-border element of the breach?
Is disclosure of the breach in the public interest?
Yes
Yes
Yes
Notify the supervisory authority(ies)
Supervisory authority informs Member States concerned and ENISA
Trust service provider or supervisory authority informs the public
Yes
Additional assessment needed?

3 Analysis of existing notification schemes

So far there has been very little experience in Member States regarding notification schemes proposed under Article 15 of the draft e-ID regulation. On the other hand, notifications are under way and first experiences are being collected as regards Article 13a and Article 4. Therefore, it is important to analyze existing reporting regimes, especially these based on Article 13a, which served as a model for drafting Article 15.

ENISA has collected information on the implementation of the respective notification articles and provided stakeholders with practical recommendations. In this chapter we first briefly describe the relevant notification articles, then display basic commonalities and differences and finally analyze to what extent the previous recommendations and guidelines are useful and relevant for the sake of Article 15.

3.1 Overview of existing articles on notification in EU legislation

For reference purposes we highlight the main points of the relevant security articles in EU legislation (apart from Article 15 covered already in the section 2.1) with the emphasis on breach/incident notifications including the draft regulation on data protection.

3.1.1 Article 13a of the revised Framework Directive

The revised Framework Directive in its Article 13a addresses notifications of incidents relating to security and integrity of public electronic communication networks and services. According to Article 13a:

- Telecommunications operators and service providers notify the competent National Regulatory Authorities (NRA) of a breach of security and loss of integrity with significant impact on the operation of network and services.
- Where appropriate, the national regulatory authorities should inform NRAs in other Member States and ENISA, when the incidents have a cross-border impact.
- When the disclosure of the incident is considered by NRAs to be in public interest, they may inform the public or urge the telecoms operators to do so.
- NRAs must provide ENISA and the EC with an annual summary report on notifications received and remedial actions taken.
- The EC may adopt further implementing measures, taking account of opinion of ENISA.

3.1.2 Article 4 of the e-Privacy Directive: Security of Processing

The revised e-Privacy Directive in its Article 4 addresses notifications of breaches of personal data and privacy related to the provision of electronic communications services. According to the Article 4:

- The telecommunications providers must, without undue delay, notify competent national authorities of a data breach.
- In case that a data breach may negatively impact privacy of individuals, the telecommunication providers must also notify data subjects of the breach, including possible remedies.
- The telecommunications providers need to maintain inventory of personal data breaches, which include information on the breaches, its effects and remedial actions taken.
- The EC may adopt further implementing measures taking account of opinions of ENISA, Article 29 Working Party and the EDPS.

3.1.3 Articles 30, 31 and 32 of the draft of the Data Protection Regulation

The EC has drafted a regulation to reform the current framework for data protection embodied by Directive 95/46/EC. The regulation extends the notification obligation to sectors other than telecommunications. Security measures and notification of breaches to supervisory authorities and data subjects is addressed in Articles 30, 31 and 32:

- Data controllers must without undue delay notify personal data breaches to supervisory authorities, and where feasible, not later than 24 hours after having become aware of it. If the notification is not made within this time frame, the data controllers have to provide justification.
- The data controllers also have, without undue delay, to notify data subjects (individuals) if the personal data breach is likely to impact their personal data and privacy.
- When the data controllers demonstrate to the satisfaction of supervisory authorities, that it has introduced appropriate security measures, notification will not be required.
- Compared to articles mentioned above this draft regulation is the most concrete on what should be included in the notification to the supervisory authority and data subjects.
- The EC may adopt further implementing measures.

3.2 Commonalities and differences of notification articles

In its report *Cyber Incident Reporting in the EU* ENISA provides a summary of all notification articles (including proposed e-ID and general data protection regulations) in EU law and draws conclusions on similarities and differences in these regimes. It also contains a figure showing information flows with reference to individual articles. The figure is reproduced below.

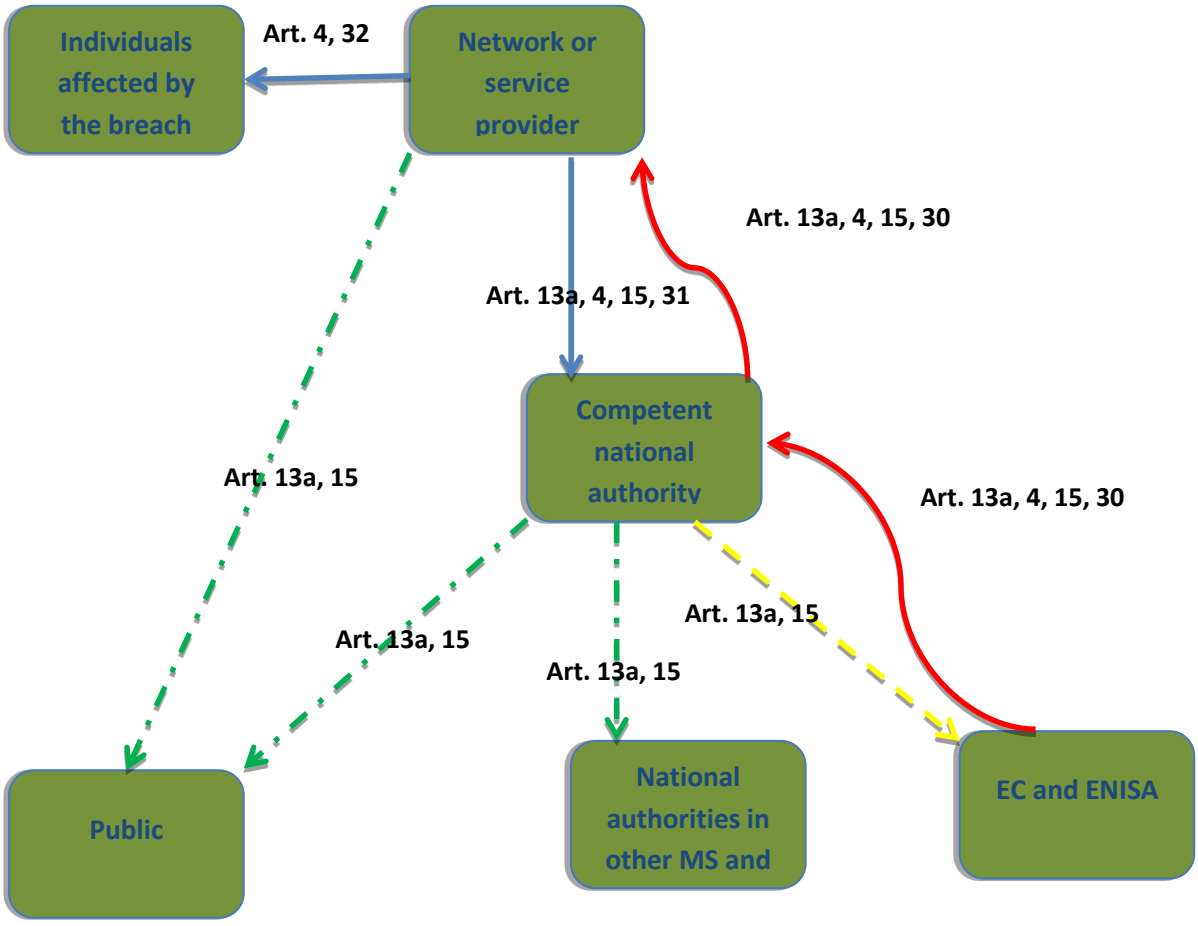


Figure 1: Commonalities and differences between security articles

Source: based on Cyber Incident Reporting in the EU, ENISA

Red curved arrows in the figure: Providers need to take appropriate security measures. For this purpose the supervisory authorities may carry out audits or require the providers to do a self-assessment. Based on the analysis of incidents and respective lessons learned, security measures may be adapted and recommendations proposed at the European level, so that the occurrence of incidents

is reduced or their impact mitigated. This approach is common for all notification articles discussed in this section.

Blue arrows in the figure: The providers notify competent supervisory authorities of the breach (common to all four articles discussed) and/or individuals affected (Article 4 and 32). The provider notifies competent national authorities and users affected by the breach (victims), which applies for Article 4 and 32.

Green dash-dotted arrows in the figure: In case of Articles 13a and 15 the supervisory authorities inform the public, if they establish that the disclosure of the breach is in the public interest. As an alternative, they may require providers to do so. When the breach has a cross-border impact, the supervisory authorities also inform their peers in the Member States concerned as well as EC and ENISA. This provision is valid for Article 13a and 15.

Yellow dashed arrows in the figure: Annually, the national supervisory authorities provide a summary of incident reports to EC and ENISA (again valid for Article 13a and 15). These inputs are important for measuring the effectiveness of EU legislation and its implementation across the EU. The lessons learned also serve the EC and ENISA for developing implementing measures and recommendations for a harmonized approach to cyber security benefitting businesses and citizens operating in the internal market.

As can be seen, Article 15 of the proposed regulation bears many resemblances to Article 13a relating to network security and integrity. But as the regulation also includes an important data protection component, it is crucial to analyze the relevance of notification schemes under Article 4. In the following sections we pick up the most relevant sections of ENISA documents relating to implementation of Article 13a and Article 4 and establish to what extent they are relevant for Article 15.

Relevance of previous ENISA notification guidelines with respect to Article 15

The notification requirement under Article 15 for trust service providers is closely linked to the notification requirements of Article 13a of the Framework Directive ("Article 13") and Article 4 of the ePrivacy Directive ("Article 4"), as well as the newly proposed EC regulation on data protection (2012/0011 (COD)). Thus, the frameworks and specific provisions regarding notification for Articles 13a and 4 should be examined in creating recommendations for implementing Article 15's requirements. ENISA has published several relevant works that provide analysis of and recommendations regarding notification requirements for Articles 13a and 4, which are listed above in section 2.2.1.

These studies should be leveraged in developing recommendations for implementing Article 15 to avoid unnecessary duplication of work and to reduce resistance from participants. Leveraging already existing processes can help ensure integration of new recommendations with wider National Emergency Management Plans, which can be an important determinant in the success of a particular recommendation and even the reporting scheme under Article 15 more broadly.

This section of the study will review the treatment of a number of topics pertaining to notification requirements in studies mentioned above. It will analyze the similarities and differences Article 15 and ongoing efforts to implement incident notification schemes of Article 13a and approach will help clarify which provisions of these recommendations should serve as a basis recommendations regarding the implementation of Article 15 for trust service providers.

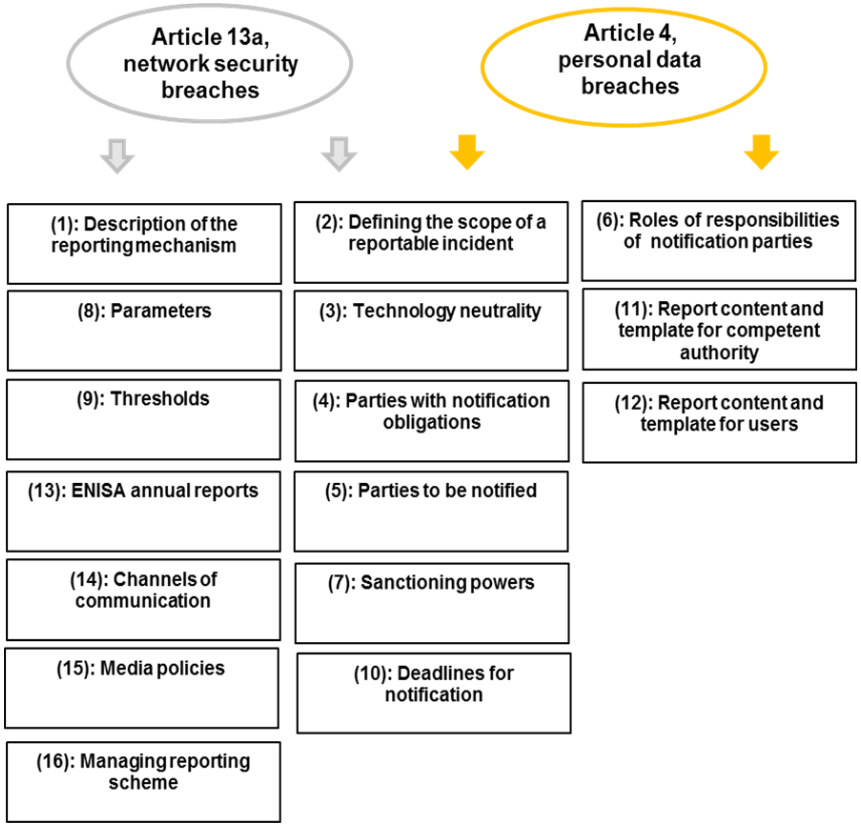


Figure 2 provides an overview of how ENISA recommendations for Article 13a and 4 were utilized for the purpose of implementation of Article 15. The boxes in the figure below include the description of the topic analysed and its corresponding number as outlined in the section below.

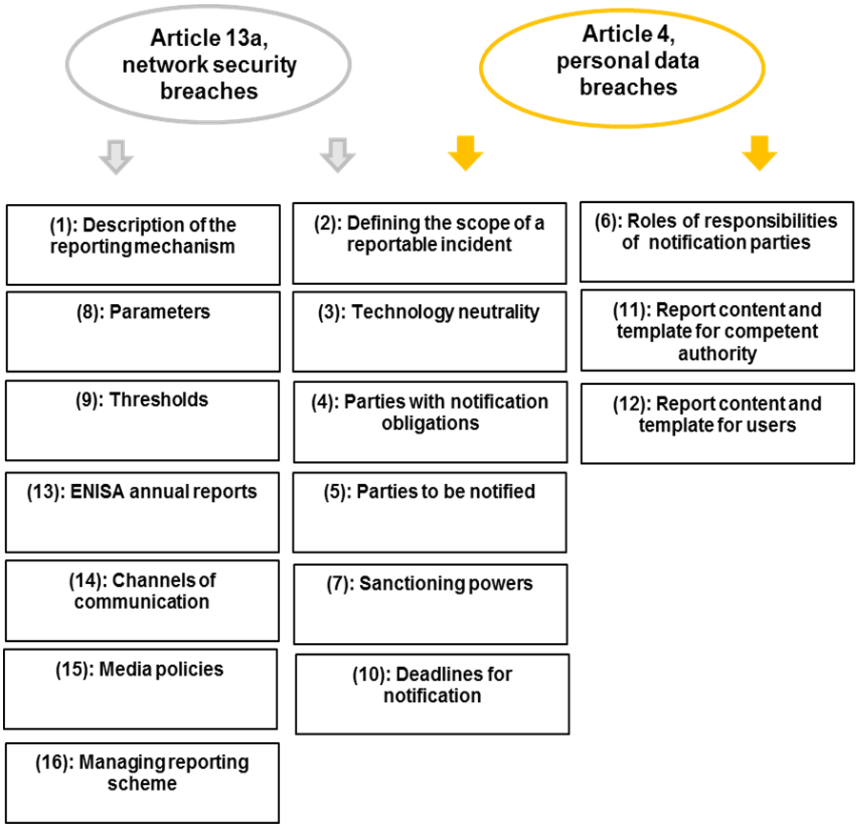


Figure 2: Use of existing recommendations for the implementation of Article 15

1. Description of the reporting mechanism

The reporting mechanism is the sum of agreed-upon rules, established procedures, and actions to be taken surrounding the reporting of a reportable incident by the relevant parties. The reporting mechanism is triggered when an incident occurs that meets the guidelines for when a party must report an incident to the competent authority(ies), its data subjects, and potentially other parties. In the *Technical Guideline on Reporting Incidents* study regarding the implementation of Article 13a for e-communications providers, the components of an "effective and efficient reporting scheme" were laid out. In particular, four aspects of a reporting mechanism were mentioned:

- Having a clear definition of the categories of root causes of an incident, and the reason why the incident occurred.
- The reporting template, the fields of which must be well defined and easily understood.
- The criteria/parameters taken into account when reporting an incident.
- The thresholds to be used to evaluate the significance of the incident and 'trigger' the reporting mechanism.

In addition, the same document discussed procedures for the reporting scheme and what the parties involved should take into account:

- Assess the impact of the incident; did it affect a service which is in the scope of e-communications providers and does the incident fall under the scope of the reporting?
- Determine if the incident is significant; according to the parameters and thresholds set, does this incident trigger the reporting scheme?
- Submit the report.

Article 13a of the Framework Directive covers e-communications providers and breaches that they experience, and e-communications providers have different customer relationships than the trust service providers covered under Article 15. Most significantly, trust service providers tend to be less “visible” to their customers than e-communications providers.

Nonetheless, circumstances in which a notification requirement would be triggered for e-communications providers and trust service providers are otherwise similar. There is nothing about the description of the reporting mechanism provided for Article 13a that suggests that a very similar description could not be used for Article 15. Like e-communications providers, trust service providers need a framework that offers a foundation for an efficient and effective system for reporting incidents. Moreover, trust service providers will be concerned with similar issues: determining what caused the security breach, minimizing the impact of the security breach, and being as discrete as possible about the occurrence of the security breach in the context of mandatory notification.

2. Defining the scope of a reportable incident

Determining the scope of what constitutes a reportable incident under Article 15 will be fundamental to the effectiveness of Article 15's reporting scheme. If the scope is too broad, then trust services providers will waste time and resources reporting incidents that have minimal or no actual impact on their customers and their personal data. If it is too narrow, then trust service providers might be able to avoid reporting impactful incidents which could cause the competent authority and ENISA to miss out on important information about security breaches. Article 13a and Article 4 both address how to define a reportable incident, but provide somewhat competing frameworks.

Article 13a calls for an e-communications provider to report a "breach of security or loss of integrity that has had a significant impact on the operation of networks or services." In the *Technical Guidelines on Reporting Incidents* report, this was further distilled to include "network and information security incidents having a significant impact on the continuity of supply of electronic communications networks or services." In preparing recommendations for Article 13a, both e-communications providers and competent authorities stressed that incident notification duties must not swamp their other responsibilities.

Meanwhile, Article 4 requires at least preliminary notification to the competent authority whenever a personal data breach occurs. Thus, under Article 4, the data breach is the reportable incident. The *Recommendations on Technical Implementation of Article 4* define a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."

Two elements of Article 13a's definition of a reportable incident could be challenging to implement with regard to Article 15. First, the recommendations for Article 13a define a reportable incident through the lens of the impact of the breach or loss of integrity on the operation of e-communications networks and services provided, which cannot be directly translated to trust services providers. Second, it does not define "breach of security" or "loss of integrity", which could make implementation challenging for trust service providers. On the other hand, Article 4 lays out explicitly when an incident report is required, which would provide more guidance to trust service providers trying to determine whether they must report a breach of security or loss of integrity to their competent authority. Breaches affecting trust services are specific because they may result in the loss of trust in the digital identity of a natural person or a legal entity.

Nevertheless; finding of a common acceptable definition has proven challenging among the competent authorities surveyed by ENISA. While a definition is proposed in this report, further discussions should be considered to resolve concerns about definitions. Areas that deserve particular attention include the very term “personal data” as well as the phrase “otherwise processed in connection with the provision of trust services”. Stakeholders consulted by ENISA stressed that there needs to be a provision addressing situations where there is a breach of security or loss of integrity but the disclosure, destruction, alteration, unavailability etc. of personal data is not (yet) determined.

This refers, for example, to a situation of the compromise of a private key of a certification authority. This would suppose a loss of integrity because the authority cannot be trusted anymore, but can later result (or not) in a breach of personal data, depending on the nature of the malicious operations performed by the attacker.

3. Technology neutrality

The European Commission and ENISA typically follow a policy of remaining technology neutral in terms of creating and adopting recommendations. From the perspective of these organizations, technology neutrality allows solutions to be implemented from all available technologies, and allows the organisations to avoid giving the perception that they favour a particular technology or vendor. The issue of technology neutrality is becoming more relevant as cloud services move into the mainstream and companies have more opportunities to make use of these cloud services in providing their services and in adhering to their notification obligations.

Articles 13a and 4 are both technology neutral in terms of the guidelines that were proposed for notification obligations. ENISA's recommendations for Article 4 specifically mention maintaining

technological neutrality as an objective, whereas those for Article 13a assume technological neutrality more implicitly as a baseline assumption rather than as an explicit goal.

With regard to imposing notification obligations on trust service providers, there is nothing about their services or activities which suggests that technological neutrality should be viewed differently than for Articles 13a or 4. Like e-communications providers, trust service providers use a variety of technologies and are sophisticated parties capable of choosing the technology best suiting them for fulfilling their obligations under Article 15. The need to observe the principles of technology neutrality is explicitly stated in the explanatory memorandum to the draft e-ID regulation with a reference to a rapid development of new technologies (especially online and mobile access).

4. Parties with incident reporting obligations

Before establishing procedures for trust service providers to follow for data breach notifications, Article 15 must provide clarity as to which parties will face reporting obligations under Article 15. Again, recommendations adopted for Articles 13a provide guidance.

In the *Good Practices Guide on Incident Reporting* for Article 13a, the requirements for parties that must bring reportable incidents to the attention of authorities were discussed with more specificity. Reporting obligations differed by the nature and size of the party:

- Large network operators must be involved in every kind of scheme.
- Smaller network operators may be excluded or charged with lesser reporting requirements.
- Key end-users should be reporting their problems for cyber-security reporting and critical information infrastructure protection.
- Key technology vendors might also be included.

Article 13a's recommendations are addressed specifically to e-communications providers, while Article 15 concerns trust service providers. As outlined in section 2.1.2, the term “trust service providers” is not yet common in the Member States. However, the term will largely correspond with certification service providers within the meaning of the e-Signature Directive 1999/93/EC. Notification obligations under Article 15 refer to all trust service providers without distinction between “qualified” and “non-qualified”. However, a balance needs to be struck between the scope of notifications of qualified trust service providers and “non-qualified” providers, due to their different legal framework.

5. Parties to be notified of a breach

Another important question that must be answered for Article 15 is: which parties must be notified of a reportable incident? For trust service providers, the scope of their notification requirement will affect the burden they experience from having to report an incident. Their burden will depend on factors such as the number of parties to which they must report notifications and frequency at which they must make such reports, as well as the impact on their relations with end users depending on how and when they must inform the public.

The *Recommendations on Technical Implementation of Article 4* looked directly at the issue of who must be informed of a reportable incident. Specifically, the report recommended requiring initial notification of the incident to the Member State's competent authority within 24 hours of the data controller becoming aware of it, with a follow-up detailed notification if it was determined that the incident had adverse effects. To the extent that a more detailed notification is required, Article 4 requires it to be provided within 7 days if the impact is serious, and within 15 days if the impact is determined to be less severe.

The *Good Practice Guide on Incident Reporting* also considers whether reporting obligations under Article 13(a) should extend to other parties such as: other participants in the scheme; stakeholders within the sector; national/governmental CERTs; regulators and authorities in other sectors affected by the incident; emergency services; other public authorities with emergency response or CIP capability, the eCommunications regulator, or the media. It recommends that duties to inform are strongest in emergency-response focused schemes, but that notification might be required legally or through obligations stemming from national crisis management teams. On the other hand, staff need to consider privacy expectations, business competition, and non-disclosure agreements before making decisions about whom to notify.

According to Article 15, the following national authorities should be notified of a breach: competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities. Depending on the security breach and its analysis, the relevant parties to be notified might include national/governmental CERTs. There was also a suggestion from an NRA consulted by ENISA for the purposes of this study that if the supervisory body is not part of the responsible ministry, the ministry or relevant section of the government with regulatory powers could be added.

However, despite the obligations stemming from the current wording of Article 15, some of the national stakeholders consulted by ENISA raised objections to involving data protection authorities in notifications in cases, where the breach has no effect on personal data. Instead, some stakeholders would opt for a model of a single point of contact, whereby the trust service providers notify only the competent supervisory authority.[16] In their opinion, the competent supervisory authority should decide which other national authorities and stakeholders need to be notified. It is not yet clear which authorities will be the main contact point, responsible for receiving notifications under Article 15. Often they may come from within FESA members, but NRAs who already manage notification schemes under Article 13a and 4 could be fit for this task.

6. Roles and responsibilities of parties involved in the notification process

[16] *The current wording of Article 15 seems to suggest that trust service providers should notify not only the competent supervisory body, but also other authorities including data protection authorities of breaches having a significant impact on the trust service provided and on the personal data maintained therein.*

To ensure that recommendations for implementing Article 15 are effective, it is important that the roles and responsibilities of each potential party involved in an incident that requires reporting are well defined. In the case of trust service providers, this means that trust service providers themselves, their customers (whether businesses or individuals), and the Member State's competent authority need to have an understanding of their roles.

In the *Implementation of Article 4* report, ENISA laid out the roles and responsibilities of generic parties to a data breach: the data controller, the individual, and the competent authority:

- Data Controller: perform risk management; implement appropriate technological and operational measures to prevent data breaches; develop procedures for responding to data breaches; detect the personal data breach; notify the competent authority or individuals without undue delay; identify the lessons learned and implement improvements; and maintain an inventory of data breaches.
- Competent Authority: Provide data controllers with clear guidelines regarding notification process; collect information about data breaches; specify and endorse appropriate technological measures; interact with data controllers after breaches; perform audits; maintain repository of data breaches notifications.
- Individuals: Notify the data controller and/or the competent authority if he/she/it detects a personal data breach; interact with the data controller and competent authority as needed; follow instructions from data controller and competent authority.

As with a number of other recommendations pertaining to the implementation of Article 4, they are relevant to the implementation of Article 15, although the fact that Article 15 pertains specifically to trust service providers may mean that they have to be tailored to trust service providers and the services they provide. The roles and responsibilities of additional parties that might have an interest in notification proceedings – including national/governmental CERTs – might need to be considered to ensure complete coverage of the types of parties that may have an interest in a particular report notification.

7. Supervisory authorities' power to sanction

In its current version, the European Commission proposal for a draft regulation on electronic identification and trust services for electronic transactions in the internal market has no provisions granting competent authorities the ability to sanction trust service providers for failing to adhere to notification requirements.

The benefits of granting sanctioning authority are clear; trust service providers are more likely to be diligent in their handling of notification incidents under the threat of sanctions. On the other hand, supervisory authorities risk upsetting their constituents if they use sanctioning authority frequently, which could ultimately backfire if trust service providers become unwilling participants in the incident notification scheme. Further, the question of which sanctions to permit competent authorities to impose must be resolved.

The subject of sanctioning power comes up in the *Data Breach Notification in the EU* report regarding Article 4, with discussion of the benefits and potential drawbacks to granting this power to supervisory authorities. Sentiment was split about the best type of sanction, with some authorities saying that financial penalties are the most effective tool for ensuring compliance, others saying that public pressure or blacklists are effective, and some extolling the virtues of creating positive incentives for data controller compliance. The report recognises that any recommendation at a European level might run up against contrary local laws or unwillingness on the part of local governments to provide national supervisory authorities with sanctioning power.

With regard to what types of remedies competent authorities should be able to adopt as sanctions, the *Data Breach Notifications in the EU* study for Article 4 recommends that competent authorities "consider a variety of deterrence measures, ranging from issuing fines to public exposure . . . as well as issuing awards and recognizing data controllers that demonstrate effective data breach notification procedures."

There is nothing inherently different about trust service providers compared to data controllers that should create more caution or enthusiasm about providing supervisory authorities with sanctioning powers. Article 9 (Liability) of the proposed regulation already states that trust service providers are liable for any direct damage caused to their clients. While using sanctions to ensure compliance is an option, authorities should consider other approaches and incentives. One supervisory authority consulted by ENISA indicated that the threat to trust services providers of losing their status as a qualified (trust service) provider is sufficient motivation for providers to comply with their security and notification obligations.

8. Parameters

Providing a framework for determining the importance of a trust service provider's reportable incident is fundamental to the effectiveness of the overall reporting scheme. Thus, Article 15 will be most effective if a framework is put in place that allows for consistency and clarity in weighing an incident's importance. As ENISA's interaction with stakeholders has shown, there is not enough clarity among them as to whether all breaches will have to be reported or rather those with "significant impact". For this reason it is important to set notification parameters and thresholds.

The *Technical Guideline on Reporting Incidents* report for Article 13a implementation provides a straightforward set of parameters that a competent authority should employ to determine the importance of a reported incident. This study names four parameters in particular:

- The number of users affected, which pertains to the percentage of a provider's customer base that is affected;[17]

[17] *However; in its analysis of incident reports from the Member State for 2011, ENISA questions the use of pecentage-based criterion and suggests that absolute numbers would better serve the purpose while ensuring that the reporting burden is*

- Duration of the incident;
- Geographic spread / region, which can be given different weights depending on the region;
- Impact on emergency calls, an incident that affects the continuity of these services will generally be considered to be more severe.

The fundamental differences between trust service providers and e-communications providers make it challenging to translate Article 13a's parameters directly to Article 15. For example, the provision in Article 13a regarding emergency calls is not relevant to Article 15. In addition, the geographic spread / region of an incident could be relevant to determining the significance of a reportable incident under Article 15, but only in combination with the intensity of the incident. For example, if a breach of security or loss of integrity occurs for several users of a trust service provider's services across Europe, the fact that the impact is geographically disperse can hardly be said to relate in a significant way to the seriousness of the breach. On the other hand, the number of users affected by a reportable incident under Article 15 would seem to provide information about the incident's nature, and the duration of the incident may indicate the trust service provider's ability to recognize and solve the problem, which also is a factor that could be considered in weighing the importance of a reportable incident affecting a trust services provider. Regarding recommendations on breach parameters, stakeholders surveyed by ENISA pointed out the need to align them with the respective exercise conducted by ENISA and the Article 29 WG as part of the data breach severity assessment.

9. Thresholds for notifying ENISA and other Member States

Determining when a competent authority must report an incident to ENISA or to a counterpart in a different country is also an important aspect of Article 15's framework.[18] Again, a balance must be struck between ensuring that sufficient and timely information flows between these parties so as to promote Article 15's objectives, and not burdening them with unnecessary work and information overload. There should be clarity surrounding what threshold should trigger a trust service provider's reporting requirement and mechanism.

---

proportional to the size of the country and NRA's resources. See page 16 of the report: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011.

[18] *According to Article 15 of the draft regulation, ENISA and EC are to be annually provided with a summary of breaches notified in the Member States.*

The topic of notification thresholds was explored with regard to notifying ENISA and other countries' competent authorities in *Technical Guideline on Reporting Incidents* report for Article 13a implementation. As a baseline matter, the standard for reporting an incident to ENISA was determined to be "every time the impact is equal to, or higher than, a set of predefined thresholds agreed between ENISA and the NRAs." It explained that the thresholds should serve as a minimum entry level for required notification, and every competent authority can then "impose stricter and more granular thresholds to trigger the reporting at national level," but that these thresholds should then also be used to trigger the process of reporting to ENISA.

The *Technical Guideline* recommendations also cover ad hoc notifications from competent national authority to competent national authority and to ENISA. It recommends that for cross-border incidents, the competent authority with knowledge of the incident inform the relevant authority in other Member States and ENISA. Meanwhile, when a significant incident occurs that affects another provider, the competent authority should also notify its counterpart in the other country and ENISA. The recommendations call for a list of relevant points to be exchanged to be published, which is to be distributed to stakeholders and periodically updated.

The baseline threshold for a competent authority to notify ENISA is as relevant for Article 15 as for Article 13a. It makes sense for individual country competent authorities to have a standard set of thresholds that they can consult, and develop an understanding of what they should report. On the other hand, cross-border incidents may be more common for trust service providers than for e-communications providers, suggesting that a blanket recommendation of informing ENISA and authorities in affected countries might be too broad. Likewise, a trust service provider is less likely than an e-communications services provider to discover that a significant incident is affecting another trust services provider, so this recommendation might be less applicable for trust services providers. In real terms, those incidents need to be notified under Article 15, where, for example, qualified certificates are issued also to citizens and businesses in other Member States. Also, compromises of certification authorities issuing certificates for website authentication should be notified on a broader cross-border level.

10. Deadlines for initial and follow-up reports

Deadlines for reporting incidents to competent authorities will be a necessary part of effectively implementing Article 15. Without deadlines, the risk exists that a trust services provider will fail to notify the competent authority in a timely manner, thereby raising the likelihood that further damaging incidents could occur, or that the competent authority will not have the information necessary to solve a problem. On the other hand, deadlines should take into account the fact that trust services providers must gather information, determine the severity of an incident, and take their own actions to counteract an incident, all while meeting notification deadlines.

The issue of deadlines is discussed in both the *Good Practices Guide on Incident Reporting* for Article 13a and the *Recommendations for the Technical Implementation of Article 4*. Both envision a tiered

approach for deadlines for data holders notifying their competent authorities and other relevant parties of a reportable incident. The recommendations for notification deadlines for Article 4 are more detailed, and deserve closer analysis. Under recommendations for Article 4, a data controller should:

(1) Make a ***preliminary notification*** of an incident to the competent authority ***without undue delay***, and ***within the range of 24 hours*** after it becomes aware of the data breach during which time it should have performed its initial assessment;

(2) Then make a ***detailed notification*** after performing further analysis of the data breach and determining the severity level more accurately and gaining information about the circumstances. For this stage, a flexible reporting deadline is proposed based upon the severity of the breach. For the most severe breaches with serious adverse effects, this detailed notification should be completed ***in less than seven days***, while detailed notifications for less serious incidents with few or no adverse effects should be completed ***within 15 days***.

In the *Good Practice Guide* for Article 13a, the recommendations also contemplate a concluding report and periodical summary reports, but specific deadlines for these types of reports are not mentioned.

The tiered approach with regard to reporting deadlines favoured for Article 4 should also be feasible for Article 15; like data controllers, trust service providers will need to take the time to fully assess a reportable incident after they become aware of it and then develop a more comprehensive overview of what occurred. Otherwise, there is no reason that trust service providers cannot meet the same deadlines for initial and more detailed notifications as other data controllers that experience breaches. However; there are specific obligations for trust service providers that highlight the critical nature of their services. For example, in the draft Regulation (Art.19) it is proposed that qualified trust service providers will obliged to include the status of any revoked certificates within ten minutes in their Certificate Revocation List (CRL).

11. Report content and template for supervisory authorities

Given that trust service providers will face requirements under Article 15 for when and to whom to report data breach incidents, it makes sense that they need an overview of the information that these reports should include and possibly even a template to make the process of reporting less burdensome.

The content that should go into a data breach notification and a suggested template are provided in the *Recommendations on Technical Implementation of Article 4* report. As a base matter, it states that "data controllers should notify the competent authorities of all relevant facts related to a personal data breach." While this is somewhat broad, the recommendations note that this is necessary to allow

the competent authority to do its job by identifying and analyzing trends and preparing concrete advice for all parties involved.

Further, the report highly recommends that a standardised reporting template be adopted across all Member State competent authorities that can be submitted electronically by data holders. By having a standardised form, data will be easily compared between Member States. Also the submission should be quicker and more straight-forward, which will tend to lead to submission of incident reports in a more timely and complete manner. The suggested template includes a number of data fields, ranging from basic information such as the identity of the reporting person, to the data and time when the data breach was established, to a short summary of the incident, to the results of the impact/severity assessment performed.

In addition to the *Recommendations on Technical Implementation of Article 4* report, the EC's draft regulation on general data protection provides a framework in Article 31(3) for what an incident notification to a competent authority should include. Specifically, the notification must at least:

- describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
- communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
- recommend measures to mitigate the possible adverse effects of the personal data breach;
- describe the consequences of the personal data breach; and
- describe the measures proposed or taken by the controller to address the personal data breach.

Trust service providers should include a baseline amount of common information in every incident report, as was recommended in Article 4 and in the EC's draft regulation on general data protection. Further, having a template – even if its use is not mandatory - would likely ease the reporting process, although any reporting template used for Article 13a or more generally for Article 4 would likely need to be adjusted somewhat to take into account the unique activities and customer relationships of trust service providers. Also, practically all national authorities surveyed by ENISA are in favour of using a single template for breach notifications.

In light of the above, the notification to be submitted by trust service providers should cover the following:

- describe the nature of the breach of security including the type of certificates (web authentication, time stamps, etc.) issued; number of affected certificates, etc.;

- communicate the identity and contact details of a contact point where more information can be obtained;
- recommend measures to mitigate the possible adverse effects of the breach;
- describe the consequences of the breach; and
- describe the measures proposed or taken by the trust service provider to address the breach.

12. Report content and template for users (certificate holders)

Trust service providers are not at this moment supposed to report incidents to their customers unlike the provisions in the e-Privacy Directive and the proposed Regulation on Data Protection. However, the current wording of the Article 15 may change in the course of debates. For example, EDPS has called for the alignment of Article 15 with the respective articles in the above mentioned EU regulations.[19] That is why, we address this topic here. Trust service providers may also feel the need to inform their customers of the breaches as part of their customer policies.

Recommendations on Technical Implementation of Article 4 suggest that data controllers notify individuals, "based on the likely adverse effects on the individuals and the appropriate technological measures in place." To the extent that notification is issued, certain information should be provided to the data subject: (1) information about the contact point with the data controller; (2) a description of the incident and what personal data has been compromised and how, in easy to understand language; and (3) what service the data controller is offering to mitigate the adverse effects and what the data holder can do itself to mitigate the impact. Further, other information such as the type of data compromised, the likely impact of the breach, the mitigation actions already put in place, and steps being put in place so as to avoid a repeat can also be provided if available.

The notification requirement should potentially differ by type of customer: there would seem to be more efficiency and need to inform customers such as enterprises and governmental bodies of breaches of security. To the extent that individuals are to be contacted, though, the general structure laid out for Article 4 and the EC's draft regulation on general data protection would also seem to make sense in the context of Article 15.

13. Use of annual reports by ENISA

The use of incident reports by ENISA will be important to the development of the framework for better protecting data held by trust services providers, as well as to learning from these trust service providers' experiences. This raises questions about how competent authorities should provide ENISA

[19] *http://www.pogowasright.org/?p=30783*

with useable data while also ensuring that ENISA does not inadvertently publish data that is confidential or proprietary or otherwise harmful to a trust service provider or a data holder.

The *Technical Guideline on Incident Reporting* for Article 13a includes an overview of what a Member State's competent authority should provide to ENISA, as well as a template for doing so. It calls on each Member State to provide to ENISA with a description of every major incident on an annual basis. It also includes a suggested template for use by competent authorities for providing ENISA with information about these incidents that includes baseline information such as the date and time of the incident, the impact of the incident, and steps taken after the incident to mitigate its impact, as well as a description of each field in the template. The recommendations for Article 13a also cite provisions in EU law that permit providers or competent authorities to claim confidentiality in the event business confidentiality or national security is put at risk by the release of information by ENISA.

The *Technical Guideline* report for Article 13a charges ENISA with drafting an annual report based on reports provided to it by Member States' competent authorities "on the status of electronic communications with regard to security, integrity and continuity of service." Further, ENISA should issue recommendations, advice, and good practices on incident collection, incident management, and preventive actions. Finally, ENISA should create statistical analysis series that will help to identify common threats, trends, and conclusions, among other things. In October 2012, ENISA issued the first annual report on incidents notified by Member States under Article 13a, while the report for incidents notified in 2012 will be published next spring. [20]

All parties involved in Article 15 – the trust service providers, competent authorities, and ENISA – will want to derive the maximum possible utility from the reporting of incidents, so the rationale behind Article 13a's treatment regarding ENISA's use of reports also applies in the context of Article 15. Logically, specific elements of the types of data that ENISA will collect under 13a that pertain directly to e-communications providers, such as "impact on emergency calls," and certain metrics such as "Interconnections affected," will not be relevant for trust services providers. Nevertheless, the information to be collected and ENISA's analysis can use experience gained from the Article 13a approach. It should be noted in this respect that the supervisory authorities will also need to gather information on their supervisory activities and on the national markets for trust services. The respective summaries (along with those relating to breach notifications received) will be submitted annually to EC and the Member States.

14. Channels of communications

This encompasses questions about technologies as well as whether a single point of contact should be established at the competent authority. Generally, competent authorities have indicated that they are

---

[20] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011*

willing to receive notifications in a number of different ways, recognizing that overly formalised or rigid requirements might not be in the best interest of the overall reporting mechanism.

The *Good Practice Guide* for Article 13a considers these questions. It does not make a specific recommendation with regard to channel of communication (phone, SMS, email, web-based forms, machine readable messages), but does stress that whatever channels a competent authority chooses must be well publicized with its constituency. It stresses that contact information should be readily accessible for anyone looking for it, and that competent authorities should consider making available user handbooks for more sophisticated reporting channels such as web-based tools or machine readable messages.

For quick alerts, the *Good Practice Guide* recommends that competent authorities invite these through any available channel, but that reports requiring an emergency response should employ a secure and resilient voice bridge, although other channels could still be employed for reporting. Further, the recommendations call for the establishment of a single point of contact because it allows the reporting party to focus its energy on resolving the problem rather than trying to determine how to report it. Finally, the *Good Practice Guide* calls on the competent authorities to support reporting parties in "developing standardized and systematic arrangements for cooperation and information distribution."

The issue of channels of communication to be used for incident reporting is not specific to the party reporting the incident, and the recommendations for 13a contain little that is directly specifically at e-communications providers. In fact, trust service providers will be focused on the same issues as e-communications providers in the event of an incident – determining what happened and how to resolve the incident. Therefore, ensuring that multiple channels of communication are open that are readily accessible would also fit into trust service providers reporting obligations under Article 15.

15. Media policies

Data breaches involving personal data often attract significant media attention. This suggests that competent authorities need to be prepared for media attention focused on reportable incidents involving trust service providers. Therefore, recommendations for Article 15 should address dealing with the media especially as the trust service providers may be obliged in some cases to inform the public of the breach, it the disclosure is in public interest.

The *Good Practice Guide* for Article 13a addressed media policies and put forward several recommendations for how competent authorities can work with the media and even use the media to their advantage. It recognised that there will be various situations in which competent authorities' staff is most likely to work with the media, including: (1) collecting information about incidents; (2) responding to media inquiries; (3) distributing information about incidents; and (4) raising awareness about threats.

With these situations in mind, the *Good Practice Guide* made three recommendations for competent authorities' media policies:

- Elaborate media policy and train/employ staff for answering media queries;
- Use media actively for distributing information about serious incidents or countering rumours and panic, and;
- Develop a long-term media strategy for continuous awareness raising.

The recommendations made with regard to media policies for Article 13a should be transferrable to Article 15 with only minor modifications. Some consideration should be given to the specific nature of trust services providers' activities, but in general competent authorities will deal with the media for similar types of matters for breaches involving trust services authorities as for e-communications providers. However, this will also depend on the target market of the trust service provider, as having strong media policies and communication strategies in place is more critical for trust service providers offering public web authentication certificates than for a governmental provider in charge of issuing internal electronic seals and/or time stamps.

16. Managing the Reporting Scheme

In addition to putting in place a solid framework and policies for guiding Article 15's implementation, it will also be important that the relevant parties, and especially the competent authorities and ENISA, monitor the implementation to improve upon it. Incidents must be monitored and evaluated to ensure that the right decisions are made regarding reactions, while the overall evolution of the framework will have to be managed.

Specifically, the *Good Practices Guide* for Article 13a takes a relatively comprehensive look at how to best manage its reporting scheme. At base, it recommends that "the organizers will need to introduce scheme management mechanisms ensuring that the scheme's objectives are met." It identifies three channels in particular that it sees as necessary to good management for competent authorities:

- To analyze incidents individually and follow up with the incident owners: In particular, the competent authorities should proactively approach their constituents to educate them about their findings.
- To evaluate incidents statistically and draw lessons: Providing useful statistical analysis is a way for the competent authority to build support for reporting requirements and to return value to its constituency and therefore provide incentives for full cooperation in incident reporting.
- To manage long-term evolution of the scheme: Competent authorities should continually strive to improve their schemes and to evolve it in line with changes to the industry or to extend it beyond its original boundaries.

It is important to consider having periodic reviews of the notification scheme. Nationally, such evaluations could be done by competent supervisory authorities as all information about security breaches will pass through them. The notification scheme should be stable for a meaningful period of

time. Further guidance from ENISA would be useful in the form of recommendations and collection of best practices for the implementation of Article 15, or even establishing a working group similar to Article 13a.

4 Summary of recommendations

This section provides recommendations for the implementation of Article 15 based on the topics analysed in the previous section. For easy reference, the recommendation topics are also presented in the same numbering order.

It is worth noting that all recommendations in this section are addressed to competent authorities in the EU and at the Member States. Nevertheless, it is possible (as was the case for Art13a and Art4) that ENISA will collaborate closely with the European Commission and competent authorities at MS level in order to put forward proposals for consideration by MS for many of the topics described in the sections below.

1. Description of the reporting mechanism

Recommendation: **Competent authorities** (to be identified) on the EU and at the Member State level need to lay out well defined reporting mechanisms to ensure that the reporting scheme is effective, bearing in mind that notification obligation will be quite new to trust service providers. This means providing trust service providers with a framework that permits them to report incidents efficiently and as a regular part of their activities. Specifically, competent authorities should ensure that they provide trust service providers with: (1) clear definitions of root causes of the incident; (2) a template with well-defined fields; (3) the criteria and parameters that the trust services provider should take into account when reporting an incident; and (4) the thresholds that should be used to evaluate the significance of the incident.

Trust services providers, through their management teams and incident response teams, should cooperate with their competent authorities in developing a reporting mechanism that is effective and efficient for them and the competent authority. They should give special care to identify issues that they are likely to face before putting a framework in place based on their experiences and input, with a special focus on the impact of incident reporting obligations on their resources and organisational structures.

2. Defining the scope of a reportable incident

Recommendation: Competent authorities of Member States should consider using the following definition or a definition close to the following for facilitating breach assessment on the national and EU level: ***A reportable breach*** under Article 15 is a breach of security and/or loss of integrity, which involves a compromise of electronic identity, and may lead to the accidental or unlawful destruction, loss, alteration, unavailability, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of trust services.

It should be emphasised, however, that the above definition needs to be discussed and potentially revised based on input from relevant stakeholders.

Further, competent authorities and trust service providers should cooperate to establish thresholds for reporting these breaches of security or loss of integrity in a way that is sensible and will not lead to over-reporting to an extent that will have a negative effect on the overall reporting mechanism. The wording of the Article 15 “significant impact on the trust service provided and on the personal data maintained therein”

supports the establishment of parameters for triggering the notification scheme.

3. Technology neutrality

Recommendation: Member State **competent authorities** should make explicit mention of the fact that they favour a policy of technological neutrality with regard to how trust service providers in their markets comply with reporting requirements and provide incident reports. **Trust service providers** should consider all types of technological solutions, which allow them to meet their incident reporting obligations in a timely and complete manner.

4. Parties with incident reporting obligations

Recommendation: **Competent authorities** should require at least initial notifications from all types and sizes of trust service providers in the event of a reportable incident. **Qualified trust service providers** should face more detailed notification obligations particularly with regard to the amount of information provided and deadlines for follow-up notifications.

Because reportable incidents impacting trust service providers are not often visible to their customers or the public, **competent authorities** should engage **trust service providers** and Member State **policymakers** to proactively discuss whether to expend resources on educating other parties such as end users, other government agencies, or telecom network services about reporting incidents involving trust services.

5. Parties to be notified of a breach

Recommendation: **Trust service providers** should be required to provide at least initial notification to their Member State's **competent authorities** for every data breach or loss of integrity that meets the definition of a reportable incident. Beyond this baseline reporting obligation, trust service providers should also provide notification based on the seriousness of the breach and the likely consequences of the breach to other actors such as competent national bodies for information security and other relevant third parties such as data protection authorities and possibly national/governmental CERTs. **Data subjects** should be notified if the incident involves personal data and is likely to have an adverse effect on them. Policymakers in the Member States and at EU level should work closely with **competent authorities** to provide guidelines to trust service providers of whom they must notify of breaches, with illustrative examples to help them determine how to fulfil their notification obligations.

Given Article 15's emphasis on creating a seamless trust services market across Europe, **competent authorities** should cooperate to make recommendations about when a trust services provider should make notifications to a competent authority in another Member State, with an emphasis on ensuring that pertinent information is shared with these bodies in a way that allows them to use it to mitigate the impact of the reportable incident on the affected parties.

6. Roles and responsibilities of parties involved in the notification process

Recommendation: The roles and responsibilities of the key parties to the incident reporting scheme under Article 15 for trust service providers – Member State competent authorities, trust service providers, and end users (certificate and data holders) – should all have clear guidelines regarding their roles and responsibilities. The task of ensuring that these roles and responsibilities are made clear must fit within the broader reporting mechanism. A Member State's **policymakers** are responsible for putting these roles and responsibilities in place, especially for the **competent authority**. In turn, the competent authority should cooperate with its **trust service**

provider constituency and other interested parties, including end users, national/governmental CERTs, industry groups, and competent authorities in other countries, to state the roles and responsibilities as clearly as possible.

The roles and responsibilities tasked to these parties should follow logically from their activities and status under Article 15's reporting scheme and include:

- Competent Authority: Provide trust service providers with clear guidelines regarding notification process; collect information about the security breach or loss of integrity; specify and endorse appropriate technological measures within the context of technology neutrality; interact with trust service providers after breaches; perform audits.
- Trust service providers: Perform risk management; implement appropriate technological and operational measures to prevent security breaches or loss of integrity; develop procedures for responding to breaches; detect a personal data breach; notify the competent authorities without undue delay; identify the lessons learned and implement improvements; and maintain an inventory of data breaches.
- End Users or Data Subjects: Interact with the trust service provider and competent authority as needed; follow instructions from the trust service provider and competent authorities, if necessary.
- Other national authorities: Offer their expertise where relevant and coordinate with the competent authority on the reporting scheme's implementation and execution.
- Other interested parties: Keep abreast of changes to the reporting scheme and offer their input on how to make the reporting scheme as efficient and useful as possible.

7. Supervisory authorities' power to sanction

Recommendation: Member State **policymakers** should give **competent authorities** sanctioning power as a means of ensuring compliance. Generally, sanctions that punish **trust service providers** should be used rather rarely and mainly for repeat violators or those that can be shown to have wilfully disregarded the rules regarding breach notification. Competent authorities should manage the use of their sanctioning power so as to not create an adversarial relationship with a **trust service provider** that could ultimately negatively affect the overall breach notification scheme.

Competent authorities should also try to create positive incentives for trust service providers to follow incident reporting guidelines. They should discuss what types of incentives might be effective with the trust service providers in their market, as well as with their counterparts in other Member States, or even other governmental bodies with experience in trying to reward parties for fulfilling their responsibilities under similar schemes. Another approach to consider is for competent authorities is to be proactive and make examples of successful providers, rather than blacklist others.

8. Parameters

Recommendation: Member State **policymakers** and **competent authorities** should put in place clear parameters that allow a **trust service provider** to gauge the severity of a reportable incident. In particular, the following factors should be considered:

- Compromise of the certification authority
- The number of individuals, companies, or government bodies who are affected by the breach (e.g. number of certificates compromised)
- The duration of the breach
- The nature of personal data/information affected
- Adverse impact on individuals affected by the breach

It is important that the recommendation on parameters is aligned with the exercise conducted by ENISA and Article 29 WG with regards to breach severity assessment.

9. Thresholds for notifying ENISA and other Member States

Recommendation: The baseline test for whether a Member State **competent authority** should report an incident affecting a trust services provider to other Member States and ENISA is whether the incident is likely to have an impact at the European Union level. The determination should be informed by an analysis conducted by the competent authority of the importance of the incident based on the same parameters for determining an incident's importance. For example, a compromise of a certification authority should warrant a notification across all Member States, even if the breach occurred only in one state. **ENISA** and the **competent authorities** should evaluate whether the competent authorities are reporting the correct types of incidents with regularity, and **competent authorities** should notify and discuss with **trust services providers** in their markets when they notify ENISA about incidents and why they made the decision to notify ENISA.

10. Deadlines for initial and follow-up reports

Recommendation: Member State **competent authorities** should adopt a tiered system for notification deadlines as is the case with Article 4 of the e-Privacy Directive. The baseline requirement for **trust service providers** is to provide their competent authority with initial notification of an incident within 24 hours from when the trust service provider became aware of the incident. After this initial notification is made, a more detailed notification of the incident should be made regarding the incident, with the deadline based on the severity of the incident, but a maximum of 15 days from when the trust service provider became aware of the incident.

Trust service providers need to develop internal processes to ensure that they are able to meet these deadlines.

11. Report content and template for supervisory authorities

Recommendation: Member State **competent authorities** should work together and promote a single template that **trust service providers** can use to report incidents. Having such a template should help to increase the efficiency of reporting and make it less of a burden for trust service providers, especially once they get used to the template. While the template does not need to be mandatory, it generally should cover common topics, which also helps ENISA compile data for comparisons and analysis.

The template should especially include the following items:

- contact details for the organisation and person responsible for notification
- date and time of notification
- date and time when the breach was established
- type of security breach or loss of integrity

- a short summary of the event
- impact of the breach including, a number and type of compromised certificates, and, where possible, a number of individuals affected or likely to be affected by the breach
- actions taken to mitigate the impact of the breach
- list of national authorities informed about the breach and channels of communication used
- authorities in other Member States informed (including channels of communication used) about the breach in case of a breach with a cross-border impact
- lessons learned about the incident (measures introduced by the trust service providers to limit the occurrence and/or impact of the breach in the future)

Trust service providers should be obliged to provide only basic information on the breach in the initial notification, while the more detailed information including lessons learned need to be included in the follow-up reports.

12. Report content and template for users (data subjects)

Recommendation: Although not specifically prescribed by the draft Regulation, the **trust service providers** should consider notifying their customers of breaches having an impact on their electronic identities and potentially also on their personal data. In this case, the following information should be provided to the customers:

- contact point with the trust service provider;
- a description (in user-friendly language) of the incident and what personal data has been compromised and how;
- measures taken to mitigate the adverse effects and what the customer can do himself/herself to mitigate the impact.

13. Use of annual reports by ENISA

Recommendation: Member State **competent authorities** should provide information to **ENISA** about incidents that their **trust service providers** reported. These authorities should provide ENISA with common information to aid it in using the data to create usable analytical outputs for the authorities and trust service providers. In turn, ENISA should publish an overview of incidents reported by trust service providers across the EU on an annual basis, including statistical analysis. Further, ENISA should offer recommendations based on this statistical analysis and discussions with all relevant parties, including competent authorities, trust service providers, national/governmental CERTs, and other interested parties – in how to prevent such incidents and how to improve the reporting process's efficiency and usefulness.

14. Channels of communications

Recommendation: Member State **competent authorities** should work to enable a variety of communications channels with trust service providers. At a minimum, this should include widely used channels such as phone, SMS, email, and web-based forms. However, the last option of web-based forms should be encouraged as it facilitates the distribution of incident data, eases the burden on trust services providers and enables collection and aggregate analysis of breach data on both national and European level.

For more time sensitive incidents including emergencies, competent authorities should provide a secure

connection for use. While competent authorities should take the lead in setting up these channels of communication, **trust service providers** also must take responsibility for knowing which channels are available to it and understanding how to reach the competent authority in the event of an urgent incident, as well as to communicate the strengths and weaknesses of each channel to the competent authority.

15. Media policies

Recommendation: Media can play an important role in disseminating information about data breaches at trust service providers. As such, **competent authorities** should try to cultivate good relationships with relevant media channels in their market to disseminate information as necessary. For these competent authorities, possible measure for consideration include:

- Have an organisational media policy and train staff for working with the media, which includes having employees that can make good judgments about which information to provide to the media and how to protect confidential information;
- Learn to use the media actively for distributing information about incidents or communicating other information, and;
- Develop a long-term strategy for using the media for creating awareness about issues relevant to data security and trust service providers.

16. Managing the reporting scheme

Recommendation: All parties involved in the reporting process of data breaches affecting **trust service providers**, but especially Member State **competent authorities** and **ENISA**, need to constantly assess the framework for trust service providers' reporting breaches to improve the process. As laid out in the recommendations for Article 13a, this should involve the following from these parties:

(1) analysing individual incidents to draw the proper lessons and analysis;

(2) perform statistical evaluations to understand the broader trends; and

(3) manage the longer-term evolution of the reporting scheme with analysis of individual incidents and statistical analysis in mind.

Competent authorities from across the EU should consult with each other where possible to share best practices, and ENISA and FESA should be actively involved in and facilitate the process. The role of these platforms should lie in gathering and exchanging best practices and providing recommendations for the implementation of Article 15. Competent authorities should in turn communicate at regular intervals with trust service providers to provide them with information about best practices and an overview of how the reporting scheme is evolving.

5 Conclusions

Although discussions between EU institutions on the final shape of the trust service regulation will still take time, the wording of Article 15 of the current draft does not seem to raise too many objections among the Member States. That is why it is useful for stakeholders – the trust service providers, the supervisory and other competent authorities on the national level as well as ENISA and the European Commission - to prepare for the smooth implementation of notification of breaches. Consultations with supervisory authorities on the feasibility of implementing Article 15 have shown, that no major changes as regards organisational aspects and resources are anticipated, although some adjustments may take place in relation to other parts of the proposed regulation.

The implementation should be facilitated by the fact that supervisory authorities in the Member States have collected experience already from notifications of breaches of security and loss of integrity on publicly available telecommunication networks under Article 13a as well as breaches of personal data under Article 4. Adapting the ENISA guidelines under Article 13a for the purpose of Article 15 will be useful for supervisory authorities when dealing with a Diginotar-type incident, which up until now, has been rather out of scope from existing security and notification articles in EU legislation.

In this report a number of recommendations have been identified that supervisory authorities and trust service providers should follow so that new reporting requirements do not represent a significant burden:

- Most of the security measures involved in Article 13a and Article 4 are common with Article 15. Consequently it is important to utilize the experience from existing notification obligations under Articles 13a and 4. The need to use existing notification schemes and reporting structures is of utmost importance also because the nature of some incidents may result in trust service providers having the obligation to submit notifications under more than one article of EU legislation.

- The procedural and content linkages between security and notification articles including Article 15 will require close cooperation of relevant supervisory bodies: national regulatory authorities, data protection authorities, trust services supervisors and possibly also national/governmental CERTs, who have developed a good level of expertise in dealing with and responding to security incidents, including the crucial aspect of cross-border cooperation.

- In order to ease the notification process both nationally and for cross-border breaches it is desirable to have common templates developed. This would enable the supervisory authorities to analyze the common features of the breaches as well as ENISA and the European Commission to make an assessment on the European level and propose actions aiming to increase the security of electronic identification and trust services.

- Special attention needs to be paid to a harmonised approach to definitions of reportable breaches, especially because not all information security and loss of integrity incidents automatically entail or lead to a personal data breach.

ENISA is looking forward to discuss with national authorities all the aspects mentioned in this report, which needs to be considered as a first attempt to devise recommendations for a future notification scheme under Article 15. Nevertheless, ENISA will further support Member States in their preparatory works for implementation of Article 15 just as it has done with Articles 13a and 4. ENISA is ready to exchange and promote best practices by means of publishing reports and benchmarking studies as well as holding workshops on its own initiative or based on specific requests of the Member States.

Annex I: References

EU existing and proposed legislation in the area of breaches notifications

- Article 15 of the Regulation on electronic identification and trust services for electronic transactions in the internal market: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm The regulation is the result of the reform of the original e-Signatures Directive: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/index_en.htm
  European Data Protection Supervisor's opinion on the draft regulation: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-09-27_Electronic_Trust_Services_EN.pdf
- Article 13a of the Framework directive of the EU regulatory framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf
- Article 4 of the e-Privacy directive, part of the EU legislative framework on electronic communications: http://ec.europa.eu/information_society/policy/ecomm/doc/24eprivacy.pdf
- Article 30, 31 and 32 of the proposed Data Protection regulation: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. The regulation is part of a wider reform of the data protection framework: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Related ENISA publication and other publicly available documents

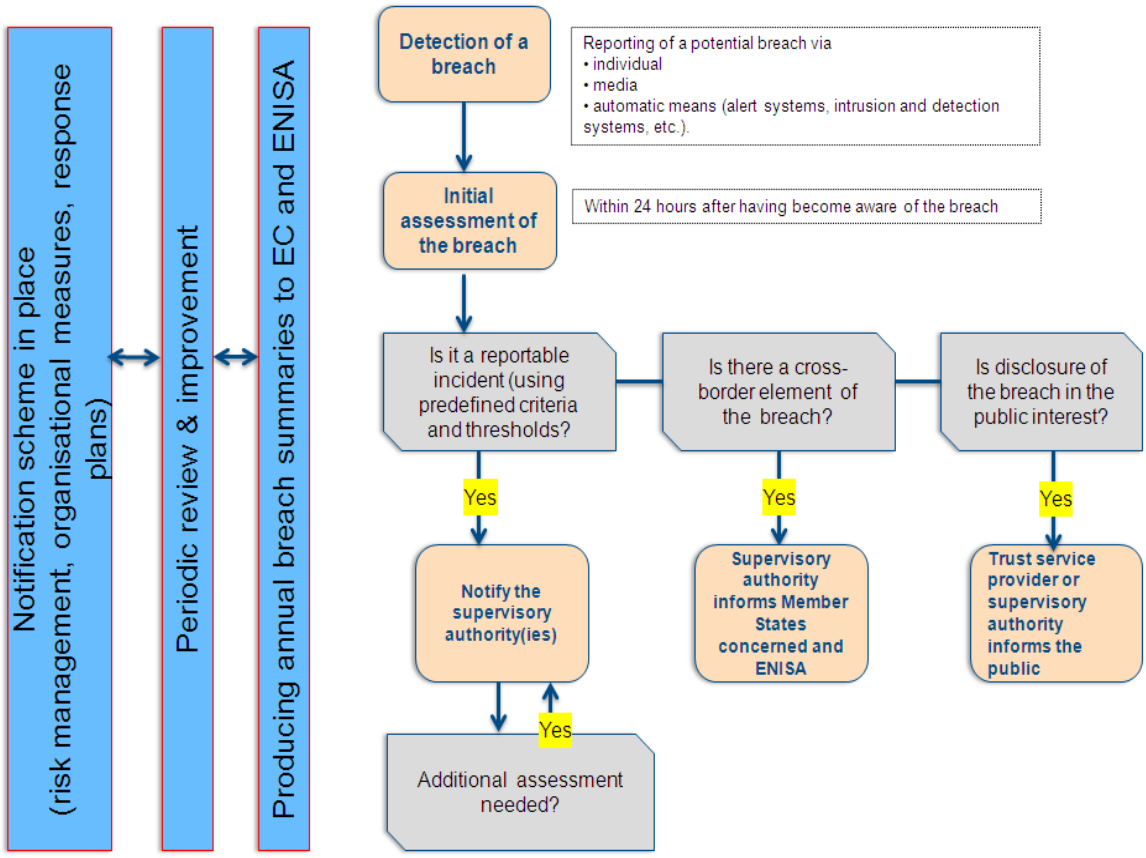
- ENISA's Cyber Incident Reporting in the EU: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
- ENISA's Technical Guideline on Reporting Incident (Article 13a Implementation): http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures
- ENISA's Good Practices on Reporting Security Incidents: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting
- ENISA's Annual Incident Reports 2011 (Analysis of the Article 13a incident reports of 2011): http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011
- ENISA's Recommendations on Technical Implementation Guidelines of Article 4: http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech
- ENISA's Data Breach Notifications in the EU: http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn

- ENISA's Managing Multiple Electronic Identities: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/mami
- European Commission's Public consultation on personal data breach notifications under ePrivacy Directive: http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/data_breach/index_en.htm
- Article 29 Data Protection Working Party opinion on cloud computing: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
- Public documents of FESA: http://www.fesa.eu/documents.html
- Critical observations on the proposed EU Regulation for electronic identification and trust services for electronic transactions in the internal market; J. Dumortier and N. Vandezande, Interdiscipinary Centre for Law andICT, K.U. Leuven: https://www.law.kuleuven.be/icri/ssrnpapers/37ICRI_Working_Paper_9_2012.pdf

Annex II: Abbreviations

CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CIIP	Critical Information Infrastructure Protection
CRL	Certificate Revocation List
CSP	Certification Service Providers
EC	European Commission
e-ID	Electronic identification
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
EU	European Union
FESA	Forum of European Supervisory Authorities for Electronic Signatures
NRA	National Regulatory Authority
PKI	Public Key infrastructure
STORK	Secure idenTity acrOss boRders linKed

Annex III: Breach notification scheme under Article 15



Annex IV: Questionnaire for the competent authorities

Questionnaire: Implementation of Article 15 of the draft regulation on electronic identification and trust services for electronic transactions in the internal market

Organisation Details

Your Name: _____

Name of your organisation: _____

Job Title/Position: _____

Contact details (phone number, email): _____

Job Description (please indicate your main responsibilities): _____

Type of your organisation	
Data protection authority	☐
National regulatory authority	☐
Other authority with responsibility for the area of electronic identification (please specify)	☐

Section A: Background and definitions

Objective of Section A – Questions in Section A are designed to understand the current status of electronic identification schemes in your country, especially as regards notification of security breaches by trust service providers. The focus of this section is on current or envisaged legal instruments, procedures and parties involved in the notifications.

A1. Which document provides the legal base for electronic identification and trust services in your country? Is the notification by trust service providers of security breaches, and/or other breaches such as network breaches and personal data breaches, covered by this or another document(s)?

A2. What is the body responsible for the e-ID agenda in your country? What body is (should be) responsible for notification of security breaches by trust service providers? Which other bodies are/should be involved in the notification of e-ID related incidents?

A3. Have any guidelines been issued on breaches notifications for trust service providers, or are notifications procedures in place at all?

A4. Can you indicate how many trust service providers are in the country? If possible, indicate the names of the organizations or provide a Web link to a list if such a list exists.

A5. Which body in your country would be the most appropriate to receive notifications from trust service providers (i.e. Data Protection Authority, telecoms regulatory authority, other designated bodies, etc.)?

Section B: Notification details and ENISA recommendations

Objective of Section B – Questions in Section B are designed to gather the views of stakeholders on recommendations that ENISA is currently considering for the implementation of Article 15, taking utmost account of recommendations made for the implementation of Article 13a and Article 4.

B1. ENISA intends to produce recommendations on the implementation of Article 15 for the following areas: definitions; procedures; thresholds; breach severity assessment; content of the report and report template; time frames for follow-up reports on how the incident is being (has been) solved;

communication channels; informing the public; media policies; evaluation of notification scheme in time.

Do you think that all the relevant areas that require recommendations are listed above or would you recommend inclusion of other areas, or on the other hand deleting any areas?

B2. A crucial issue for notification schemes is the question of definitions. In the case of Article 15 definitions need to be clarified for the portion of the Article that reads "breaches of security and loss of integrity having a significant impact on trust services provided and personal data maintained therein"? Is the following definition suitable for reportable incidents or would you recommend any modifications?

Definition of the reportable breach	Breach of security and loss of integrity leading to the accidental or unlawful destruction, loss, alteration, temporary unavailability, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of trust services.
Your comment:	

B3. In case of a reportable breach, a number of stakeholders at the national level must be notified within 24 hours after the trust service provider becomes aware of the breach. ENISA suggests that, apart from the competent supervisory authority, at least one or more of the following authorities (provided they are not the competent supervisory authority themselves) should be informed: national regulatory authorities; data protection authorities; national security agencies; and national / governmental CERTs.

Tell us your opinion on this shortlist and whether to include or, on the other hand, delete some of these bodies from the shortlist of bodies to be notified of a breach.

B4. In order to trigger the notification scheme it is important to define thresholds beyond which the incident is considered as having significant impact and be reported? In your opinion, what criteria should be used to determine when a notification should be triggered?

B5: For reportable breaches ENISA is considering the following content of a notification to the competent authority: contact details for the organisation and person responsible for notification, date and time of notification, date and time when the breach was established, type of personal data breached, a short summary of the event, impact of the breach including number of individuals affected or likely to be affected by the breach, actions taken to mitigate the impact of the breach, list of national authorities informed about the breach and channels of communication used, authorities in other Member States informed (including channels of communication used) about the breach in case of a breach with a cross-border impact. For the follow-up reports ENISA (except more detailed information) suggests inclusion of lessons learnt and measures adopted to minimize or exclude the occurrence of the breach in the future.

Tell us your opinion on whether the content is sufficient or whether more areas should be included in the content of the notification.

B6: ENISA is considering that there should be one template for reporting breaches that could be used by trust service providers (possibly adjusted to conditions in individual Member States) to notify incidents to both competent supervisory authorities nationally as well as in other Member States and to ENISA. It would also help in the process of compiling the information for the annual report on notifications to be delivered to ENISA and the European Commission.

Tell us your opinion on whether there should be a single template to be applied across all Member States.

B7. ENISA is considering that the initial notification is submitted within 24 hours after the trust service provider has become aware of a breach, while the following and updated reports are delivered to competent supervisory authorities within the next five working days at the latest. The means of communication include e-mail or web-based form for the initial report complemented by phone calls and personal meetings or any other secure communication means.

Tell us your opinion on the suggested approach.

B8. Owing to the fact that the Article 15 requires informing the public on breaches when it is in public interest ENISA is considering appropriate measures concerning media policies. It includes monitoring media coverage, elaborating media policy, and train employees on these topics and use media actively for distributing information about serious breaches in order to counter rumours and panic and contribute to awareness rising.

Tell us your opinions on the recommended measures in the area of media policy.

B9. Every notification scheme needs to take account of its validity and usefulness as the nature of breaches evolves. ENISA therefore is considering a periodic overview of notification schemes based on annual reports on breaches of competent supervisory authorities and subsequent evaluation of reports by ENISA, which will include recommendations. Such an evaluation should be undertaken also nationally while involving all the relevant stakeholders in the area of notification.

Tell us your opinion:

Section C: Domestic Cooperation

Objective of Section C – Questions in Section C are designed to gather the views on domestic cooperation regarding implementation of Art. 15 and eID and trust services issues in general.

C1. Does your organisation have the legal power to issue binding instructions to trust service providers? If not, which is the organisation that has the respective power?

C2. Do you communicate with trust service providers? What is the nature of communication with the trust service providers (informal, voluntary, memorandum of understanding) and how often do you communicate with them?

C3. If you do communicate with trust service providers, what means of communication (personal meetings, phone calls, web forums, workshops…) do you use when communicating with trust service providers and what are the main topics?

C4. Are there any working arrangements between the relevant authorities, including competent supervisory data protection authorities on notifications under the proposed Art. 15? Please describe. Which other stakeholders are included in these arrangements?

C5. Do you cooperate with the media on the issues of electronic identification and trust services, especially as regards notification of breaches? If yes, could you please briefly describe your media strategy (whom do you communicate with, how often do you communicate, what kind of information to you communicate to the media, etc.)?

Section D: International Cooperation

Objective of Section D – Questions in Section D are designed to gather the views on international cooperation regarding implementation of Art. 15 and eID and trust services issues in general.

D1. What international fora regarding electronic identification and trust services does your organisation take part in?

D2. Does your organisation exchange views including best practices with authorities in other Member States? If so, what are the frequency and means of such communication?

D3. Would your organisation be in favour of ENISA providing additional support on the implementation of Article 15 with regards to guidelines, identifying best practices, developing templates, holding workshops, etc.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu