enisa
European Network and Information Security Agency

Data breach notifications in the EU

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created as a response to security issues of the European Union. The Agency's mission is essential to achieving a high and effective level of network and information security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of network and information security for the benefit of citizens, consumers, business and public sector organisations in the European Union. ENISA is a centre of competence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between European institutions, the Member States and industry players.

Contact details

For enquiries about this study, please use the following contact details:
European Network and Information Security Agency
Technical Competence Department
Email: sta@enisa.europa.eu
Internet: http://www.enisa.europa.eu/act/it/eid

Supervisor of the study: Sławomir Górniak – ENISA
Authors: Andreas Rockelmann, Joshua Budd, Michael Vorisek – IDC CEMA
ENISA staff involved in the project: Demosthenes Ikonomou, Rodica Tirtea

Acknowledgements

We particularly wish to thank the following organisations for their support during the compilation of this study:

- European Commission, DG INFSO B.1, Electronic Communications Policy – Policy Development
- European Commission, DG JUSTICE C.3, Fundamental Rights and Union Citizenship – Data Protection
- The members of the Article 29 Working Party
- European Data Protection Supervisor

Legal notice

Table of contents

Executive summary

Recent high profile incidents of personal data loss across Europe have prompted wide discussion on the level of security given to personal information shared, processed, stored and transmitted electronically. Gaining and maintaining the trust and buy-in of citizens that their data is secure and protected represents a potential risk to the future development and take up of innovative technologies and higher value added online services across Europe and will be a key challenge for organisations going forward.

The introduction of a European data breach notification requirement for the electronic communication sector introduced in the review of the ePrivacy Directive (2002/58/EC[1]) is an important development with a potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data is being secured and protected by electronic communication sector operators. Against this background, ENISA aims to review the current situation and to develop a consistent set of guidelines addressing the technical implementation measures and the procedures, as described by Article 4 of the reviewed Directive 2002/58/EC.

The telecommunications sector recognises that data breach notifications have an important role in the overall framework of data protection and privacy. Nevertheless, operators are seeking support and guidance on an EU and local level over a number of issues, which if clarified, would better enable European service providers to comply effectively with data breach notification requirements. Key concerns raised by telecom operators include the following:

- **Risk prioritisation** – The seriousness of a breach should determine the level of response. In order to prevent 'notification fatigue' for both the operator and the data subjects, breaches should be categorised according to specific risk levels

- **Communication channels** – Operators want assurances that notification requirements will not negatively impact their brands. It is important for operators to maintain control of communications with relevant data subjects, as much as possible, to ensure that operators can effectively manage any impact on brand perception brought about by the data breach and subsequent notification.

- **Support** – In preparation for mandatory notification requirements, operators are looking for support in terms of guidance on procedures. In particular, guidance should provide a methodology for categorising types of private data and combinations of private data, as well as how to proceed with notifications based on the level of risk attributed to each breach.

Data protection authorities (DPAs) take varied approaches to enforcing data protection and privacy. Some follow EC Directives closely, while others take on additional responsibilities beyond those outlined in the Directives. Although there are exceptions, the majority of DPAs surveyed in this study support mandatory notifications for telecom operators. Those that did not support mandatory notifications mostly indicated that budgetary limitations were a key factor in influencing their opinion. As notifications are not yet mandatory in most countries, regulatory authorities have little experience in handling notifications. Since regulatory authorities have a number of responsibilities, there are concerns that additional duties must not interfere with pre-existing responsibilities. Notifications are not viewed as a number one priority for most authorities. A smooth transition to mandatory notifications will consequently depend on a resolution to a number of factors, outlined here:

- Resources – Budgetary allocations for regulatory authorities should reflect new regulatory responsibilities. Concern has been raised that resources at some regulatory authorities are already occupied with other priorities. Bandwidth for additional responsibilities is limited

1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

- **Enforcement** – DPAs indicated that sanctioning authority enables them to better enforce regulations. Data controllers will be less incentivised to comply with regulations if regulatory authorities do not have sufficient sanctioning powers. Some authorities indicated that financial penalties are seen as the most effective tool for pressuring data controllers to comply, while others indicated that public criticism and black lists could be effective too

- **Relevant authorities** – Local legislation will determine who the relevant authority is for regulating data breach notifications in the telecommunications sector, when mandatory notification requirements are transposed into local legislation. Although many data protection authorities indicated they are communicating effectively with other authorities already, it is important for legislation to clearly delineate relevant responsibilities, in order to mitigate or prevent potential conflicts

- **Technical expertise** – In some cases, businesses have a high level of technical sophistication, which allows them potentially to conceal valuable information regarding breaches from regulatory authorities, which do not have comparable resources and expertise. Hiring new staff with relevant expertise is important in order for regulatory authorities to remain effective

- **Awareness raising** – A high public profile is an important element in demonstrating the influence of regulatory authorities. A common strategy in communicating the importance of data protection to the public could be useful in better educating data subjects about their privacy rights, and the role of notifications in the overall framework of data protection

Smooth implementation of data breach notification procedures requires close cooperation between data controllers at the service providers and the relevant regulatory authorities. While most operators and regulatory bodies surveyed recognise the importance of notifications, there are a number of issues where interests of the parties involved might conflict.

- **Undue delay** – Regulatory authorities want to see a short deadline for reporting breaches to authorities and data subjects, in order to prevent controllers from concealing evidence and also to give data subjects ample time to protect themselves. Service providers, however, want their resources to be focused on identifying if the problem is serious and solving the problem, instead of spending time reporting details, often prematurely, to regulatory authorities

- **Traffic monitoring** – Private data belonging to employees or customers running over a corporate network remain a challenging issue for both regulatory authorities and operators. Telecom operators are often requested to monitor and analyse traffic data on behalf of their customers, particularly in cases where companies want to monitor the actions of their employees. In this context, regulatory authorities see traffic monitoring as a privacy risk, due to the fact that employers may be exchanging private information on the corporate network, to which the employers would then have access

- Content of notifications – The content of the notifications can have a direct impact on customer relations and retention. Operators want to make sure that the content of the notifications does not impact negatively on customer relations. Regulatory authorities, however, want to see that the notifications provide the necessary information and guidance in line with the rights of the data subjects

- Audits – One service provider indicated that it performed its own security audits internally, with the aim of detecting and solving any potential vulnerabilities that could result in data breaches. The operator believed that its internal expertise were sufficient to ensure it was using the latest techniques for securing data and compliance with regulations, suggesting its expertise surpassed that of the national regulatory authorities. Regulatory authorities, however, indicated that their ability to perform audits and spot checks provides the authority necessary to enforce compliance

While the recent telecoms reforms make notifications mandatory for telecom operators, there remains ongoing debate about extending mandatory notifications to other sectors.

- **Telecommunications operators:** In comparison to other sectors, regulatory authorities indicated that telecommunications operators ranked high in terms of their security measures and ability to limit data breaches.

Telecom operators have at their disposal some of the top networking, communications and security experts. But this is true mostly for the larger operators. Smaller alternative operators and local ISPs do not necessarily have resources comparable to the large international companies and incumbent operators

- **Finance sector:** Finance institutions are considered to be at great risk, due to the sensitive nature of the data they possess. Nonetheless, financial institutions are already subject to regulations across Europe, with regulations being enforced by various bodies, including central banks. Consequently, extending data breach requirements to financial institutions would require careful coordination with other responsible authorities, which may already require incidents of data breaches to be reported

- **Healthcare:** Data protection authorities regularly pointed to the healthcare sector as an area of high risk. Due to the large amount of very sensitive private data stored on doctors' and nurses' laptops, which are often unencrypted, there is high risk for exposure or leaks

- **Small businesses:** Small businesses pose a major challenge. Collectively, they have a lot of personal data, but individually they do not have resources or know-how to secure their data. Due to the sheer number of small businesses, regulation would prove challenging. Educating and making businesses aware would require significant efforts and resources. As more and more small businesses develop online strategies, the risk for exposure is increasing

Glossary[2]

Personal data: any information relating to an identified or identifiable natural person (data subject)

Data subject: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Processing of personal data: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

Data controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law

Data processor: a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller

Third party: any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data

Data recipient: a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients

DPA: Data Protection Authority

Regulatory authority: National regulatory authority (NRA), the body or bodies charged by a Member State with any of the regulatory tasks assigned in the specific Directives[3]; legally distinct from and independent of all organisations providing electronic communications networks, equipment or services. The NRAs, responsible for the ex ante regulation of markets, must not accept instructions from any other body.[4]

Privacy officer: A resource responsible for handling notifications of breaches to both the regulatory authorities and the data subjects will issue a notification, once the incident response team has made the decision. The privacy officer has responsibilities for overseeing implementation of the company's privacy policy, and has a board-level sponsor

2 The definitions used in this study are derived from EC Directives mentioned in Appendix B
3 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:HTML
4 http://europa.eu/legislation_summaries/internal_market/single_market_services/l24216a_en.htm

1. Introduction

1.1 Policy context

Recent high profile incidents of personal data loss across Europe have prompted wide discussion on the level of security given to personal information shared, processed, stored and transmitted electronically. Gaining and maintaining the trust and buy-in of citizens that their data is secure and protected represents a potential risk to the future development and take up of innovative technologies and higher value added online services across Europe and will be a key challenge for organisations going forward.

The introduction of a European data breach notification requirement for the electronic communication sector, introduced in the review of the ePrivacy Directive (2002/58/EC), is an important development with a potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data is being secured and protected by electronic communication sector operators. Against this background, ENISA aims to review the current situation and to develop a consistent set of guidelines addressing the technical implementation measures and the procedures, as described by Article 4 of the reviewed Directive 2002/58/EC.

1.2 Objectives

The document compiles feedback from regulatory authorities, legal experts, private companies and industry experts to better understand the challenges facing the telecommunications sector in the face of mandatory notifications for data breaches. The basis for this document is a survey conducted by ENISA with relevant stakeholders, followed by in-depth interviews. The document represents a stock-taking, which can lead to the future development of best practices designed to help both regulatory authorities and telecom operators prepare for the new regulatory realities brought about by the review of Directive 2002/58/EC. In order to illustrate the current outlook for data breach notification procedures in Europe, the report aims to analyse:

- Views and opinions of regulatory authorities and telecom operators on traffic monitoring and the notion of personal data traffic
- The current understanding of the definition of what is considered as "personal data" on the basis of Article 29s's work and the differences that may occur when professional/corporate data/traffic are considered
- The possibility for mandating/recommending the reporting of data breaches model followed in other fields (for example by CERTs) and the creation of a common reporting format
- Similarities and differences between different business sectors (e.g. financial vs. telco)
- Views on the time duration for a company to notify the relevant authority on a data breach
- Views of Data Protection Authorities and the industry on the notification of data breaches to the citizens affected and in those cases on the type of information to be provided
- Beyond reporting, is there a need to have an audit mechanism in place? If yes, is this role expected to be fulfilled by DPA's or 3rd parties?
- Whether any of the above points/areas would benefit from a pan-European approach

1.3 Methodology

ENISA prepared this report by surveying and interviewing public authorities, operators of public telecommunications networks, and ICT industry experts about their experiences and recommendations for effective practices in planning and implementing data breach notification procedures.

A questionnaire was prepared and distributed to the stakeholders. They were located primarily in Europe, though some were also located in other parts of the world, particularly in the United States. Based on the responses, interviews were arranged with as many of the survey respondents as possible. In total, ENISA surveyed 15 telecommunications service providers in 12 countries, 18 regulatory authorities in 17 countries, and 13 other private organisations and experts in 10 countries. In total, ENISA surveyed stakeholders in 23 European Union countries, plus Norway, Turkey and the United States. For more details on the survey sample, please see Appendix A.

The questionnaires[5] were initially sent out in February and March of 2010, with interviews then taking place in the following months up until June 2010. In total, 37 completed questionnaires were received, 33 interviews conducted, and a total of 46 organisations contributed either in the questionnaire, the interviews, or both. In parallel to the survey and interviews, ENISA conducted secondary research to identify data breach notification procedures in other regions of the world.

Following completion of this research, the results were analysed, good practices were identified, and these findings were then prepared in the form of this document.

The document was submitted to external experts for review, comments and validation. This document represents a broad consensus of a wide selection of public- and private-sector experts on data breach notification practices.

1.4 Target audience

The report aims to assist public authorities and private organisations in the EU and Member States as they implement data breach notification policies. It aims to support those who do not have significant experience with such policies. Additionally, it may also serve as a tool for improvement for those managing or working with existing notification policies. Furthermore, it also serves as a basis for discussion by all stakeholders about how national procedures should be coordinated, and how they can better cooperate and harmonise with one another under the new telecoms regulatory framework.

Finally, it also aims to serve as input to the relevant European Commission services responsible for the revision of the ePrivacy Directive, as well as in future policy initiatives in the area.

1.5 Structure of the report and how to use it

To begin with, regulatory factors influencing data breach notification requirements in the EU are put in context by reviewing the status to date of legislation on an EU level. The following two chapters summarise in detail feedback gathered by ENISA from surveys and in-depth interviews conducted with relevant stakeholders, beginning with regulatory authorities and legal experts, and then followed by private companies, including consultants and industry experts. The analysis in both of these chapters follows the order of the questionnaire used by ENISA to survey the stakeholders, backed up by additional feedback gathered from in-depth interviews. The results of the survey and interviews are followed by an analysis of issues where opinions between regulatory authorities and private companies diverge. ENISA believes regulatory authorities should be aware of these divergent opinions, so that they can better prepare to resolve potential points of contention raised by industry stakeholders as they prepare to comply with regulatory requirements.

5 Both questionnaires are available for download at http://www.enisa.europa.eu/act/it/dbn/

In line with the anonymous nature of the survey and interviews, ENISA made an effort to avoid direct references to respondents. Direct examples referenced in the report that are connected with a specific organisation are based on publicly available information.

All personal data collected were processed in accordance with Community Regulation (EC) No 45/2001 of the European Parliament and of the Council (OJ L8 of 12.01.2001, p1)[6] on the protection of individuals, with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

6 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32001R0045&model=guichett

2. Data breach notifications in context

Data breach notifications are not yet mandatory in most countries in the European Union. The EU telecommunications regulation reform package[7] passed in November 2009, however, requires EU Member States to introduce mandatory data breach notifications into local legislation. Nonetheless, it is important to note that some countries have already introduced data breach notification requirements into local legislation and regulatory codes of practice. The following section provides an overview of the legislative steps introduced by the European parliament, in order to illustrate what requirements will have to be transposed by member countries into local legislation. It also provides an overview of what steps member states have taken independent of the reforms package.

2.1 Legislative background

In November 2009, the European Parliament and the Council of Ministers reached an agreement on EU Telecoms Reform, after negotiations brokered by the European Commission. The reform, proposed by the Commission in November 2007, aims to strengthen competition and consumer rights on Europe's telecoms markets, facilitate high-speed internet broadband connections to Europeans and establishes a European Body of Telecoms Regulators to complete the single market for telecoms networks and services. One of the reforms included in the package requires telecoms and internet service providers to issue notifications for personal data breaches. It is the first law of its kind in Europe. Communications service providers will be obliged to inform the authorities and their customers about breaches affecting their personal data. Transposition of the telecoms reform package into national legislation in the 27 EU Member States is to take place by May 2011.

The EU telecoms reform package comprises 5 different EU Directives (Framework Directive, Access Directive, Authorisation Directive, Universal Service Directive and the E-Privacy Directive) and a new Regulation setting up the European Body of Telecoms Regulators BEREC. It has been accompanied by a Directive to reform the GSM Directive of 1987 to free airwaves for 3G and other mobile services. The E-Privacy Directive (officially Directive 2002/58 on Privacy and Electronic Communications[8]), which the reform package amends with the data breach notification requirement, is an EU Directive on data protection and privacy and is targeted at operators of public communications networks. It presents a continuation of earlier efforts, most directly the Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[9]). It deals with the regulation of a number of issues, such as confidentiality of information, treatment of traffic data, spam and cookies. Directive 2002/58 has been transposed in all EU member states. The transposition took place mostly in 2003, although several states were delayed in implementing the Directives in local law.

Data breach notification requirements in the reforms package are included in Directive 2009/136/EC[10] of the European Parliament of the Council of 25 November 2009, which amends The E-Privacy Directive (2002/58/EC). The paragraphs relevant for data breach notification requirements are listed here as follows:

> "3. In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.
>
> When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.
>
> Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data relevant to the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

7 http://ec.europa.eu/information_society/policy/ecomm/tomorrow/index_en.htm
8 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
9 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
10 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:EN:HTML

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

4. Subject to any technical implementation measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.
Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken, which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3.The inventory shall only include the information necessary for this purpose.

5. In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency(ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementation measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders, particularly in order to be informed of the best available technical and economic means of implementation of this Article."

It should be noted that data breach notifications are not yet mandatory in most EU countries, as the member states are still preparing to transpose the Directives. Nonetheless, there are examples of countries that have implemented in local legislation a requirement to notify authorities and/or data subjects in case of a data breach, or keep a log of data breaches that could be accessed by regulatory authorities in case of an investigation or audit. Additionally, there is an instance of a DPA that has the authority to force data controllers to issue notifications, as part of a Code of Practice that is designed to protect the rights of data subjects. Below are select examples illustrating such cases found in Europe:

- **Germany** – An obligation to issue notifications in cases of data breaches entered into force in September 2009. This obligation is included in Section 42a of Germany's amended Federal Data Protection Act (BDSG)[11]. Controllers are obligated to notify both the DPA and the data subjects. The law is modelled on the security breach notification laws that have been enacted in the United States. It applies to:

  - Bank and credit card data
  - Telecommunications data and data collected online
  - Data related to criminal offences
  - Other particularly sensitive data

11 http://www.bfdi.bund.de/EN/DataProtectionActs/DataProtectionActs_node.html

- **Spain** - The Royal Decree 1720/2007[12], which approves the regulation implementing Organic Law 15/1999, states that data controllers, as part of their security policy, shall draw up a security document containing, among other aspects, provisions related to a procedure of notification, management and response to incidents. Moreover, article 90 of the decree states that "There shall be a procedure for notification and management of incidents that affect personal data and a register established for recording the type of incident, the moment it occurredor, if appropriate, was detected, the person making the notification, to whom it was communicated, the effect arising from it and the corrective measures applied."

- **United Kingdom** - In 2008, the United Kingdom's Information Commissioner's Office (ICO) issued a guidance note on notification of data security breaches to the ICO[13]. The ICO advised that it should be notified of serious breaches, although there was no legal obligation.

- **Ireland** – The Irish DPA has issued a Code of Practice that includes a section on notifications to data subjects in cases of a breach[14]. Once the DPA is notified of a breach, the regulator can decide if the data subjects should be notified. If the data controller resists, the DPA can issue an enforcement notice. The Code of Practice states that "Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected."

It should be noted that in Ireland local authorities took it upon themselves in 2009 to examine whether legislative changes were needed to address the issue of data breaches, with particular reference to mandatory reporting. A Data Protection Review Group was established by the Minister for Justice, Equality and Law Reform to examine this issue. The group was established in January 2009 as a response to the rise in instances of devices being lost or stolen, and the subsequent concern about the potential damage that could result from the misappropriation of data. The review group published recommendations in May 2010, including the following[15]:

- Legislation should provide for a general offence by a data controller of deliberate or reckless acts or omissions in relation to the data protection principles – including contraventions of the security principle in relation to data breach incidents. This would complement the existing offence under the Data Protection Acts of failure to comply with an Enforcement Notice issued by the Data Protection Commissioner (DPC) - including an Enforcement Notice directing a data controller to inform individuals of a data breach affecting them

- The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice, as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the DPC, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the DPC

- The Code should be reviewed on a regular basis by the DPC and amendments submitted to the Minister as necessary to keep the legislation current

- The DPC should continue to develop his investigation and audit activities in a targeted way, with a particular focus on organisations that hold sensitive personal data, in compliance with emerging risk-based approaches to enforcement

- Legislation should provide for the timely publication of the outcome of such DPC audits, as an aid to good practice and in the interests of transparency

- The DPC should continue to develop public awareness activities in this area

12 https://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/reglamentolopd_en.pdf
13 http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf
14 http://www.mop.ie/publications/Irish-Data-Protection-Commissioner-approves-personal-data-security-breach-code-of-practice.htm
15 http://www.justice.ie/en/JELR/Pages/Ahern%20Publishes%20Data%20Review%20Report

2.2 Conclusions

ENISA's research has found that even in countries where data breach notification procedures have not been introduced into local legislation, regulatory authorities and service providers are aware of the telecoms reform package and are already beginning to prepare for the introduction of mandatory notifications. As a result, stakeholders are looking for information and best practices from countries that already have notification procedures, either as a mandatory law or as a code of practice. Countries that have already introduced data breach notification procedures can serve as a model for other countries that are only just beginning.

3. Regulatory outlook – A survey of data protection authorities in Europe

Data protection authorities (DPAs) take varied approaches to enforcing data protection and privacy. Although there are exceptions, the majority of DPAs surveyed in this study support mandatory notifications for telecom operators. Those that did not support mandatory notifications indicated that budgetary limitations were a key factor in influencing their opinion. One opposing voice suggested that prevention and education were sufficient, and that mandatory requirements for notifications would do little to better secure personal data beyond that which is already being done. In this context, one regulator suggested that it was more important to ensure that data controllers have evaluated the risks and put documented procedures in place to secure data.

Recommendations

- **Both Germany and Ireland stand out as useful examples of countries that are already in the process of implementing data breach notification procedures. It would be important to conduct a progress review in both countries over time in order to gather experiences, best practices, and lessons learned.**
- **Stakeholders should take time to communicate with local lawmakers, voicing concerns and suggestions for introducing legislation that is effective.**

As notifications are not yet mandatory in most countries, regulatory authorities have little experience in handling notifications. Since regulatory authorities have a number of responsibilities, there are concerns that additional duties must not interfere with pre-existing responsibilities. Notifications are not viewed as the number one priority for most authorities. Consequently, regulatory authorities are seeking clarification and support in a number of areas, so that they can better prepare themselves as data breach notifications become mandatory for service providers.

3.1 Background

Resources assigned to data breach notifications

As notifications of data breaches to regulatory authorities and data subjects are not yet mandatory in most countries in the EU, few authorities have dedicated resources to handle data breach notifications. Nonetheless, there are instances of countries where regulatory authorities do recommend or require notifications, although such notifications are not limited necessarily to telecoms service providers. At one authority interviewed by ENISA, resources have been allocated with responsibilities for overseeing notifications. The allocated resources, however, have other responsibilities beyond just handling notifications. One DPA surveyed by ENISA had allocated 2 resources (out of a total of 21 full time staff employed by the authority) to overseeing notifications to data subjects that are issued by data controllers, out of which the resources dedicated approximately 15-20% of their time. In another case, one authority has allocated notification responsibilities to 6 employees, out of a total of 33 employed by the authority. In other instances, authorities indicated that their auditors had competencies to deal with notifications, should the issue arise, but that their expertise was in other areas, such as auditing and inspecting data breaches.

Concern has been raised that resources at some regulatory authorities are already occupied with other priorities. Bandwidth for additional responsibilities is limited. Feedback from regulatory authorities that are concerned about budget restrictions suggested that budgetary allocations for regulatory authorities should reflect new regulatory responsibilities. Consequently, budgetary allocations should be designed in such a way as to anticipate predictable responsibilities (i.e. planned audits and inspections) and make room for unpredictable responsibilities (i.e. a potentially large, yet unforeseeable, number of data breaches that require notifications). Nonetheless, a number of authorities do not expect a large number of notifications. Consequently, budgetary concerns were not raised by all authorities, as they expected the extra workload would not be overwhelming. Feedback compiled by ENISA indicates that the majority of regulatory authorities believe that prioritising notifications according to risk and mitigating the number of notifications would help in part to alleviate concerns regarding limited resources.

The number of data breaches reported to regulatory authorities ranges from country to country, and depends greatly on local legislation. The number of breaches reported over the past 2-3 years to regulatory authorities interviewed by ENISA, ranges from less than ten, to dozens, to more than one hundred. For example, in its annual report for 2009, Ireland's Data Protection Commissioner reported that the Commission received 119 data security breach notifications, 95% of the total including notifications to subjects. This is up from 81 in 2008. It should be noted that the increase in notifications in Ireland is not necessarily related directly to actual breaches, but more to greater awareness.

> *"Rather than an increase in the absolute number of data security breaches, I attribute this increase to a greater awareness among organisations of their data protection responsibilities. As a matter of good practice when faced with a data security breach, more organisations are contacting my Office for advice on how to deal with the matter,"* **Twenty-First Annual Report of the Data Protection Commissioner 2009, Ireland**

3.2 Working definitions and criteria for personal data, data subjects and data breaches

Definitions of personal data

Regulatory authorities surveyed by ENISA referred consistently to Directive 95/46/EC as the basis for their respective countries' definitions for personal data and data subjects. Few authorities indicated any problems in working with the definitions. Regulatory authorities also referred to Directive 2002/58/EC as a basis for their definition of traffic data. In general, comments from regulatory authorities indicated that there were no serious problems applying the definitions and using the definitions to distinguish personal data from other types of data. Nonetheless, problems have been identified in distinguishing personal from corporate data. For example, what if an employee uses a company email address to issue personal emails, or if an employee uses a company phone to make personal calls? A question was also raised in regard to telephone numbers, i.e. whether the mere telephone number, outside the context of a communication, is considered traffic data, or simply personal data.

Determining data breach events

Criteria for defining what equates to a data breach vary from country to country. Not all countries have criteria for defining a breach at all. Some regulatory authorities suggested that a very broad definition be applied, while others suggested specific types of breaches. In one country, for example, the regulator outlined specific examples of incidents that they would consider to be a breach:

- Processing personal data for direct marketing purposes without consent of the data subject
- The use of a personal identification number without consent of the data subject
- A disclosure of debtor's data without a written reminder to the data subject about the default
- Processing personal data by automatic means without notifying State Data Protection Inspectorate

In some cases, countries distinguish between a security threat and mismanagement that does not violate security protocols. In Spain, for example, local legislation implies that possible data breaches not strictly related to security (that is, concerning personal misuse,without breaking security schema), are not currently covered by the notification process. In Ireland, a broad definition applies. Any incident involving the inappropriate release of personal data and breaching the requirement to hold personal data securely can qualify as a breach. Other countries have similarly broad definitions, in which case any incident involving the inappropriate release of personal data and breaching the requirement to hold personal data securely can qualify as a breach.

Despite the broad range of definitions and criteria, regulatory authorities that have been monitoring breaches identified a number of types of breaches that can serve as a useful reference:

- **Loss of IT equipment** – misplaced or stolen equipment – laptops, USB sticks, etc.
- **Mailing** – distribution of a letter in the mail or an email to an incorrect address that includes personal data
- **Improper disposal of documents** – leaving personal data in documents deposited in a garbage bin that can be accessed by the public
- **Hacking** – malicious attacks on computer networks
- **Technical error** – unforeseen complication in an IT system exposing data to outside parties
- **Theft** – data in the form of documents, electronically stored data, etc. that is stolen
- **Unauthorised access** – employees taking advantage of vulnerabilities to access personal data of customers stored in files or electronically
- **Unauthorised distribution** – distributing personal data on P2P networks

Determining risk

As the criteria for determining a breach can be broad, there is a chance that even frivolous breaches that pose no real risk to the rights of data subjects could require notifications. In order for procedures to be effective, there is a view that decisions should be risk-based. In other words, if there is no real risk to the data subjects, a notification would be redundant. For example, if the data breached was encrypted, it is not likely that the information could be exploited in any way.

> *"A risk-based approach could also reduce notification fatigue."*

Consequently, regulatory authorities and data controllers alike are faced with the challenge of determining the level of risk that each breach poses, so as to avoid disproportionate responses to potentially frivolous breaches. In most cases, regulatory authorities did not have any formal criteria for measuring risk. Consequently, determining risk is done mostly on an ad hoc basis. But several respondents did reveal criteria they take into consideration when determining risk. On one hand, the determination can be based on quantitative indicators. In other words, how many people are affected by the breach and how much data was breached? On the other hand, qualitative indicators, such as the type of data, are taken into consideration. For example:

- Physical or mental health data
- Information relating to the sexual life of the data subject
- Information relating to the alleged or actual commission of a criminal offence by a data subject
- Political, philosophical or religious beliefs
- If the data subjects involved are minors
- Whether or not the data breach involved financial data

3.3 Notification and handling procedures

ENISA interviewed regulatory authorities to gather their opinions about the best procedures for data controllers to issue notifications of data breaches to regulatory authorities and to data subjects. During the research process, ENISA found that few regulatory authorities actually have formal procedural guidelines, as notifications are not yet mandatory in most countries. Nonetheless, ENISA was able to gather a wide range of opinions on handling procedures and what regulatory authorities would expect when mandatory notifications come into effect.

There are instances of select regulatory authorities that have issued guidelines for data controllers on how to notify both the regulator and data subjects when personal data is breached. This applies not only to telecom operators, but data controllers in other sectors as well. For example, Ireland's Data Protection Commissioner has drafted guidelines for data controllers and published them on its Web site[16]. The guidelines recommend that data controllers notify the authority by telephone or email once they determine that the personal data for which they are responsible has been compromised. Depending on circumstances, the data controller could be asked to provide a report outlining:

- The amount and nature of the data that has been compromised
- What action (if any) has been taken to inform those affected
- A chronology of the events leading up to the disclosure
- A description of measures being undertaken to prevent a repetition of the incident

The majority of regulatory authorities interviewed by ENISA indicated that data controllers should be responsible for issuing notifications, once the decision to issue a notification had been made.

Notification triggers

The decision to issue a notification can be taken either by the data controller itself, or be based upon a directive from the regulatory authority. As both regulatory authorities and data controllers can apply different criteria for determining if a breach notification should be issued, ENISA spoke with regulatory authorities to gather their opinions on existing experiences. Overall, regulatory authorities did not indicate that they currently had any formal criteria for determining what should trigger a notification. In some cases a data controller voluntarily decides to notify the regulatory authority and issue a notification to the data subject, based on its own criteria. In other cases, a notification could be triggered if a complaint is received at the regulatory authority by a data subject, or through a report in the media. In such cases, an investigation would have to be conducted to determine if a breach has occurred, and only then would a decision be made to request that the controller issue notifications to the data subjects. Otherwise, most regulatory authorities agreed that the decision to trigger a notification to the regulatory authority and to data subjects should be taken by the data controller.

Content of notification

Regulatory authorities indicated that they would be open to receiving notifications in a number of ways, when mandatory notifications take effect. A phone call and an email were considered to be sufficient. In many cases, respondents indicated that the contents of the notification could be left up to the data controllers and should be considered on a case-by-case basis. Nonetheless, regulatory authorities pointed to a number of relevant points that would be expected to be included in the notification. Feedback indicates that the notification should include:

16 http://www.dataprotection.ie/viewdoc.asp?DocID=901&ad=1

- A description of the nature of the breach (if it was isolated or widespread), the nature of the data exposed (financial data, health data, etc.);
- The number of people affected;
- What is being done to contain the breach

Follow up notifications are expected, with updates on how the breach is being resolved. Overall, there was little pressure from regulatory authorities to formalise the process in standard templates, with a number of regulatory authorities suggesting that such templates would be difficult to design, owing to the fact that each breach is unique.

Means of communication with data subjects

Regulatory authorities expressed openness to how data controllers notify data subjects of a breach. Regulatory authorities highlighted a variety of media that data controllers in their respective countries could use to notify data subjects of a breach, ranging from letters in the post to posting notifications on Web sites, and press releases. Regulatory authorities indicated that the most convenient method for the service provider was sufficient. Feedback also suggests that regulatory authorities would be open to the data controllers deciding on the format of the notification. Regulatory authorities did not indicate that they had in mind a specific template for required information in the notification. Each case, they believe, should be taken on an ad hoc basis. Nonetheless, recommendations for basic information that should be included are:

- Background of the incident, cause of the breach
- What has been done to prevent such a breach occurring in the future
- Advice on what data subjects can do to protect themselves

It should be noted that the means of communication can often be dependent on the quality of contact information available to the data controller. For example, if a breach requires a notification to a large number of data subjects, it is possible that the contact information for many of the subjects will be out of date or incorrect. As a result, the notification could go to the wrong address or wrong person. Consequently, the content of the notification should not further disclose personal data.

Undue delay

ENISA spoke with regulatory authorities to gather their opinions on the issue of undue delay and deadlines for issuing data breach notifications to both regulatory authorities and data subjects. Opinions were mixed. A number of respondents indicated there should be clear and specific deadlines, while others suggested a more flexible approach, where updates are scattered over time as more and more information becomes available. For example, an immediate notification could be issued to authorities once a breach had been identified, simply stating that fact. This could then be followed with updates at a later time with more specific details, followed by a notification to the data subjects.

Regulatory authorities suggested that data controllers notify both authorities and data subjects, 'as soon as possible,' or within a matter of days. In one case, a regulator suggested that authorities and data subjects be notified within 72 hours to one week.

Additionally, the nature of the breach could impact how soon regulatory authorities expected data controllers to notify the subjects. For example, if information deemed to be sufficiently risky were left in a public place, the regulator would expect a hastier notification to be issued to subjects than if the breach posed less risk to subjects. In countries where regulatory authorities have experience receiving notifications of breaches from controllers, respondents indicated that notifications to their offices are typically received within a matter of days. Regulatory authorities agreed that deadlines should consider the requirements of data controllers, allowing time to determine if a breach had in fact taken place, and to allocate resources to prevent the problem from spreading.

Nonetheless, there was concern that if the deadline was too flexible, data controllers could have time to manipulate evidence. Feedback suggests that there should at least be clear guidelines for determining a realistic deadline that fulfilled the need for undue delay. Without clear deadlines, requirements for issuing notifications in sufficient time would be hard to enforce.

> *"There is a need for clear deadlines. There is no sense in having general criteria if you cannot enforce it properly. After too much time, the response would be useless."*

ENISA spoke with one regulator in a country where notifications are already issued according to local law. In this case, the deadline requirement refers to "without delay." Internally, the ministry responsible has said this should be 14 days, but a specific number of days does not appear in legislation. In this case, the regulator has the authority to judge if the notification has been issued in a timely manner.

3.4 Compliance

Regulatory authorities already apply a number of techniques to enforce existing data protection regulations, ranging from fines to public awareness campaigns, which serve as a reference for understanding the measures that regulatory authorities may take in the future when enforcing data breach notification requirements. In order to ensure compliance with existing data protection legislation, regulatory authorities take varied approaches across the EU, ranging from the imposition of penalties and fines, to an approach that focuses more on education and prevention. For example, when applying for a permit to process data, a regulator can request that the controller and or processor provide a security policy that illustrates the measures they are taking to protect the data. The policy should also include a risk impact assessment and a disaster recovery/contingency plan. Audits are a common approach as well, although some regulatory authorities indicated that resources are limited for audits. Nonetheless, sanctioning powers are often limited by local legislation. In some cases, regulatory authorities are not permitted by law to issue fines.

Slovenia can serve as an example of a regulator that takes a proactive approach, performing audits and investigations and imposing fines. The Slovenian data protection authority has the authority to enter the premises of the controller and seize documentation, interview people, and suspend operations. The regulator in Slovenia has conducted a number of high profile and very public investigations in order to expose abuses. In one case, the regulator went to a tax office and did an investigation to determine if employees were accessing information for personal reasons. They identified a list of famous people and asked the tax office to show us if personal data belonging to the celebrities had been accessed. They identified several people who had accessed the data without having the rights to do so. As a result, the regulator issued warnings and fines.

DPAs indicated that sanctioning authority enabled them to better enforce regulations. Data controllers will be less inclined to comply with regulations if regulatory authorities do not have sufficient sanctioning powers. Feedback suggests that financial penalties are seen as the most effective tool for pressuring data controllers to comply. The size of penalties imposed by DPAs varies greatly. In one country included in the research for this study, for example, the minimum administrative fine for breaches was a warning, whereas the maximum was a financial fine of Euro 150.000. ENISA came across a number of countries where fines are typically in the thousands of euros. But there are cases where these fines can be multiplied by the number of people affected by the breach. One regulatory authority described a case to ENISA in which an insurance company sold personal data belonging to more than 2,000 people. Fines in the country for breaches are typically a few thousand euros, but since the breach involved thousands of people, the total fine amounted to more than Euro 100.000, as the fine was multiplied by the number of people involved.

Beyond financial penalties, regulatory authorities indicated other techniques that can be used to better enforce compliance. A number of regulatory authorities mentioned negative publicity as an effective tool. For example, regulatory authorities can develop blacklists, which highlight serious abusers of personal data. Such tools are particularly relevant for countries that do not permit regulatory authorities to issue fines. There are examples in the EU where regulatory authorities cannot issue fines, although in some cases they can escalate cases to the courts, which can in turn impose fines. Nonetheless, there was a consensus that regulatory authorities should not be dependent on fines alone. Proactive incentives were also mentioned during interviews with regulatory authorities. For example, a regulator could issue awards to companies that demonstrated effective compliance with data protection laws.

3.5 Comments and opinions

Monitoring of traffic data

Monitoring of traffic data proved to be a contentious issue among regulatory authorities. Out of the regulatory authorities surveyed by ENISA, 41% responded positively when asked if they thought data traffic should be monitored in order to discover data breaches. Those who responded positively, however, indicated that such monitoring should be conducted under strict legal conditions. In other words, the purpose of the monitoring should be clearly defined and relevant authorities should oversee the process. . One regulator further suggested that the proportion of data monitored should be restricted only to the data required for the discovery of the data breach.

Discovery of data breaches

Opinions differed on the issue of a stronger role for regulatory authorities in the early detection of data breaches, as opposed to reacting to data breaches after the fact. Eighteen percent of regulatory authorities surveyed by ENISA indicated that regulatory authorities should be involved in early detection of breaches. Such regulatory authorities had already indicated that they conducted spot investigations and audits to detect violations of data protection legislation. Other authorities indicated detection of breaches should be left to the data controllers themselves.

Role of third parties in notification procedure

Involving third parties in the notification process could raise a level of complexity to an already complex process. Consequently, regulatory authorities in general were sceptical of the role of outside parties participating in the notification procedure. As an example, ENISA asked regulatory authorities about the potential role of CERTs in the notification procedure. Opinions varied. Not all countries currently have CERTs, consequently such a system would be difficult to roll out on a EU-wide level. In countries where there are CERTs, regulatory authorities suggested that they could have a positive roll in public awareness. For example, CERTs could use their resources to make the general population aware of potentially widespread breaches, and what could be done to mitigate the risks of being exposed. CERTs could also develop blacklists of companies that they deemed to be risky or negligent in protecting data.

Extension of notification requirements to other sectors

The telecoms reform package passed in 2009 applies mandatory notification requirements to telecom and Internet service providers. With this in mind, ENISA asked regulatory authorities their opinions about the differences between data protection standards among telecom operators compared to other sectors. In general, regulatory authorities indicated that telecom operators ranked quite highly in terms of their data protection practices. They did, however, point to other sectors that pose a greater risk. In most cases, regulatory authorities indicated the financial sector posed a high risk, due to the nature of the data they store and process. Nonetheless, in many countries, banks are subject to regulation by authorities separate from the data protection authority, which may already require notifications. Consequently, extension of mandatory notifications would potentially conflict with other regulatory authorities and, as a result, the jurisdiction of regulatory authorities would have to be clearly defined.

Regulatory authorities also pointed frequently to the health care sector as an area of concern. Doctors and nurses often have sensitive information stored on laptops, which can be easily lost or stolen. Hospitals and clinics often do not encrypt the data stored on their servers and laptops. Consequently, there is a high risk of exposure.
Small and medium sized businesses also pose a particular risk. Individually, they may store a small amount of data, but collectively they can account for a significant amount of data in a given country. Small businesses typically do not have the budgets or expertise to invest in high level security processes that may be necessary to protect customer data against breaches, or monitor data processors. Consequently the SMB sector as a whole presents a significant challenge to regulatory authorities, if mandatory notifications are extended.

3.6 Conclusions

Although there are exceptions, as noted above, the majority of regulatory authorities surveyed by ENISA indicated their support for regulation of mandatory data breach notifications for the telecoms sector. Many raised concerns about their ability to handle the workload, fearing that the sheer number of breaches would result in a large number of investigations. In one case, a DPA indicated that according to local legislation every single notification would trigger an investigation/infringement procedure. Most agreed that a system to prioritise notifications would be the best approach. Just how to prioritise such breaches, however, would require further discussion. On this topic, regulatory authorities suggested that support on a European level to come up with a common approach to prioritising breaches would be useful.

Beyond this, DPAs raised concerns about the feasibility of preparing an effective data breach notification process. For example, developing automated systems for data breach notifications processes, including a common notification format capable of providing information about the breaches, with statistics and indicators that can help to evaluate and understand the situation. One regulator suggested that such indicators should be obtained at a national and European level. Consequently leadership on an EU level, with cooperation from DPAs across the region, would be necessary.

Regulatory authorities indicated that they were in "wait and see mode" to establish how local legislation would transpose the EU Directives. Only then would they be able to prepare and take the necessary steps to enforce regulations. This would suggest that it is necessary to engage local lawmakers now, to make them aware of the resource constraints of their respective regulatory authorities. Legislation will be ineffective if regulatory authorities do not have the resources to oversee compliance. Local legislation can be consistent with EU Directives, while at the same time enabling regulatory authorities the ability to prioritise breaches and consequently focus on the most serious incidents, rather than have their workforce overwhelmed with more frivolous violations.

Recommendations

- **Data protection authorities must be prepared for a trial period in the early stages of mandatory data breach notifications as data controllers learn to prioritize and define data breaches. Data controllers could report a large number of incidences that may or may not count as breaches, in order to ensure that they are complying.**
- **DPAs should publish guidelines explaining a simple set of procedures for reporting breaches to the regulatory authority and data subjects, outlining the means for notification and guidance on the content of the notifications.**
- **Data protection authorities should consider a variety of deterrence measures, ranging from issuing fines to public exposure of serious offenders in the media, as well as issuing awards and recognizing data controllers that demonstrate effective data breach notification procedures.**

Private sector outlook – a survey of telecommunications operators in Europe

Operators surveyed by ENISA overwhelmingly agreed that it was in their best interests to secure private data belonging to their customers. Public reaction to data breaches can be extremely negative, and could motivate customers to abandon their provider for another. In case a breach does occur, operators want to demonstrate competent leadership and prove to customers that they are doing what is necessary to solve the problem and mitigate any potential problems. Within this context, a number of operators in Europe already issue notifications to both regulatory authorities and data subjects in case of serious breaches, even though such actions may not be mandated by law.

Reforms to European telecommunications regulations issued in November 2009 make data breach notifications to both regulatory authorities and data subjects mandatory. The reforms have been issued in EU Directives, which must be transposed into local legislation. Operators will be faced with potentially damaging legal consequences if they do not comply correctly, once local legislation is passed. Although respondents surveyed by ENISA recognised the importance of data breach notifications within the overall framework of data protection and privacy, operators raised a number of questions relating to notification requirements, in order to ensure that they are complying correctly. They want to be prepared for new administrative and logistical demands that could arise from mandatory notifications, so that they can manage efficiently any new procedures that would be necessary to align their operations with relevant regulatory conditions.

4.1 Background

Out of the operators that responded to ENISA's survey, 64% indicated that they are notifying both regulatory authorities and data subjects of breaches and in some cases risks of breaches. Most respondents that do issue notifications indicated that they had begun issuing notifications within the past 1-5 years. Nonetheless, ENISA did encounter respondents that have been issuing notifications since as early as 1998 and 1999.

Oversight of data breach and notifications usually falls under the responsibility of multiple departments within operators that work together, depending on the nature of the breach. From the operators that issue notifications to regulatory authorities and/or data subjects, 25% indicated that notifications fall under the regulatory affairs department. Almost half (44%) of the operators had an individual identified as a data protection officer or data ombudsman, or a division set up specifically to handle data protection and privacy. Of the remaining operators that issue notifications, the responsibility is usually taken by a mix of security, IT, legal and corporate departments. Of these, there is usually a representative that handles security who will take the lead. External communications sometimes go through a legal department that oversees external communications.

The rate of data breaches that result in notifications to data subjects varies greatly from country to country. Operators reported a small number of breaches in the past year that resulted in a notification to data subjects, ranging from 2 to 5 in the past two years. The majority of notifications to regulatory authorities result in a notification to data subjects, but this is not true in all cases. In countries where notifications are recommended or required by regulatory authorities, there is a higher rate of notifications to regulatory authorities, but not all notifications in these cases result in notices being sent to data subjects. In countries where notifications are recommended or required by regulatory authorities, operators are very careful to report every risk, or potential breach, to the regulator, in order to ensure that they are complying. In this case, there can be several reported breaches a day. The breaches are communicated to the regulator in a template, with details illustrating the nature of the breach or potential breach. In such a case, a small number of breaches are actually communicated to the data subjects. The aim is simply to make sure the regulatory authorities know that they are complying.

Some respondents indicated that data breaches can be seasonal. Hacker behavior can be seasonal. In one case, July was reported as a particularly active month for hackers. This month is a particularly popular time for people to take vacation. Hackers will often use the down time to plan and implement their attacks.

The bulk of data breaches that resulted in notifications were the result of technical error, administrative error or negligence. Only one of the operators that reported breaches in the past two years indicated criminal intent as the cause of the breach. Additionally, some of the notifications issued to data subjects and regulatory authorities were the result of a risk of data breach and not due to an actual breach. Breaches can be IT based, or non-IT based. Non IT-based breaches can involve employees leaving contracts containing confidential information in public areas, or in disposal bins without properly destroying the documents, so that they are unreadable by others. Breaches can involve exposure of customer data or exposure of employee data. The following categories summarise the types of IT-related breaches and risks that operators surveyed reported, as well as those that selected regulatory authorities have reported, along with examples:

Actual breaches

- **Process vulnerability** – An individual used a Web-based application offered by an operator to connect social security numbers with names that were already publicly available from different sources
- **Technological flaw** – A public email system distributed emails to other subscribers, revealing private data
- **Administrative error** – An employee of an operator accidentally forwarded emails with customer details to other customers
- **Loss of equipment** - An external consultant lost a laptop with private employee information
- **Criminal intent** – An individual illegally obtained confidential network information from a physical location in order to hack into the operator's servers

Risk of breaches

- **Legislative changes** – Servers belonging to an operator were stored in another country that introduced new laws permitting governments to secretly inspect emails. The operator warned customers that their emails could consequently be inspected
- **Viruses** – An operator became aware that a number of computers belonging to its customers were infected with viruses that could potentially expose the contents of the computer

4.2 Working definitions and criteria

In order for companies to comply with regulations, they must have a clear understanding of the definitions of key terms in the relevant legislation. ENISA surveyed operators to determine how they define key terms such as "personal data" and "data subjects", to better learn what definitions they are applying and if they have encountered any problems applying the definitions in real-world situations. All respondents indicated that the definitions they used were in line with EC Directives on personal data.

"Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Article 2, Directive 95/46/EC

The definition is very broad. A wide variety of data points count as personal data, ranging from names and phone numbers to addresses and identification numbers. Operators indicated few, if any, challenges in interpreting the definition for personal data. There was no real indication that the definition should be altered in any way.

Questions were raised, however, about the role of publicly available data in legislation. There are countries where personal identification and business identification numbers are based on birth dates. Consequently, a publicly available identification number includes personal data. This raised questions about the role of publicly available data in breaches, and the extent to which a breach of publicly available data represents a threat to the rights of data subjects.

While definitions of personal data are being applied consistently among respondents, operators are also applying consistent criteria for defining what counts as a breach. Respondents referred to "unauthorised" access to personal data as a key factor in defining a breach. There were examples of operators that indicated the risk of a breach, or compromise of personal data, was sufficient to classify an event as a breach.

Nonetheless, there is still concern about the nature of incidents that are not easily definable as a breach, or that could be defined as a breach but represent little or no risk to the data subjects. For example, there can be delays in renewing or settling contracts between data controllers and processers, before personal data is transferred. This could count as a breach from a legal point of view, because the contracts were not finalised in time. But if the data was transferred safely, the rights and interests of the data subject were never at risk from a technical perspective. Issuing a notification in this case could raise undue concern.

Determining the risk of a breach poses a particular challenge for operators, who have varied approaches to determine risk. Most agree, however, that it is important to rate incidents according to a specific threat level. Few operators indicated that they had a specific methodology or procedure for determining risk level. In most cases, the process takes place on an ad hoc basis. In some cases, the risk level is dependent on the type of data in question. Factors taken into consideration include:

- The number of data subjects at risk
- The quantity of data at risk
- Age of data
- Nature of the breach, i.e. technical, human error, or theft

In determining the risk represented by data that is being processed by a third party, data controllers are often dependent on the information that is provided by the processor. In this case, clear criteria need to be included in the contract. But, overall, operators indicated that it was difficult to measure risk, particularly in advance, as many incidents are unique and unpredictable. In one case, an operator referred to the ISO 31000:2009[17] risk management standard as a basis for its own risk management processes.

17 http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170

4.3 Notifications and handling procedures

The unpredictability of breaches poses a challenge to operators, even those with risk management processes. While auditing and forensic services can be effective, most operators rely on information from third-party data processors and complaints from customers. Media reports after the fact are also common ways in which operators identify that there has been a breach or there is a potential breach. Almost two thirds (64%) of service providers surveyed by ENISA indicated that they performed audits and used software monitoring tools to secure their networks and look for breaches.

As notifications are not yet mandatory in most EU countries, operators are less likely to trigger steps that would lead to a notification, unless there are specific factors impacting the brand of the operator, or harming the customer. The decision to issue a notification to regulatory authorities and/or data subjects in virtually all cases is determined on a case-by- case basis. Brand is an important issue for all operators. If a breach becomes publicly known, operators are more likely to take necessary steps to issue a notification, as a means pf managing any potentially negative reactions. Few operators have developed clear policies and criteria for determining what kind of event would trigger a notification. In countries where notifications to either regulatory authorities or data subjects are recommended or required, the decision to trigger a notification is made much faster. In one case, an operator automatically issues a notification to the regulator once a breach or risk of breach has been identified. The debate is not about whether to issue a notification or not, but how to measure the level of risk the breach will represent to the data subjects and the operator, how to take necessary steps to solve the problem, provide the right support for customers, and assure the regulator that the operator is doing what is necessary to protect the rights of the data subjects.
In this context, the contents of the notification play an important role. As notifications are often issued to regulatory authorities and data subjects, the contents of the notifications have to be adjusted to take into account the interests of the recipients.

Notifications to regulatory authorities

In countries where notifications to regulatory authorities are already taking place, operators indicated that regulatory authorities had provided guidelines for details that should be included in the notification. A phone call or email is typically sent to the regulator notifying them of the basic details. This is followed by a formal report in a template that is in line with guidelines issued by the regulator.

Notifications to regulatory authorities follow less formal procedures in countries where notifications are not mandatory. In such cases, the number of notifications to regulatory authorities is quite small. As a result, initial communications are provided in an email or a telephone call. The parties then agree on next steps, based on the seriousness of the breach. In cases of serious breaches, information submitted as part of such informal communications typically addresses the following issues:

- Background facts explaining the incident
- Description of steps taken to solve or limit the breach
- Description of any communications sent to relevant data subjects
- Description of steps taken to avoid similar problems in the future

Notifications to data subjects

Not all notifications to regulatory authorities are necessarily followed by a notification to data subjects. Operators surveyed by ENISA indicated overwhelmingly that it was in their best interests to issue notifications to data subjects when necessary, as it allowed the operators to mitigate any potentially negative effects on customer relations. Operators indicated that they should determine the contents of the notifications and the means of delivery. There was no serious objection, however, to regulatory authorities reviewing the contents of the notification after it has been delivered, to ensure proper compliance.

The contents of the notification will depend to a great extent on the nature of the breach. Nonetheless, elements of notifications that have already been issued demonstrated commonalities, such as:

- Explanation of the type of data that was breached, e.g. bank account details, addresses
- Details on when the breach occurred
- Recommended steps to mitigate the impact of the breach, e.g. instructions on how to change passwords and user names
- Explanation of what the operator is doing to better secure customer data and prevent similar incidents in the future

If a notification is issued to customers, it often emanates from the customer relations department. Marketing and communications representatives contribute to the contents of the notification, which can also include input from the legal department and regulatory relations department.

Respondents indicated concern that regulatory authorities might not be sensitive to cost issues relating to notifications. Sending letters through the post could be a potentially costly undertaking. Consequently, operators preferred to decide what means should be used to issue the notifications. There are examples of operators that have called data subjects directly to notify them of a breach. But in cases where a large number of data subjects have been involved, emails have been used. There are concerns that data subjects will not easily identify the email, and it could get lost in the spam filter. Operators commented that data subjects are more likely to open a letter that is sent through the post than an email. The most common means for issuing notifications include:

- Letters delivered through the post
- Notifications on Web sites
- Notifications included in monthly account statements
- Statements to the press and press releases

Sample procedure

While few operators indicated any formal procedures for data breach notifications, ENISA did come across examples of operators that have procedures already in place, or are in the early stages of development. Policies encountered by ENISA leverage several key elements:

- **Response teams:** At least two groups are active in responding to data breaches, an incident response team and a technical response team. The incident response team will receive notice of the breach from the source, which could be an employee that discovers a breach, or a complaint from a customer, etc. This team is lead by a representative from a legal department or CTO/CSO/CEO level. The technical response team, consisting of IT experts, will determine the nature of the breach, how widespread the breach is and analyse how to implement a solution.
- **Decision making:** After an internal investigation has taken place, the incident response team will decide whether or not to issue a notification to the regulatory authorities and data subjects. The seriousness of the breach will determine the content of the notification to the regulatory authority. Low risk breaches will be followed up with a brief email or phone call to the regulatory authority, indicating that a breach has taken place and that steps are being taken to address the breach. More serious breaches will result in more detailed notifications, explaining the nature of the breach and giving more details of what is being done to contain the breach
- **Privacy officer:** A resource responsible for handling notifications of breaches to both the regulatory authorities and the data subjects will issue a notification, once the incident response team has made the decision. The privacy officer has responsibilities for overseeing implementation of the company's privacy policy, and has a board-level sponsor. The incident response team will also have a say about what content goes into the notification

- **Evaluation:** Once the breach has been resolved, an evaluation will take place with relevant stakeholders, such as a manager responsible for the area where the breach occurred. The evaluation will make clear any lessons learned and draw up necessary action items to improve processes
- **Policy development:** A resource responsible for developing and implementing privacy policy is responsible for overseeing a company-wide privacy and notification policy. Regular meetings are held over the course of the year to discuss privacy issues and areas for work and improvement, regulatory developments, etc. This resource is sponsored by by a board member

Undue delay

Data subjects require a timely notification, so that steps can be taken to protect their data. ENISA surveyed operators to better understand some of the time required to issue notifications to both data subjects and regulatory authorities and determine what kind of guidance could be applied. There were examples of operators indicating that regulatory authorities are typically notified of breaches within a day or two, while in other cases it can take up to two weeks. Similarly, when notifying data subjects, notifications have been issued within a matter of days, while some have taken up to two weeks. The nature of the breach and how it is discovered obviously impact on the time required to issue notifications.

Service providers want to make sure that deadline requirements do not become too stringent. Strict deadlines could potentially limit the effectiveness of their ability to solve the problem at hand. There is a concern that resources would be focused more on meeting deadlines than identifying the source of the breach and resolving it. With this in mind, operators are requesting that deadlines be flexible and take a tiered approach.

Regulatory authorities should be aware of how much time operators need to identify that a breach has, in fact, taken place, determine how widespread it is (number of individuals effected), identify the nature of the data breached, if the breach is an isolated incident or will it be repeated, and what steps are needed to resolve the problem. Regulatory authorities also need to be aware that while some breaches can be identified immediately, it takes time for the company's specialists to measure the risk level.

Respondents indicated that a tiered approach to notifications could be used, which can meet basic deadline requirements and at the same time not burden the operators' resources.

> *One option is to send a notification immediately to regulatory authorities, indicating that a breach has been detected but not include any other information. The objective is to notify the regulator so that they should be prepared for a potential breach. Once the problem has been identified, a follow up call and/or email can be sent with more specific details on the nature of the breach and a basic estimate of how serious it could be.*

Based on this information, the regulator can decide on how to respond. This approach would satisfy requirements to notify the regulator in a timely manner, but not require the service providers to include so much information in the initial notification that time and resources would be diverted from resolving the problem.

Relationship with regulatory authorities

Regulations concerning data protection and security are not always easily interpreted. The majority of operators surveyed by ENISA indicated that they looked to regulatory authorities for guidance in interpreting legislation to ensure proper compliance. Although they recognise the sanctioning powers of regulatory bodies, operators expect to receive constructive support and guidance from regulatory bodies so that they can prevent violations before they happen. Such a regulator can have a positive impact on an operator's ability to comply.

Some operators surveyed by ENISA indicated that they maintained positive relationships with regulatory authorities. In such cases, operators signified that the regulatory authorities provided regular support when questions arose regarding elements of legislation that were difficult to interpret. Brochures published by regulatory authorities, guidance and opinions published on Web sites, and workshops organised for the industry were all examples of support that operators found constructive. Respondents also referred to an open-door policy at the regulator, which permitted them to call anytime and ask questions and seek guidance as circumstances arose. This open door policy was reciprocated, with operators indicating that the regulatory authorities could call directly anytime and request information, or ask questions.

Nonetheless, other respondents in the survey reported a less constructive relationship with their respective regulatory authorities. One respondent in particular indicated that the only time they heard from the regulator was when there was an inspection and the authorities were looking for violations. In this situation, the regulator was seen only as a sanctioning authority. Such a relationship created a sense of mistrust between the service provider and the regulator and placed the service provider in a defensive position. As a result, there could be a reluctance to cooperate.

The relationship between operators and regulatory authorities is often influenced by the size of the operator, and the legal and technical resources available to it, compared to the resources that are at the disposal of the regulator. Feedback from one operator interviewed by ENISA indicated that they had technical expertise that surpassed the expertise available to the local regulator. Additionally, they had legal departments staffed with regulatory experts who could advise on difficult compliance issues. Consequently, the amount of support and guidance sought by these operators would be less significant than smaller operators that did not have comparable resources.

Roll of third parties

Operators increasingly rely on third parties for processing of data. As a result, third parties are often involved in the data breach notification procedure, primarily by reporting any known breaches to the data controllers. Those operators surveyed by ENISA that indicated they relied on third-party data processors, stated that if third parties were involved with data processing, strict conditions were stipulated in contracts that required them to report any breaches or suspected breaches. But notifications to the authorities, or data subjects themselves, were handled by the operators themselves.

In some cases, operators hire outside consultants to perform security audits. This is more common in smaller operators, which do not have in house expertise. Larger operators indicated a reluctance to rely too much on external auditors, indicating that their in-house staff had sufficient expertise.

Evaluation and best practices

Interviews conducted by ENISA with service providers indicate that 44% of operators that report notifications conduct an evaluation after the procedure has been concluded. One reason for conducting an evaluation is to ensure that resolving the incident has not resulted in any new breaches. Evaluations are often conducted by the individuals overseeing a response to the breach, but also include representatives from various departments, ranging from legal to security to IT. On one case, the national data protection authority was involved to a certain degree in the evaluation, as part of its investigation to ensure that the operators had taken the necessary remedial steps. But otherwise evaluations are all conducted internally.

Traffic data monitoring

Monitoring of traffic data could be used as a tool to detect breaches, but could in itself be a violation of privacy legislation. Operators already monitor traffic data in some cases, one example being - billing purposes. In terms of detecting breaches, however, operators surveyed by ENISA indicated a range of responses. Out of the total respondents, 50% indicated that traffic data should be monitored for the purpose of detecting breaches. Two operators that opposed monitoring traffic data cited logistical challenges as the main reason for their opposition. One indicated the large amount of data made it nearly impossible to effectively monitor traffic data. Another suggested the costs of monitoring traffic data were prohibitively high. A further opposing voice indicated that traffic data could be considered personal data, so monitoring the data could consequently violate privacy laws.

One argument in favour of monitoring traffic points to the ability to track down and identify potential hacking attacks. But the effectiveness of monitoring for such attacks can be limited by the nature of the technology used. A security expert who spoke with ENISA stated that hacking attacks are becoming increasingly sophisticated. More and more attacks are coming from malware, which collects data and encrypts the payload. In such a case, traditional traffic monitoring would be ineffective.

Role of authorities in notification procedure

Service providers interviewed by ENISA indicated as a consensus that it should be the operators themselves who took the decision to notify, and decided whom to notify. The role of the authority should primarily be that of an advisory body and of a review body, to make sure that procedures are in line with regulations. The operators view their communications channels with customers as strategically important to their business. Communications with the customers through a third party could jeopardize the customers' faith in the service provider.

However, in cases of wider breaches, affecting the greater population, there is more support for the regulator taking a stronger role in notification procedures. This is particularly true in cases where a breach or risk of breach could impact the public beyond the specific customer base of a given operator, or a select group of customers. In such cases, the regulator could use press releases or other media for notifying the public at large.

Role of CERTs

ENISA questioned respondents about the role that Computer Emergency Response Teams could play in the data breach notification process, due to the access they have to telecommunications network data and the communications channels, which they maintain with telecom operators and the public. CERTs could use their position to inform the public of potential risks, thereby offloading some of the burden from service providers. Feedback from respondents indicates that involving a third party in the process could add additional complexity, which some service providers do not want. By adding another body to the procedure, there is room for error or additional unforeseen complications. The relationship between CERTs and service providers is based on trust. Operators must be assuredthat the CERT will not use its data in a way that would violate that trust. This relationship could be challenged if the CERT plays a part in decisions that could result in sanctions against the operators.

4.4 Conclusions

As data breach notifications are not yet mandatory in most countries surveyed for this study, operators indicated satisfaction with the current status of notification standards in their respective countries. Where notifications are a part of local legislation, there is still concern that the triggers for a notification are not sufficiently defined. Consequently, this could be an area of focus for legislators and regulatory authorities as they transpose EC Directives into local legislation. Service providers are aware that notifications will become mandatory, and did not express any major objections. There was concern, nonetheless, that the public will single out telecom operators,, due to the fact that mandatory notifications are not yet extended to other sectors of the economy. Since notifications will be coming primarily from service providers, the public might react unfairly, deeming operators to be somehow less safe than other companies.

Recommendations

- **Service providers should allocate legal, marketing and technical resources to oversee data breach notification procedures, with direct access to board-level decision makers who can oversee decisions to issue notifications in serious cases.**

- **Operators will have to invest in updating their contact records for customers, ensuring that information is current and accurate. This will avoid missed notifications or notifications being issued to the wrong data subject.**

- **Operators should prepare a list of examples of potential incidences that do not clearly fit into legislation, and seek guidance in advance from authorities in order to avoid any future confusion.**

Operators indicated a high level of confidence in their own internal procedures for data security and data breach notification policies. Operators indicated that more support might be needed as requirements became clearer and outlined in local legislation. There are a few specific areas where operators have already requested support. Assistance in interpreting local legislation is of particular importance. Case examples illustrating how regulatory authorities cooperate with businesses in resolving compliance issues could be one form of support that operators find useful. Such examples should illustrate how regulatory authorities and companies cooperate as instances arise, and how the parties involved find a reasonable level of understanding for each other's priorities. Additionally, operators indicated that any advice or support for IT security standards would also be useful. While operators are confident in their own measures, they would consider references and case studies outlining effective security measures to be productive.

Stakeholder interests – identifying divergent objectives of regulatory authorities and the private sector

Smooth implementation of data breach notification procedures requires close cooperation between data controllers at the service providers and the relevant regulatory authorities. While operators and regulatory bodies surveyed recognise the importance of notifications, there are a number of issues where interests of the parties involved might diverge.

Undue delay – Regulatory authorities want to see a short deadline for reporting breaches to authorities and data subjects, in order to prevent controllers from concealing evidence and also to give data subjects ample time to protect themselves. Service providers, however, want their resources to be focused on identifying if the problem is serious and on solving the problem, instead of spending time reporting details, often prematurely, to regulatory authorities. A compromise will have to be found that gives controllers time to solve problems, while providing authorities with the basic information needed to ensure compliance.

Traffic monitoring – Private data belonging to employees or customers, running over a corporate network, remain a challenging issue for both regulatory authorities and operators. Telecom operators are often requested to monitor and analyse traffic data on behalf of their customers, particularly in cases when companies want to monitor the actions of their employees. In this context, regulatory authorities see traffic monitoring as a privacy risk, due to the fact that employers may be exchanging private information on the corporate network, to which the employers would then have access. Regulatory authorities will have to work closely with the private sector to provide clear guidance on traffic monitoring, particularly relating to procedures and legislation, to ensure that operators can comply with the relevant legislation correctly.

Content of notifications – The content of the notifications can have a direct impact on customer relations and retention. Operators want to make sure that the content of the notifications does not impact negatively on customer relations. Regulatory authorities, however, want to see that the notifications provide the necessary information and guidance in line with the rights of the data subjects. Regulatory authorities and operators will have to work closely together to ensure that the content of the notifications is in compliance with regulations, while at the same time taking into consideration the operators' relations with their customers. A number of regulatory authorities surveyed indicated that the content of the notifications should be left up to the operators, but that they should be able to review the notifications after they had been issued, to ensure compliance. Counter measures could then be applied in cases where the content was not in compliance with the spirit of the regulation.

Audits – One service provider indicated that it performed its own security audits internally, with the aim of detecting and solving potential vulnerabilities that could result in data breaches. The operator believed that its internal expertise was sufficient to ensure it was using the latest techniques for securing data and compliance with regulations, suggesting its expertise surpassed that of the national regulator. Regulatory authorities, however, indicated that their ability to perform audits and spot checks helps in enforcing compliance. Consequently there was a reluctance expressed by regulatory authorities to rely on any external parties for auditing security measures utilised by service providers.

5.1 Conclusions

Both service providers and regulatory authorities should develop a list of issues that could prove to be contentious and strive to resolve the issues in advance of mandatory data breach notifications being introduced into local legislation. Coming to an understanding on undue delay for issuing notifications will be a priority. While both regulatory authorities and service providers recognise the urgency of reporting breaches in a timely matter, strict adherence to a set timeline may prove to be counter-productive. Regulatory authorities and service providers should consider confidence building measures, which allow data controllers transparently to keep regulatory authorities informed of their progress in responding to breaches, while at the same time permitting a degree of flexibility, in order to allow the data controllers to resolve the problem with the resources available. Other disputes can potentially be resolved similarly, ensuring transparency and at the same time recognising the needs of the stakeholders. Both regulatory authorities and service providers should ultimately take into consideration the best interests of data subjects when resolving potential conflicts.

6. Next steps

ENISA has identified a number of areas that require additional support on an EU and/or local level, so as better to enable a smooth transition to mandatory notifications:

Risk assessment – Notifications should follow breaches of personal data that are likely to cause harm to data subjects or violate their rights. For example, if breached data is encrypted, there may be no real risk that the data will be exploited, and consequently a notification would be redundant. Issuing notifications for breaches that pose no risk will undermine customers' confidence in the organisation, and cause fatigue for data subjects, data controllers and regulatory authorities. Issuing notifications in cases where there is no risk could also desensitise customers and, as a result, they may overlook more serious notifications. It would be useful to provide guidance or develop guidelines for determining risk for both data controllers and regulatory authorities.

Notification threshold – Both regulatory authorities and telecommunications operators raised concerns that mandatory notifications could lead to "notification fatigue" for the data controllers, regulatory authorities and data subjects alike. Guidance on how to prioritise breaches, along with suggestions on specific indicators that can be used to prioritise breaches, would enable a consistent methodology across Europe. Relevant indicators to consider for such a threshold could include:

- Number of people affected
- Nature of the data that has been breached (financial, health, etc.)
- Nature of the breach (widespread, or an isolated incident)
- Security level (has the data been encrypted)

Procedures – Smooth implementation of a mandatory notification requirement will be dependent largely on clearly outlined procedures, so that stakeholders know how to respond in case of breach. Clear instructions outlining a necessary response pattern would give service providers the guidance and assurance required that they are complying with regulations

Evaluation period – Implementation of mandatory notifications is likely to encounter challenges and unexpected problems along the way. Consequently, there should be a preliminary period when the notification process can be reviewed and assessed. Relevant stakeholders should receive a template for tracking specific performance indicators that can then be analysed on an EU level after a trial period. Upon review, changes and recommendations can be made

Automation – Member states could aim toward developing an automated system of data breach notifications, whereby regulatory authorities have a Web-based form that data controllers can use to notify them of breaches. An automated procedure with basic requirements could be developed on an EU level. This procedure would enable the gathering of consistent statistics that could then be analysed to measure to what extent notification procedures are improving data protection standards

Extension of mandatory notifications to other sectors – With the exception of a few regulatory authorities who voiced opposition to mandatory notifications for telecom operators, the majority of regulatory authorities interviewed by ENISA supported extending mandatory notifications to other sectors. A number of telecom operators supported such an initiative too, arguing that current legislation singles out telecom operators, and could imply that they are less secure than other sectors. Before extending mandatory notifications to other sectors, however, it should be noted that some sectors are already subject to a regulatory regime that requires notifications through other regulatory bodies, that are distinct from data protection authorities. Consequently, extension of mandatory notifications should not necessarily come from an extension of the ePrivacy Directive, as this is geared toward telecom operators.

External auditors – Bringing in third parties to perform audits to ensure compliance with regulations adds a level of complexity and could raise the risk of additional breaches. Large operators indicated that their internal resources were sufficient to oversee compliance with regulations. Regulatory authorities did not voice any specific demand for the use of external auditors, rather preferring to hire additional resources, budgets permitting, so that the necessary expertise could be maintained internally.

Appendix A – profile of contributors

ENISA collected 37 questionnaires and conducted 33 interviews. Some respondents provided either the questionnaire or the interview. Altogether research covered 46 organisations or organisation bundles (cases). It has been one of the priorities of the research to ensure that a wide spectrum of perspectives be represented. ENISA has sought to include opinions from both private and public sectors, and from a variety of national and international contexts.

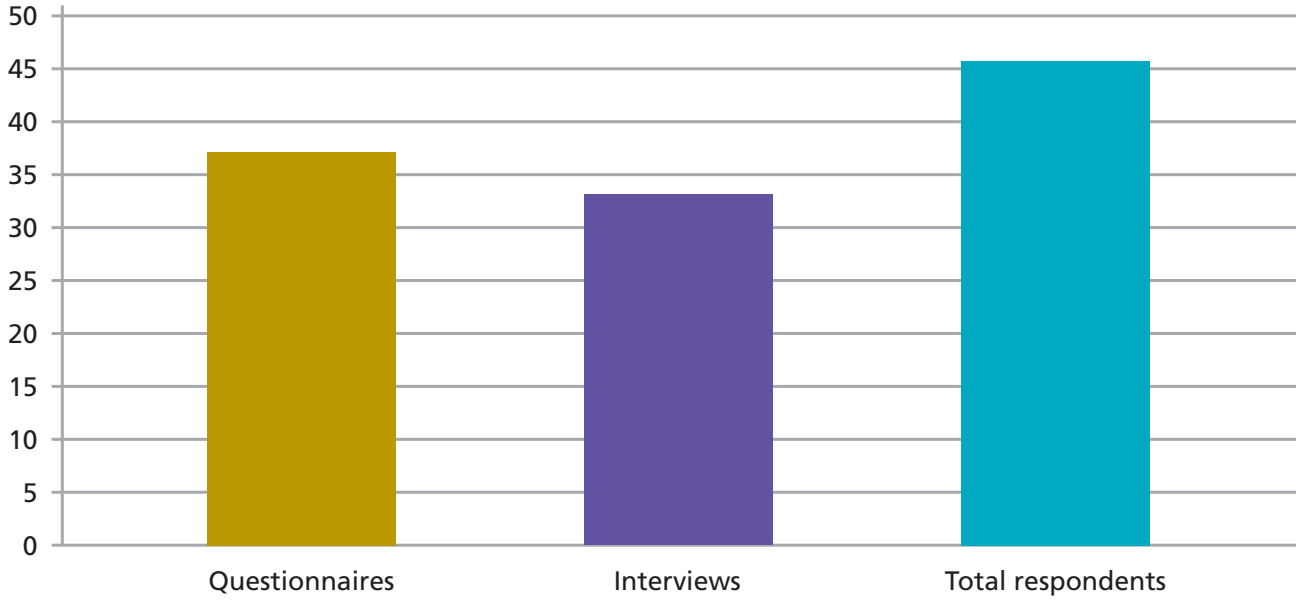


Figure 1: Organisations participating in the research by type of response.

Research participants ranged from national data protection authorities, national telecom regulatory authorities, telecom operators, consultants working for the private sector, and banking industry associations. Data protection authorities surveyed for this study oversee regulations for a combined population of more than 287 million people in Europe. Telecom operators surveyed reflected a range of operator types, ranging from fixed and mobile, to incumbents and alternative players, as well as operators with a regional presence, or a presence in only one country. Altogether, the operators surveyed for this study represent more than 160 million subscriptions to fixed and mobile services.

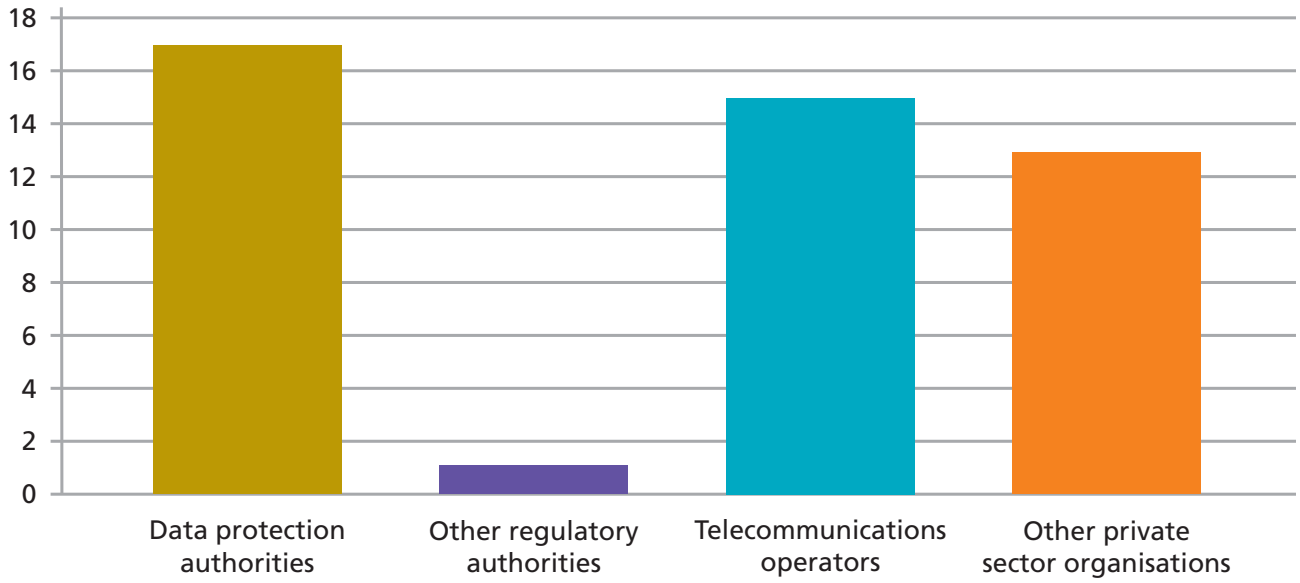
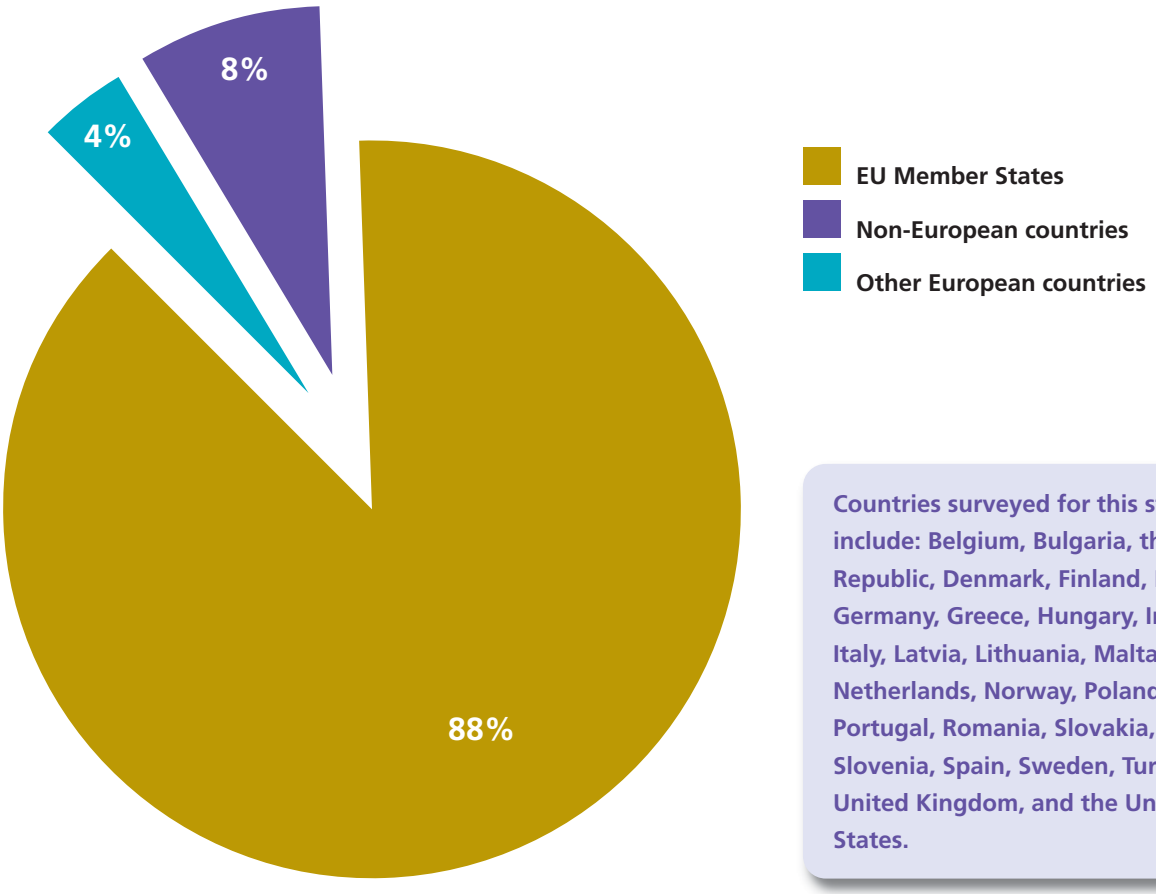


Figure 2: Organisations participating in the research by type of organisation.

Geographically, most respondents were located within the EU. In addition, ENISA also spoke to organisations with headquarters in Norway, plus the USA and Turkey. Most respondents referred to a specific national reporting environment, though some were also able to make regional and international comparisons.



Countries surveyed for this study include: Belgium, Bulgaria, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, the United Kingdom, and the United States.

Figure 3: Headquarters of organisations participating in the research.

Appendix B – secondary sources

The references for secondary sources were mentioned as footnotes throughout the text. We are grouping the most prominent ones here.

LEGISLATION

EUR-Lex "Directive 2002/58/EC," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

EUR-Lex "Directive 95/46/EC," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

EUR-Lex "Directive 2009/136/EC," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:EN:HTML

European Commission Information Society "Transposition table" http://ec.europa.eu/information_society/policy/ecomm/library/national_transposition/index_en.htm

EUROPA "Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens," http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/491

REGULATORY

Data Protection Commissioner, Ireland "Twenty First Annual Report of the Data Protection Commissioner 2009," http://www.dataprotection.ie/viewdoc.asp?DocID=1062&m=f

Data Protection Commissioner, Ireland "Personal Data Security Breach Code of Practice," http://www.dataprotection.ie/viewdoc.asp?DocID=1082&m=f

Data Protection Commissioner, Ireland "Report of the Data Protection Review Group" http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwithcover.pdf

Slovenian Information Commissioner, Slovenia "Information Commissioner Annual Report 2009," http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual-report-2009.pdf

PRIVATE SECTOR

Verizon Business "2009 Data Breach Investigations Report," http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Trustwave "Global Security Report, 2010," https://www.trustwave.com/whitePapers.php

7Safe "UK Security Breach Investigations Report," http://www.7safe.com/breach_report/Breach_report_2010.pdf

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu