Recommendations on technical implementation guidelines of Article 4

April 2012

enisa
European Network and Information Security Agency

About ENISA

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

Contact details

The editors of this report are Barbara DASKALA and Slawomir GORNIAK.

For questions related to this report or for general enquiries on the Privacy and Trust area in ENISA, please use the following details:

Email: sta@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Contributors to this report

This report was produced by ENISA using input and comments from an expert group. It should be noted that group members participate as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and individual group members may not agree with all of the observations and recommendations made in the report.

The contributors are listed below in alphabetical order:

- **Darren Bilby,** Google
- **Manuel García Sánchez,** Spanish Data Protection Authority, ES
- **Gwendal LeGrand,** Commission Nationale de l'Informatique et des Libertés (CNIL), FR
- **Jean Gonie,** Microsoft
- **Miroslaw Maj**, Cybersecurity Foundation
- **Konstantinos Moulinos**, Greek Data Protection Authority, GR
- **Sjoera Nas**, Dutch Data Protection Authority, NL
- **Melanie Shillito**, Promontory Financial Group, UK
- **Tomasz Soczynski ,** Polish Data Protection Authority, PL
- **David Sutton,** TACIT.TEL, UK

Acknowledgements

We would also like to acknowledge the following for their useful input at certain phases of our work (listed in alphabetical order):

- **Laurent Beslay**, European Commission, DG JRC, Institute for the Protection and Security of Citizens (IPSC)
- **James Gray,** European Commission, DG INFSO/B1 (observer)
- **Achim Klabunde,** European Commission, DG JUSTICE/ Data Protection Unit (observer)
- **Alain Pannetrat,** Commission Nationale de l'Informatique et des Libertés (CNIL), FR
- **Louis Velasco,** European Data Protection Supervisor
- **Pat Walshe,** Global Director of Privacy, GSM Association, UK

1. Executive summary

The introduction of a European data breach notification requirement for the electronic communication sector in the review of the ePrivacy Directive [5] is an important development with the potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data are being secured and protected by electronic communication sector operators. It is already clear that the legal requirements will go further, towards a general obligation of reporting data breaches to the competent authorities and individuals affected.

Article 4 of the ePrivacy Directive [5][6][7] foresees that the EC may adopt technical implementation measures, after consultation with three stakeholders: namely the Working Party on the Protection of Individuals (Art29WP), the European Data Protection Supervisor and ENISA. In this context, in 2011 ENISA set up an expert group comprising experts from the European Commission (DG Information Society and DG Justice), the European Data Protection Supervisor (EDPS), the Article 29 Working Party and the national Data Protection Authorities, as well as from the industry (telecommunication and other sectors). This group developed a set of recommendations for implementing the provisions of Article 4 of the Directive, focusing on the implementation areas that we believed would benefit from more specific technical guidelines. The top recommendations we make in our report are:

- **There is a need for a holistic personal data breach management procedure** – We do not see the personal data breach notification as a standalone process, and thus propose a set of steps / phases to be followed, based on standards and best practices for incident response management but with a particular focus on personal data protection: Plan and prepare, Detect and assess, Notify and respond, Collect evidence and Forensics, Review and improve.
- **It is important to be proactive and to plan appropriately** – The Directive states that providers must take appropriate technological and organisational measures to 'ensure a level of security appropriate to the risk presented'. To this effect, we highlight the important of having an appropriate risk management framework in place, presenting the minimum elements that such an approach should have and also providing a set of minimum appropriate technical and organisational controls, that the controller may define, and with a particular focus on those controls rendering data unintelligible. Companies should also define in advance appropriate plans to deal with personal data breaches, which can ensure that they respond quickly and effectively to a personal data breach.
- **Assessments** – Appropriately identifying the circumstances surrounding the personal data breach, as well as determining its severity and impact, is a major part of this work. We recommend performing the assessment in two stages: an initial stage (within 24 hours of detection of the data breach) and a more detailed one, which will enable the data controllers to comply with the provisions of Article 4, while appropriately identifying the severity of the breach. We also propose a specific methodology / approach to be used to calculate the severity / impact of the personal data breach;

- **Notifications** – According to the Directive, the data controller is obliged to notify the competent authorities without undue delay. Our recommendations on the notification process itself include, apart from the descriptions of the notification steps to be performed (two-phased notification, matching the two-phased assessment), the triggers and timing, the content of the notification and channels of communication to both the competent authorities and the individuals involved. Finally, we propose a common template that could be used by data controllers to notify the personal data breach to the competent authorities.
- **Review and improve** – Ensuring the continuous improvement of the data breach handling process is considered very important. Specifically, we make concrete proposals on identifying lessons learnt, as well as on keeping a data breach inventory.

Finally, we note that since the procedures of handling and notification of personal data breaches are still in an early stage of development, the proposed approach, and particularly the severity assessment methodology proposed, should be tested in practice, ideally using real cases. As ENISA intends to perform such pilots in 2012, the proposed severity assessment methodology, as well as other parts of the recommendations made in this report, may be updated as appropriate to reflect the results of the pilot.

2. Introduction

2.1 Background information

The introduction of a European data breach notification requirement for the electronic communication sector in the review of the ePrivacy Directive is an important development with the potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data are being secured and protected by electronic communication sector operators.

Moreover, Article 4 of the ePrivacy Directive [5][6][7] explicitly provides that the EC may adopt technical implementation measures, after consultation with three stakeholders: namely the Working Party on the Protection of Individuals (Art29WP), the European Data Protection Supervisor and ENISA.

Against this background, and in order to be appropriately prepared for this consultation, in 2010 ENISA reviewed the implementation measures and the procedures in EU Member States, as described by Article 4 of the reviewed Directive [5]. The study revealed that 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 [14].

As a continuation of its activities in the area of data breach notifications, on 24 January 2011 ENISA organised a dissemination workshop to present the results of the above-mentioned work, assess the current state of affairs and develop ideas on the way forward. During the workshop, several issues that need further attention were identified, including:

- Lack of a unified approach towards data breach notifications among sectors and among Member States, and in some cases a complete absence of such schemes
- Different understanding of the nature of a data breach
- Lack of guidelines, best practices, common formats of notifications
- Lack of guidelines on effective technical measures for protection of data
- Lack of guidelines on follow-up actions after notification
- Economics of notifications
- Cases of exemption from notification
- Lack of reliable and comprehensive data on data breach (trends and statistics)

Considering the above, ENISA launched its work on assisting the implementation of Article 4 in 2011, the result of which is the current report. More information on the scope and objectives of this work is given in the section below.

2.2 Scope and objectives

This report is the result of the work performed in the context of ENISA's work package on 'Supporting the implementation of the ePrivacy Directive (2002/58/EC)' (WP

3.3, ENISA Work Programme 2011) [13]. The work was done in consultation with an expert group set up and coordinated by ENISA. Members of the expert group included experts from EU Institutions (European Commission, EDPS) and the national Data Protection Authorities, as well as from the industry (telecommunication and other sectors).[1]

Its objective is to make specific recommendations for this implementation, providing appropriate guidance on the following aspects:

- A holistic approach to addressing data breaches and specific steps that the data controller needs to perform, with a particular emphasis on the prevention aspect
- The appropriate technological and organisational measures, provisioned by the Directive, especially those relating to 'data unintelligibility'
- Detection and assessment of the personal data breaches, and particularly on a methodology to assess the impact and severity of detected personal data breaches
- Procedures of notifications to competent authorities and individuals, in particular regarding timing, content and channels of communications.

At present the specific data breach notification obligation specified in Article 4 of Directive 2002/58/EC [5] only applies to a limited category of telephony and internet access providers. However, a general data breach notification obligation, applying to all data controllers in the public and private sector, has already been provided for in the reform proposal of an EU General Data Protection Regulation [articles 31 and 32]. In some EU Member States broader data breach notification obligations have already been implemented, and in some others it is likely that a general breach notification obligation will be introduced shortly, before the revision of the data protection directive.

Given these developments and the likelihood that the general requirements will be very similar to the existing specific ones, this work addresses *all categories of personal data breaches,* regardless of the nature of the data controller. We thus believe that these guidelines could be implemented not only by telecommunication service providers, but by parties in other sectors as well.

Finally, it should be noted that the focus of our work has been to provide input from an information security perspective, and while we recognise their importance, we have not considered any related legal issues. We have also aimed to propose guidelines that are technology-neutral, so the particularities of different technological platforms (e.g. cloud computing) have not been considered.

1 See the 'List of Contributors' section at the beginning of this report for the complete list of experts.

3. Definitions

Personal data breach: 'means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community' (in the amendment by Directive 2006/24/EC [6] and Directive 2009/136/EC [7] of Directive on Privacy and electronic communications 2002/58/EC [5]). It can be the result of an information security incident (see below) or of loss of user control.

Information security incident: 'An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security' [11].

Personal data: '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(a) of Directive 95/46/EC [4]). In our study we considered the analysis performed by the Art29WP on the explanation of the 'personal data' regarding the four main 'building blocks' that can be distinguished in the definition of 'personal data': i.e. 'any information', 'relating to', 'an identified or identifiable', 'natural person' (Opinion 4/2007 of the Article 29 Data Protection Working Party) [1].

Individual: any living natural person affected by the personal data breach. This includes users and subscribers, for private or for business purposes, without necessarily having subscribed to the service that is affected by the breach.

Sensitive personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. The scope of sensitive personal data is broad; for example, membership of a political party is seen as data revealing a political opinion (Directive 95/46/EC) [4]

Data controller:2 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 (Article 2(d) of Directive 95/46/EC) [4]

Data processor:3 the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Article 2(e) of Directive 95/46/EC) [4]

Control: measure that is modifying risk [10]

2 Refer also to the Article 29WP opinion 1/2010 on the concept of 'controller' and 'processor' WP169 [2]

3 Ibid.

NOTE 1: Controls for information security include any process, policy, procedure, guideline, practice or organisational structure, which can be administrative, technical, management, or legal in nature which modifies information security risk.

NOTE 2: Controls may not always exert the intended or assumed modifying effect.

NOTE 3: ‘Control’ is also used as a synonym for ‘safeguard’ or ‘countermeasure’.

4. Personal Data Breach Management Procedure: Overview

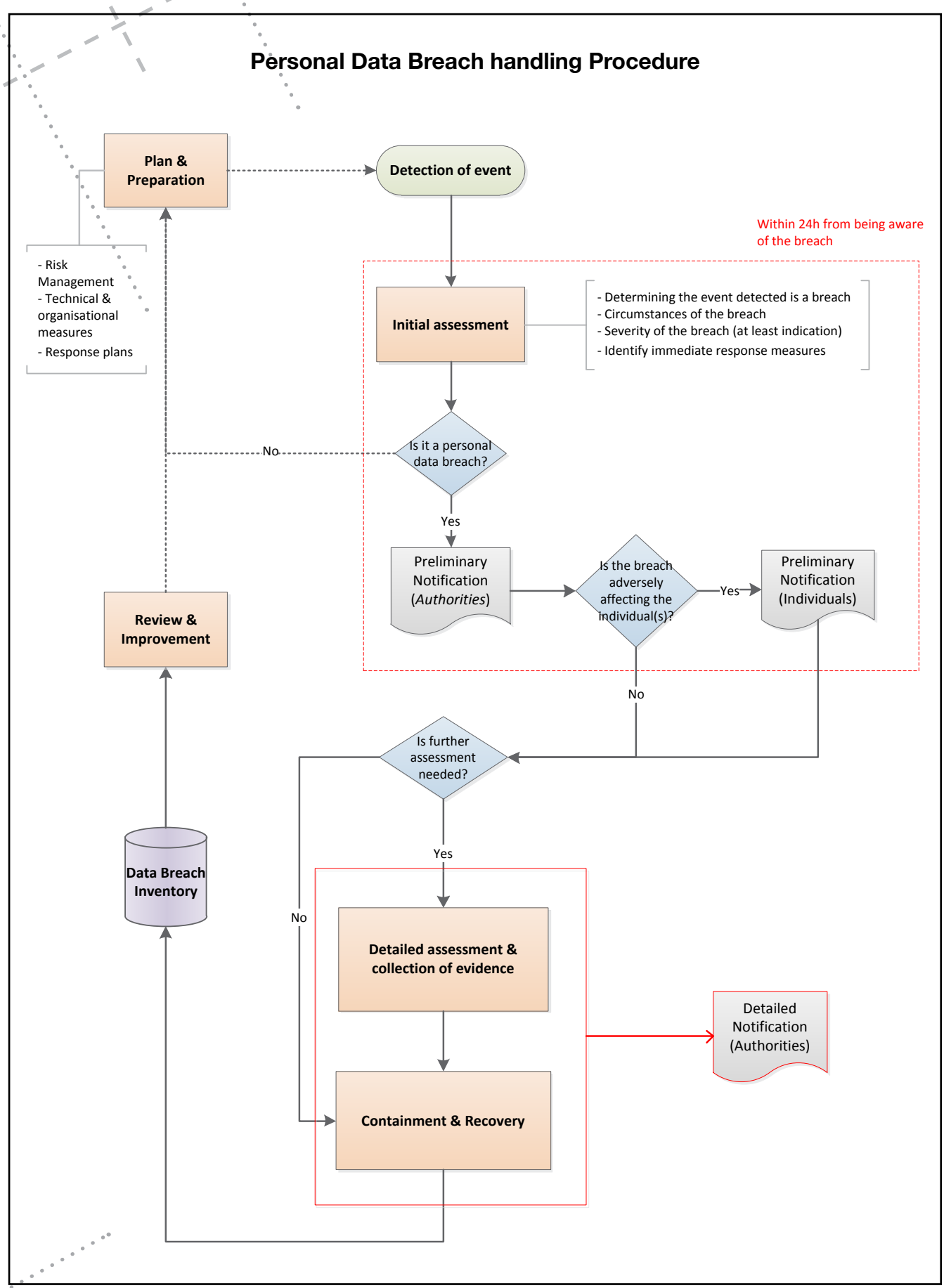
The data controller's obligation to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented, as well as to notify the personal data breach to the competent national authority and the individual, cannot be considered as standalone activities, especially from an information security management perspective. Since there are many additional requirements to consider in order to ensure the efficient and effective implementation of these two very important obligations, we recommend that they form part of a holistic and comprehensive personal data breach management procedure. We have therefore identified the following generic phases that should be considered in the implementation of a personal data breach management procedure, and which are based on existing security incident response management procedures (e.g. ISO standard [11]):

1. Plan and prepare
2. Detect and assess
3. Notify and respond
4. Collect evidence and carry out forensic analysis
5. Review and improve

These five phases are analysed in detail in the chapters that follow. In each one we make concrete recommendations focusing on the areas we believed would benefit from more specific technical guidelines.

Finally, the following flowchart presents an overview of the procedure, highlighting the major decision points that need to be made, particularly in the assessment and notification phases.

Personal Data Breach handling Procedure



5. Plan and prepare

The Directive specifically states that providers must take appropriate technological and organisational measures to ensure sufficient protection of personal data.[4] In the information security sphere this includes an entire spectrum of security controls. However, with regard to this obligation, we would like to highlight some basic elements that need to be considered and implemented.

5.1 Implement Risk Management procedures

Article 4 of the 'Directive on privacy and electronic communications' [5] states that: 'these measures shall ensure a level of security appropriate to the risk presented' and 'In case of a particular risk of a breach of the security of the network of the network, the provider [...] must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken'. Consequently, risk management practices constitute an important consideration for the implementation of Article 4.

The emphasis here is not the provision of the measures per se, but rather that those measures are 'appropriate', which is not always easy to determine. In order to accomplish this, organisations need to establish and follow a risk management framework. In this way potential risks can be determined, and most importantly, the appropriate controls be identified, in accordance with the levels of risk (acceptance of risk), importance of assets, etc. It is also important that organisations should consider carefully any residual risk that may be present after controls have been implemented in order to understand where there may still be potential for data breaches to occur.

Risk assessment is a core component of any information security management standard and framework (e.g. ISO 27001). Since this is a generic best practice for organisations, and is also in accordance with international standards and best practices, we will not present in much detail the risk management process that needs to be followed.[5]

To be better prepared to prevent, detect and react to personal data breaches, an organisation needs to have a risk management framework in place. The framework needs to be **focused on the protection of personal data, and identifying potential impact for the individuals,** as opposed to focusing on the risks concerning the business only, and on the protection of organisations against legal risks. We mention here the major elements that should be considered as a minimum in such a risk management process, and we also specify those that need to be considered additionally, especially for preventing personal data breaches:

1. **Identification and valuation of assets:** this step is a very important one, as it helps determine the system of reference on which the whole risk assessment will be based. The organisation needs to identify all the personal data it collects and where it is stored. The valuation phase means that the organisation would need to determine the value of these assets and the possible impact on the business processes and the individuals.

4 Article 4(1) of the ePrivacy Directive [5]. The obligation is included without prejudice to Directive 95/46/EC requirements [4].

5 For an overview of the major risk management best practices, standards and tools, see: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

2. **Identification and evaluation of vulnerabilities and threats:** having identified the assets, the organisation should identify the vulnerabilities of the assets, as well as the threats that are likely to exploit these vulnerabilities. There are many ways to do this, e.g. vulnerability assessments (host and network-based, penetration tests, etc.), as well as review of internal procedures, interviews of key personnel, etc. The estimation of the threats and vulnerabilities values may also be performed using various methods, depending on the risk management methodology used.

3. **Identification and evaluation of the final risk and the risk acceptance levels:** based on the above, the final risks and their risks levels should be determined. Normally, this marks the completion of the risk assessment, and at that point the organisation would need to determine its acceptance risk levels, i.e. which risks it is willing to accept.

4. **Risk treatment:** based on the previous step, the organisation will need to treat the risks that it is not willing to accept. The following strategies, based on ISO/IEC 27005:2011 [10], can be used to this effect:

   - **Risk reduction:** The first option is to mitigate risks, which means identifying appropriate controls that address the threats and vulnerabilities; in some cases they might even reduce the value of the asset. The appropriate technological and organisational measures provided for by the Directive can be identified at this stage (see next paragraph for more information on this).
   - **Risk Transfer:** The transfer of risk usually involves making a third party responsible for the action, for example by means of insurance against the possible financial consequences. However, in the context of personal data breaches, risk transfer would not normally appear to be an appropriate method of treating risk, since the data controller would still remain responsible for the data breaches. If the controller uses a data processor, the data processor must also implement appropriate technical and organisational measures to protect personal data against breaches and other unlawful forms of processing. However, the responsibility for the security of the processing remains with the initial data controller: the risk cannot legally be transferred to the processor.
   - **Risk Acceptance** (also referred to as risk tolerance): Risks should only be accepted when there is clear evidence that the cost of mitigation would greatly exceed the cost of the personal data breach. It may in some cases be possible (e.g. where data has been rendered unintelligible by some form of encryption) to accept the risk of a data breach, but the competent authority has to be notified anyway. Therefore risk acceptance must be carried out knowingly and objectively, it must be fully documented, and be subject to regular review.

5. **Dealing with residual risks:** It may also be the case that there are risks remaining after the risk treatment has been carried out (residual risks), in which case the organisation might choose to explore further mitigation procedures or to accept them. It is however important that the residual risks (especially if

accepted) must still be fully documented and notified to the competent authorities. This will help the competent authority to gain a better understanding of the organisation's risk environment.

5.2 Appropriate technological and organisational measures

Based on the risk assessment performed and in the context of the risk reduction exercise, the data controller should identify appropriate measures, i.e. measures that address the identified risks efficiently and effectively. In many risk management best practices and standards, the measures are also referred to as 'controls'. Below we provide examples of such controls and measures. It should be noted that this is not an exhaustive list of appropriate controls that the data controller can implement. In addition, measures in place need to be fully and clearly documented and subjected to review.

5.2.1 Policy & Organisational controls

- **Identify roles within the organisation:** Assign specific members of staff who may come into contact with personal data, instruct these staff appropriately in security awareness and give undertakings through contracts of employment, codes of conduct and acceptable use policies.
- **Promote a culture of security awareness amongst staff,** so that this approach is seen as the norm, rather than an additional requirement.
- **Comply with the data minimisation principle:** collect and store only the personal data that is absolutely necessary.
- **Compile and maintain an inventory of personal data breaches:** Whilst it is a legal obligation for data controllers in the electronic communications sector to maintain an inventory of personal data breaches (pursuant to Directive 2002/58 [5] amended in 2009 [7]), such an inventory is also an essential tool for the management to determine how to improve the security and robustness of the systems and procedures in place within the organisation. In this way, an inventory can be used in a preventive manner, as an important input to the risk management process. If an event has been classified as a personal data breach, it should be listed in the inventory of breaches. This inventory comprises at least the facts surrounding the breach, its effects and the remedial action taken. The person to whom the potential data breaches are reported should be in charge of keeping the inventory up to date. For more information on the inventory of the breaches, see section 8.3.

5.2.2 Technical controls

- **Identification, authentication and logical access control** in the systems used and operated by staff, to ensure that only authorised staff can access personal data, e.g. passwords, biometrics, two-factors authentication
- **Anonymisation of data6**

6 Data may be rendered anonymous when identification of the data subject is no longer possible.

- **Rendering the data unintelligible to any person who is not authorised to access them:** it is very important to mention this here, since according to the Directive, the implementation of this preventive control to the satisfaction of the competent authority might exempt the data controller from notifying the individuals.[7] For example, data stored in a simple password-protected file cannot be considered unintelligible. Data shall be considered unintelligible if either of the following apply:[8]

- It has been securely encrypted or hashed:

(a) The data was encrypted with a standardised secure symmetric or asymmetric encryption algorithm, or was hashed with a standardised cryptographic keyed hash function.

(b) The key used to encrypt or hash the data was not compromised in any security breach.

(c) The key used to encrypt or hash the data was generated so that it cannot be guessed by exhaustive key search with current available technological means.

- It has been securely deleted:

(a) It was on a medium that was physically destroyed or

(b) It was on a medium that was degaussed or

(c) It was deleted with a secure erasure algorithm (DoD, NIST, etc.)

- **Logging (event, security) and audit trails:** logging is an important detective and also deterrent control, capturing who did what and when.

5.2.3 Physical controls

These primarily relate to controlling the physical access to the systems, ensuring that only suitably authorised staff can access areas of the business where personal data are stored and processed, e.g. video surveillance, logging, escorting guests, etc.

It is noted that there are additional classifications of controls, e.g. into preventive, deterrent, detective, which are described in more detail in most risk management methodologies, best practices and standards.

5.3 Response plans to personal data breaches

7 Differences may also arise as far as the implementation of the exception relating to technological protection measures, which must render the data unintelligible to any person who is not authorized to access it. Such possible divergences may arise because under Article 4(3) it is for national competent authorities to assess whether the technological measures are appropriate and if they were applied' (Art29WP opinion WP 184) [3]

8 Information provided by Alain Pannetrat, Commission Nationale de l'Informatique et des Libertés (CNIL), FR

Companies should draw up appropriate plans to respond to personal data breaches. Such plans will be useful to ensure that they react adequately and in a timely manner if a personal data breach occurs. The goal of this section is to identify the key elements of an operational organisation that enable an efficient response to personal data breaches.

Again, it should be noted that these plans may form part of the security incident management procedures that may already be in place in organisations.

The business objectives of the plans concern rules and procedures at two different time scales:

- **short term:** to respond, contain personal data breaches, and get back to a normal situation. Containment procedures define the adequate responses depending on the assessment of the severity of the breach. In addition, the plans describe how to get back to the normal situation, if the containment procedures or if the breach itself has degraded the system. Notification procedures should also be included in this phase.
- **medium and long term:** to improve the security of the system. Indeed, response plans complement and feed into the risk analysis and breach prevention plans. The latter concern mainly theoretical scenarios and estimates of the risks to help manage security, whereas the former concern personal data breaches that have actually occurred, describe how to react in the short term and also how to make a post-mortem analysis, whose level of detail will vary according to the severity of the breach.

Consequently, the personal data breach response plan should consider at least the following elements *(for more information, please refer to Appendix D):*

1. **Identification of appropriate roles and responsibilities within the organisation**
2. **Identification and documentation of procedures:** the procedures for reporting potential personal data breaches should be documented and in line with the internal security incident management procedure, so as to facilitate their implementation.
3. **Response and collection of evidence procedures.** For each severity level, the procedures to react to personal data breaches should be defined, in order to contain them and limit their consequences. For a high level of severity, such procedures should include scenarios for which business operations will be temporarily stopped to avoid greater consequences of personal data breaches.
4. **Notification to competent authorities and individuals,** providing appropriate information about the personal data breach, as provided for in Article 4 of the Directive [5][6][7].

5.4 Exercising the plans

Responding effectively to a personal data breach requires regular testing of response plans and procedures to ensure that an organisation is fulfilling its duties in protecting personal data. Depending on an organisation and the risks it faces, exercising

response plans may be something done informally at regular intervals, or may be the function of a dedicated response team.

Generally an exercise will involve playing out an escalating personal data breach scenario. An exercise coordinator will be assigned to come up with a scenario and the key stakeholders will play out that scenario attempting to utilise the training and procedures that have been developed. Much has been written on the process of conducting response exercises or drills but, at a minimum, the following points in the response process should be covered in a data breach exercise:

1. Detection of the incident
2. Escalation procedures
3. Internal communications plan
4. Investigation procedures
5. Assessment of impact and severity
6. Notification procedures

For a brief summary of the possible options for exercising personal data breach plans, see APPENDIX E – *Options for exercising personal data breach plans.*

Example Scenarios

The following are some example scenarios that have been successfully used in conducting data breach exercises:

Scenario	Exercise phases
Laptop lost in taxi	1. User reports laptop stolen to IT department. Notes that he hadn't had time to run the encryption software on the machine. 2. Further information shows the user is in Sales and kept a spreadsheet called CustomerList.xls on his Desktop, which contains all customers including names, phone numbers and addresses. 3. Customer list contains customers in France and Germany. 4. Laptop is recovered 10 days later from a rubbish bin. Hard disk is missing.
Website compromise	1. Internal security audit of public web server shows a new administrative user created called adm1n. 2. Forensic analysis of web logs shows the download of 5GB of data from the website shortly after the user was created. 3. Analysis shows this is the size of the database at the time. Database contains credit cards, transactions and delivery information for 100,000 customers. 4. Two days after the account is removed, a copy of the database is posted publicly.
Attacker attempting blackmail	1. An anonymous party calls a company's public phone number and details a file they have that contains the salary and insurance information for all the company's employees. Threatens to release the file publicly unless they are paid €10,000. 2. Attacker offers proof in the form of two lines from the file. 3. Internal investigation shows the file exists on a shared file server in the company accessible to any employee. 4. Data from the file appears in a newspaper report exposing salaries and personal details of the top 10 earners in the company.
Unauthorised access to data stored pursuant to Directive 2006/24	1. Data extracted from a data warehouse for marketing purposes is stored on a USB stick owned by an employee of the sales department. File contains relevant data from a huge group of customers. 2. After being saved in a personal computer at the employee's home, the file is shared on the internet (P2P network) without being noticed 3. After three months, the controller receives a notification alerting over the issue. 4. There are no logs related to the extraction of the information from the data warehouse. The file does not offer clues over its origin. 5. After an investigation carried out by a competent authority, the file is linked to an IP address, the one corresponding to the internet service contract of the employee.

6. Detect and assess

6.1 Detecting the personal data breach

Possible risk areas where personal data breaches are more likely to occur should have been identified previously, during the risk management exercise. Therefore, the data controller should already have information on the following:

- **Critical assets** (procedures and data), which are likely to be affected by a personal data breach
- **Vulnerabilities of the assets,** that expose them to threats
- **Potential threats that can exploit the vulnerabilities.** Those can be:
  - **Man-made,** where the threat agent is human
  - **External** e.g. malicious attackers, internal e.g. disgruntled employees, accidental, or deliberate
  - **Physical / Environmental or non-human,** e.g. natural disaster, fire any form of automated malware

Having completed the risk management exercise successfully, the data controller is better prepared, thereby increasing the probability of detecting personal data breaches rapidly.

As mentioned previously, a personal data breach may occur in the context of an information security incident. In view of this, the detection of a personal data breach is related to the detection of an information security event. In this case information security incident management standards and best practices may be applicable. It should also be noted that not all information security incidents entail or lead to a personal data breach.

Reporting of a potential personal data breach may take place via human (e.g. individual, media etc.) or automatic means (e.g. alert systems, monitoring, intrusion and detection systems, etc.).

If the reported event involves personal data, then it is possible that a potential personal data breach has occurred, and the data controller needs to conduct an assessment of the breach.

Considering the provision of the Directive that the data controller needs to notify the personal data breach to the competent authorities and the individuals concerned without undue delay, as well as that in certain cases the data controller might actually need more time to determine the full impact of the personal data breach, we propose that the assessment of the detected potential data breach be done in two stages:

- **Phase I – Initial assessment**
- **Phase II – Detailed assessment**

It should be noted that this proposed two-phased approach aims to help the data controllers to correctly identify the circumstances around the data breach, giving them more time (beyond the 24 hours) to perform the assessments if needed, while still providing the minimum information to the compe-

tent authority and the individual, as specified in the directive. In this context, it follows that should the data controller be able to determine all the circumstances of the personal data breach and evaluate the severity and impact of the individuals within the threshold 24 hours, they do not need to follow this two-phased approach in assessing the personal data breach, and thus they would need to make only one notification.

6.2 Phase I – Initial assessment

The initial assessment should start as soon as it is determined that personal data are involved in the event detected. The objective of this phase is two-fold:

- the data controller determines whether the detected event is indeed a personal data breach
- to enable the data controller to determine to the extent possible (given the limited time frame) the circumstances of the breach and its severity, and notify without '*undue delay*', since this stage should not take more than 24 hours to complete (and will result in appropriately notifying the competent authority).

More specifically, at this stage, the data controller would need to identify the following:

- The cause of the event: and by what or whom
- Who and what the event affects or could affect
- At least an **indication** of the *severity* of the breach, using a pre-determined scale as indicated in 5.3 below. An '*indication*' means that the data controller may not be able to determine the final severity of the personal data breach at this stage, since they may not have full information about the event, as explained in the end of the previous section; however, the controller may still be in a position to estimate this severity, based on the information they have up to the point. The estimation of the severity of the breach will be based on the following two criteria:
  - The **type of personal data** involved in the event [for the definition of this see section 5.3] and the resulting identifiability
  - The **level of the exposure** (e.g. unauthorised disclosure, modification, loss of a device, theft, etc.)

Given the time limits data controllers have in order to notify, at this stage it may not be possible to perform a full impact assessment of the detected personal data breach. Hence, data controllers should always estimate the **potential maximum impact** considering the two criteria above. For more information on evaluating these two criteria, please refer to *APPENDIX B – Assessing the impact of a personal data breach [Informative].*

- Immediate response measures that could be taken

Since this is an initial assessment, it should take place immediately after the person-

al data breach is detected and the personal data breach can be notified without undue delay to the competent authority, in accordance with the Directive.

The results of this step would be presented in the preliminary notification to the competent authority (see next section for additional details on the timing and the content of the notification), which would need to be made *regardless of the impact / severity levels of the personal data breach.*

It should also be noted that it is important to verify the results of the initial assessment in the detailed assessment, when the data controller will have more time and more information, unless of course the data controller actually manages to perform the full detailed assessment in one step. This also means that the data controller should perform the detailed assessment regardless of the severity level estimated in the initial assessment, even if the initial estimation of the severity of the personal data breach detected is *Very Low* or *Negligible*, because further investigation might result in a change in this level.

6.3 Phase II – Detailed assessment

As we have already noted, the limited time frame of 24 hours might not be enough in certain cases for appropriate identification and assessment of the personal data breach. We would therefore recommend that in these cases the data controller performs a more detailed assessment to better *determine the circumstances around the breach and assess the impact of the breach.* The results of this assessment would then be part of the secondary notification to the competent authority (see section 7.1.1.1 for more information on this).

As noted in the Introduction to this report, we consider the assessment of the severity as a critical task in the personal data breach notification handling. In this context, we have worked on a methodology that could be used to appropriately assess the severity of the personal data breach, particularly focusing on the criteria that could be used to determine the severity, considering existing best practices and standards of impact assessments, and we present it in the following paragraphs, as well as in *APPENDIX B – Assessing the impact of a personal data breach [Informative].* We envisage that the proposed methodology be used by both the data controller and the competent authority (after they receive the notification) to assess the severity of the detected and notified personal data breach.

First of all, a personal data breach severity scale may be used to ‘grade’ the impact of personal data breaches. The following scale is proposed:

Overall impact assessment scale		
Overall Score	**Rating**	**Adverse effects**
1	**Low / Negligible**	No or negligible: Little problems or unpleasantness that can be easily overcome (e.g. loss of time, irritation, etc.)
2-3	**Medium**	Any adverse effects are not very serious and can be overcome, e.g. economic loss.
4-5	**High**	Considerable / somewhat serious, but they can be overcome with some effort, e.g. significant economic loss, social / reputation-related adverse effects
6-7	**Very High**	The adverse effects are extremely serious and significant effort would be required to address them or with possible permanent consequences that cannot be overcome by the people concerned; e.g. effects on health, or a combination of severe economic loss and bruising of one's reputation

The method used to assess the impact of the personal data breach has a particular focus on **the impact or the 'adverse effect'** [as specified in the Directive] that it will have on **the individuals** whose personal data have been breached.

In the second phase of our assessment, it is assumed that the data controller has determined most, if not all, of the data breach particulars, so the evaluation of the criteria below can be performed based on actual events and not on potential or probable ones.

We recommend that the following two criteria be considered when assessing the impact / severity of a personal data breach for the individuals:

A. **Identifiability of data:** the ability to identify an individual based on the personal data breached. The easier the identifiability, the higher the impact. In order to determine this, the type of personal data breached would need to be identified, e.g. ID data (name, address, data of birth, gender etc), sensitive data in the sense of the article 8 of Directive 95/46/EC [4] (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life).

B. **Level of exposure accomplished:** this will be based on the following:

   1. **Nature of the data breach, type of exposure:** the type of breach that took place, e.g. unauthorised or unlawful access, destruction, alteration / modification, disclosure, transmission, processing, storing, accidental or unlawful loss of personal data.

   2. **Preventive controls in place:** e.g. proper access control, encryption, backups and unintelligible data: the less the effort needed to use the data, the higher the exposure, and the severity of the personal data breach. These should

ideally have been determined through a risk management procedure, to ensure that they were appropriate.

3. **Delay to identify the breach:** The delay in identifying the breach is a parameter worthwhile considering, since the longer the delay the greater the possibility that the exposure levels have increased.

Both criteria will be evaluated using a scale from 1 to 4. The final impact will be calculated based on the following table:

Calculation of impact				
B. Level of exposure \ **A. Identifiability**	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**
2	**2**	**3**	**4**	**5**
3	**3**	**4**	**5**	**6**
4	**4**	**5**	**6**	**7**

For additional details on this and for a concrete approach to calculation see APPENDIX B – Assessing the impact of a personal data breach [Informative].

It should be noted that the data controller should also determine **the number of people affected by the personal data breach**, which although it should not be used as a criterion for assessing the impact of the personal data breach, is a parameter that needs to be notified to the competent authority.

It should also be noted that the assessment of the severity of the data breach is not a one-off process. This means that in the course of the forensic analysis, which may follow the data breach assessment, and in the light of new findings, extra assessments might take place. The data controller is then obliged to update, using the severity scale, the status of the data breach. Possible additional changes to the notification must be communicated to the competent authority without undue delay.

The results of this assessment should be included in the detailed notification to the competent authority.

It is a matter of fact that the outcome may vary according to the subjective scoring of its elements (especially as far as the data breaches of low and moderate impact are concerned). Thus, the competent authorities may, after consultation with the data controller, decide to readjust the scores of the data breach sever-

ity. It is thus important that **both the competent authorities and data controllers should apply the same criteria when determining if a breach notification should be issued to the individual.**

Once the personal data breach has been detected and confirmed, it should be registered in an inventory, regardless of whether it triggers notification to individuals or not (for more information on this see section 8.3). We consider that it is necessary for a data controller to have an incident handling capability as a prerequisite for maintaining this data breach database. The person who receives the initial report must initially log appropriate information related to the data breach and then determine if a particular security incident involves the breach of personal data.

6.4 Collection of evidence, forensic analysis

6.4.1 Collecting of evidence

Evidence gathering and handling is generally an essential part of the incident response basic flow.

Evidence collection depends on the type of investigation being carried out. As with police investigations, it is important to view the scene and survey the site. Computing systems are one point of investigation, but papers and digital media also hold important information for the investigation. For instance, certain encryption will only decrypt when the digital media is plugged in, and therefore the media is imperative to the investigation. In other cases the media may hold information that the suspect has deleted from the system. For more information on collecting evidence from computing resources, see *APPENDIX F – Collecting evidence from computing resources.*

Although the primary reason for gathering evidence during an incident is to resolve the incident, it is often needed for legal proceedings, too. For both reasons it is important to clearly document how all evidence, including compromised systems, has been preserved, as well as to collect the evidence according to procedures that meet applicable laws and regulations. In addition, creating a 'chain of custody' ensures documented transfer of evidence from person to person, and chain of custody forms should detail the transfer and include each party's signature. Evidence needs to be bagged, tagged and photographed. Each piece of evidence should be accompanied by a single evidence form; these forms should then be compiled into a multiple evidence form. It is always important to continue a proper chain of custody when further forensic analysis is required.

It should be noted that when collecting evidence regarding a personal data breach, the data controller needs to consider not only the internal needs, but also the requirements of the competent authorities and the individuals affected. If this is done properly, it will help avoid unnecessary duplications or even to omit necessary checks that can be formally requested by the authority during the investigation.

6.4.2 Forensic analysis

Forensic analysis is not a mandatory step in this procedure. If performed, it allows

the data controller to collect and analyse data breach evidence for better understanding of the incident itself, as well as to increase the chance that the data breach attack source will be determined and the criminals responsible caught. Activities related to forensic analysis should aim to answer the fundamental questions related to a data breach:

- Who is the source of the personal data breach?
- When did it happen?
- How was the attack conducted?
- What happened, especially what and how much data were breached?

The forensic analysis should be conducted in a structured manner, and, as relevant, identify what may be used as evidence, whether for internal disciplinary procedures or legal actions. The facilities needed for forensic analysis can be categorised into technical (e.g. audit tools, evidence recovery facilities), procedural, personnel and secure office facilities. Each forensic analysis activity should be fully documented, including as relevant photographs, audit trail analysis reports and data recovery logs.[9]

9 • ISO/IEC 17025:2005

7. Respond and notify

7.1 Containment and recovery

The containment and recovery actions would need to be performed after the completion of each assessment phase, namely:

- **Immediate response:** Based on the personal data breach assessment results after the initial assessment, the data controller should proceed immediately with the implementation of appropriate measures to contain the breach and to recover immediately any data loss to the extent possible.
- **Additional containment and recovery:** After conducting the detailed assessment and further evidence collection and forensic analysis, additional containment and recovery actions may need to be identified and implemented

The containment and recovery controls / measures to be taken should already have been identified in a personal data breach and response plan. In addition, they will depend on the actual circumstances of the personal data breach. However, we mention here a few examples of the containment and recovery tasks which should be carried out:

- Change passwords to all operating systems and applications which were involved in the data breach. If these credentials are used in any other mechanisms (e.g. data transfer applications) they should be changed in these mechanisms.
- Change or cancel all credentials that were breached, or advise individuals to do it. This concerns especially credentials data of other services (e.g. email accounts) or credit card data.
- Identify and remove all processes from systems which are not original and are not documented in systems' documentation. This process can include malicious operations and mechanisms which can cause further breaches of data. It should be taken into account that some malicious processes are not easily detected by standard operating systems tools and this process needs some deeper investigation.
- Identify and remove all system and application files from systems which are not original or authorised and are not documented in systems' documentations. Alternatively, they should be replaced with original files if it is known that they were corrupted. One way of detecting this is to compare their checksums (e.g. for this purpose the programs for integrity checking can be used).
- Limit access to attacked services. At the beginning of the recovery process generally the best option is to limit or even block access to all services. Then, after it has been determined which parts of services were attacked, access to them should be limited. In particular, the data controller should investigate suspect or vulnerable processes and user accounts which could be used to attack a system. It is best practice to make a copy of the corrupted system for the further investigation; the copy should be done with tools which ensure read-only operations to protect the original integrity of the affected system.
- In case encrypted data has been compromised (e.g. copied, etc.), then the data should be re-encrypted in the system using another key.

This should provide feedback for the review and improvement process (see chapter 8). Also, since this is the first response, additional containment and recovery actions might be deemed necessary later on.

All the actions performed during this phase should be properly documented, and should also be include in the notification to the competent authority, as provided for in the Directive.

7.2 Notification to the competent authority and the individual

The Directive imposes an obligation on providers of publicly available electronic communications services that all incidents in which personal data has been put at risk ['accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure'] should be reported to the competent authority.

Notwithstanding this obligation, the national competent authorities may adopt their own guidelines and, where appropriate, issue instructions concerning the circumstances in which data controllers are required to notify personal data breaches to the competent authority, the format of such notification and the manner in which the notification is to be made (Article 4(4)) [5] [7]).

7.2.1 Triggers and timing of the notification

The definition of what constitutes a personal data breach in the revised e-Privacy Directive is very broad. This means that, at one end of the scale, notification will be triggered when the breach has the potential to result in financial, physical, or other harm to the individual. At the other end of the scale, notification could be triggered merely by the risk, i.e. the 'possibility' that personal data was breached.

7.2.1.1 To the competent authorities

The wording in the revised e-Privacy directive, 'without undue delay', seems to give some leeway as to the timing of the notification, but only insofar as this is justified. In other words, individuals and authorities should be notified as soon as possible. The Directive has not been transposed in the same way in all Member States regarding the time thresholds. Some require notification within 24 hours, others give more flexibility, linking it to the assessed severity of the breach, i.e. the more severe, the tighter the deadline to notify, as well as performing periodic reports that would cover minor breaches, mostly to minimise the risk of a possible notification fatigue,[10] where the competent authorities receive too many notifications. Moreover, it is argued that less frequent notifications are more likely to attract individuals' attention.

Considering this, and the limited time the Directive has been in place, we have limited experience and indications regarding the actual requirements, and of whether there is in fact a high risk of such notification fatigue.

10 As mentioned in the ENISA report [14].

In this context, we would like to recommend a two-phased approach to notification, based on the two-phased assessment presented in the previous chapter, which may better address these concerns, namely:

- **Preliminary notification** – the data controller should make this notification without undue delay, and within the range of **24 hours** after the data controller has become aware of the personal data breach, during which time the data controller should have performed the initial assessment (see section 6.2). As provided for in the Directive, the preliminary notification would actually include some basic information on the personal data breach gained from the initial assessment, and should be quick and easy for the data controller to make. In the next paragraph, we discuss the notification content in more detail. The data controller can use the same notification template as in the detailed notification, and just fill in the fields that they can at that stage. For a proposed notification template please refer to *APPENDIX A – Example template of a data breach notification form to the competent authorities.*
- **Detailed notification** – when after the preliminary assessment of the breach, the data controller has performed further analysis on the breach, determining its severity level more accurately, as well as gaining more information on the circumstances, then the controller needs to notify these additional assessment results in a follow-up detailed notification to the competent authority. Depending on these results, the data controller may also need to notify the individual. In terms of time thresholds, we recommend that the data controller be given additional time to perform a detailed assessment of the personal data breach, in case the first assessment was not comprehensive enough, and also in order to notify the results of this assessment properly to the competent authority. Specifically, we would recommend that the detailed notifications be done as quickly as possible, but no later than the following thresholds based on the initial impact assessment results:

Proposed timescales for detailed notification to CAs		
Overall impact	**Adverse effects**	**Thresholds**
2-3	Impact is limited: any adverse effects are not very serious and can be overcome	**<15 days**
4-5	The adverse effects are somewhat serious, but they can be overcome	**<10 days**
6-7	The adverse effects are very serious and significant effort would be required to address them	**<7 days**

If a data controller initially estimated a severity that is much lower than the severity / impact assessed in the detailed assessment, then the data controller needs to take note and observe the above thresholds, as soon as possible.

We consider that this approach achieves the correct balance between notifying all personal data breaches without undue delay to the competent authority and the need to allow the data controller sufficient time, if needed, to further assess the circumstances surrounding the personal data breaches and their impact. We recommend that **if the severity of a personal data breach is estimated in both initial and detailed assessments as of low or negligible impact (overall score 1), no further notification to the competent authority should be required.**

This is also in line with best practices followed in information security incident management [see diagram from ISO/IEC 27035:2011 standard in *APPENDIX C – Information security event and incident flow diagram [ISO/IEC 27035:2011]]*, where a first assessment with an initial decision is envisaged. This also allows for confirming whether a personal data breach is actually a false alarm.

In the case that a data breach occurs at or by a data processor, the data controller remains ultimately responsible for the breach. This means that where required, the personal data breach notification to the individual(s) should come from the data controller with whom the affected individuals already have a relationship. The data processor must notify the data controller without undue delay in the case of a personal data breach.[11]

It is recommended that the obligation of the data processor to notify the data controller immediately if a personal data breach occurs be set out in a contract. To the extent possible, the data processor should provide the data controller with the identification of each individual affected by the breach as well as any information that the data controller is required to provide in its notification to the authorities and affected individuals. Other important issues of such a contract, such as the notification costs, legal costs and investigation costs, are beyond the scope of this document. Cloud computing cases, when a data processor is in the cloud, might be handled in a similar fashion.

7.2.1.2 To the individuals

It is particularly relevant to assess the consequences of potential personal data breaches to determine whether or not a notification to individuals is required. The adverse effects that an individual may suffer as a result of the data breach are an element of the data breach assessment method proposed in chapter 4.

Taking into account the proposed approach and the requirements of the Directive, the data controller can be exempt from notifying the individuals in the following two cases:

- The *appropriateness* of the implemented technological measures, specifically *unintelligibility* of the compromised data: if such measures have been

11 If there is a legal agreement between the data processor and the data controller which assigns the notification responsibility to the data processor, then this rule will not apply.

applied and they render the data unintelligible, then notification to the individuals is not required.

The *impact* of the data breach (see chapter 6 on assessing a personal data breach): if the adverse effects of the personal data breach are **very low / negligible** (according to our metric scale in the table in section 6.3, then the data controller does not have to notify the individual.

For personal data breaches that do not fall in any of the above two cases and where the personal data breach is likely to adversely affect the individual, the data controller must notify the individuals as well. It should be noted that this notification is an important element of risk mitigation of a data breach as the sooner it is notified the sooner the individual concerned can take appropriate countermeasures. As a result, undue delay is determined on the basis of whether the subscriber is able to take appropriate measures to mitigate the risks involved with the specific data breach.

As provisioned above in the preliminary notification to the competent authority, the data controller should notify the individuals without undue delay and **within 24 hours after the controller has become aware of the personal data breach affecting the individual.** Even if not all possibly affected individuals are identified and / or can be notified within that time period, the data controller should start by notifying those individuals who have been identified and whom he can reach.

A personal data breach may be the result of a criminal action that the data controller either wishes, or is required, to report to the relevant law enforcement authority. If the law enforcement authority, in consultation with the competent authority, deems that notification of the breach to an individual will compromise an ongoing investigation, the reporting procedures and timelines will need to be amended accordingly.

If a data processor is involved, then the above-mentioned timelines must be applied on the data processor. The data controller should then notify the affected individuals within 24 hours.

7.2.2 Content of notification

Data controllers should notify the competent authorities of all relevant facts related to a personal data breach. Some of the information included in the notification will be used by the competent authority for data breach case analysis. This is very important to enable the Competent Authority to fulfil its duty of building awareness among data controllers as well as the general public (individuals). The competent authority will be able to observe and analyse trends and prepare concrete, helpful advice for all parties involved in personal data processing, as well as individuals.

The data controller decides whether or not individuals have to be notified, based on the likely adverse effects on the individuals and the appropriate technological measures in place (see section 7.1.1.2). However, the authority verifies the notification (or absence thereof) after the face, exploring whether or not a decision not to notify is justified, and, if a notification was given, whether the notification meets the legal criteria. To allow for this ex-post verification, the notification file should contain a field where the data controller

explains and motivates a decision not to notify (some) individuals.

It is highly recommended that the personal data breach notification format be:

- **standardised across all competent authorities.** The recommended method for ensuring this is to prepare the standardised form (e.g. web-form with the necessary high level of protection). A requirements description using a semi-formal language of such process is presented in *APPENDIX A – Example template of a data breach notification form to the competent authorities.*
- **submitted electronically to the competent authorities:** this is specifically recommended for the preliminary notification, in order to allow for quicker and more straightforward submission.
- **A reliable source of comparable statistics and indicators at national and EU level**

7.2.3 Notification to the competent authority

The notification content is described in Art. 4(3), of the ePrivacy Directive as follows:

> *'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 to the notification to the data subjects, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.'*

As such, the following is the minimum set of information a provider must report to the competent authorities. For the preliminary notification, the data controller should notify with only the information they have ready at the time, based also on what is recommended in section 6.2 of this report:

1. Contact details (e.g. name, postal address, email address) for the organisation and the reporting person
2. Information about contact person for this notification (if different from the one who is reporting)
3. Data Controllers involved (for large global organisations, a breach can occur across more than one entity)
4. Date and time of notification
5. Date and time when the data breach was established
6. (Estimated) date and time of occurrence of the data breach
7. Type of personal data breached
8. A short summary of the event (when, why, who, what happened, etc.)
9. The results of the impact / severity assessment performed, including the way this was calculated, based on the criteria laid out in section 6.2 above: this will

include the nature and the consequences of the data breach, provisioned in Article 4(3) of the ePrivacy Directive [5][6] [7].

10. Number of individuals impacted or likely to be impacted
11. Actions taken or services offered to the individual
12. Information about the resolution of the data breach:
    a. actions taken to handle the data breach and its impacts,
    b. actions planned in order to prevent further breaches.

Other useful information that might be reported, to the extent that it is available, includes:

13. Content of the notification to the individuals (if applicable) or reason for not notifying the individuals affected (e.g. appropriate controls in place, list of the controls)
14. Communication channels used to notify the affected individuals (if applicable)
15. Cross-border data breach (if applicable), e.g. competent authorities that have been informed

7.2.4 Notification to the individuals

The notification to the individuals must, at least, include:

- Information about the contact point (where the individual may go to get more information about the data breach) with the data controller
- Incident description including what personal data has been compromised and how. The information should be in language that is easy to understand
- If relevant, what service the data controller is offering the individual to mitigate the adverse effects as well as what steps individuals could consider taking themselves in order to mitigate the adverse effects.

Other useful information that may be reported, to the extent that it is available, includes:

- Type of data lost or compromised
- Likely impacts from the breach
- Mitigation actions already taken or that will be taken by the data controller
- Steps being put in place so to help ensure it will not happen again.

The level of detail of the information communicated to the individuals is left at the discretion of the data controller. Technology-neutral solutions must be selected to automate the data breach notification process. This solution should emphasise not only on the internet but also mobile applications.

7.2.5 Channels of communication

Every data controller must be prepared to respond to a possible data breach. Apart from the technical skills, the data controller should have the right communication capabilities in order to inform the parties involved in the data breach notification

process. For this reason, the controller must prepare a communication plan emphasising: a) internal communications, b) communication with competent and law enforcement authorities where relevant, and c) communication with the affected individuals. The aim of this communication plan is to minimise the impact of the breach on the individuals and on the reputation of the organisation. The data controller should exercise the effectiveness of his communication plan from time to time and keep it up to date.

It is recommended that when notifications are communicated to either the competent authority or to the individuals by electronic means, a technology-neutral solution must be selected to automate the process. This solution should emphasise not only the internet but also mobile applications. Particular measures must be taken in order to protect the security of the communication channel (e.g. encryption) and the authentication of the data subject.

7.2.5.1 Communicating with the competent authority

The revised e-Privacy Directive is not specific about the means of notifying the competent authority. Possible ways of notification are:[12] by telephone, by fax, by letter, by email and by electronic form on a website. The template of this form may be either stored in a file using a word processing tool (e.g. word, pdf etc) or designed using a form design tool.

Because of the flexibility and efficiency of electronic communication a notification procedure by an electronic form on a website or an XML-based messaging exchange system is highly recommended. A telephone channel and email are recommended as redundant solutions. A web-form helps data controllers to notify efficiently, while keeping the administrative overhead relatively small – especially if it is complemented by an electronic registry of incoming notifications. Particular measures must be taken to protect the security of the communication channel (e.g. encryption) to ensure the breach is not compounded further by communicating the details over a non-secure channel.

7.2.5.2 Communicating with the individuals

Notification should take place in a manner which ensures that the individuals affected receive fast and actual notice of the incident and the steps they should take to reduce the adverse effects they might suffer due to the personal data breach. Providers may use different means of notifying subscribers or individuals, depending on the type of data breach. Such means include registered mail, traditional mail, telephone (GSM or PSTN), email, press, broadcast media and website postings.

Data controllers should be allowed to determine the appropriate channel of secure communication for notification of personal data breaches to individuals, taking into account the circumstances of the data breach. For example, in cases where it is important to immediately and specifically address the individual in order to provide

12 "It should be noted that legal means of notification can vary according to the national legislation.

guidance on mitigating the risks caused by the data breach (e.g. to change passwords), direct communication means should be used (telephone or email). If email is used no personal data should be included in the title or body of the email unless it is sent over an encrypted channel. In cases where this is not possible (e.g. the communication information of the user is not known) or is not needed (e.g. when the subscriber or user cannot take immediate action to mitigate risks), web postings or media could be used.

An important issue when communicating with individuals is the quality of the contact information. For example, if a breach requires notification to a large number of individuals, it is possible that the contact information for many of the subjects may be 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 [14].

Although email is a quick and effective method of communication, the data controller should take into account, when sending email, that individuals tend to discard emails concerning breaches or security events because they might consider them as phishing or spam. In addition such an email communication would need to be encrypted, to ensure that it remains confidential.

The competent authority should be able to test these notifications against objective criteria to make sure that the notification fulfils its purpose, which is to appropriately inform the data subject. For it to do this, some formal and some material criteria have to be met. Formally, the information must:

1) be likely to reach the end-user;
2) be readable in terms of font size, colour and layout. Consideration should be given to special categories of people such as the elderly, and people with visual or hearing impairments or speech difficulties. For example, a large font size posting might be needed for people with vision problems;
3) be comprehensible to the average customer: conciseness and with good quality information in relation to the targeted individuals. If the average customer of a specific service is a minor, the message has to be age-adapted. The notification must be adapted to the language agreed with the data subject to the extent that this is possible;
4) be communicated separately from other information or communication.

8. Review and improvement

8.1 Introduction

The preceding chapters have analysed in detail all the issues related to how to detect, mitigate, evaluate and proceed with a notification to the competent authorities and / or individuals in the event of a security breach. Nevertheless, after the incident there are still pending tasks related to the analysis of the breach as a whole in order to identify the lessons learnt, the improvements to the security measures and controls in place as well as, if needed, to the data breach management scheme itself.

One of the main goals of the data breach notification system is to ensure that a feedback cycle is put in place allowing for continuous improvement on all the processes related to information security as well as proper dissemination and sharing of best practices and lessons learnt.

This task must be assumed by both the competent authorities and providers and is clearly defined in recital 58[13] of Directive 2009/136/EC [7], when stating the role of the competent authorities in promoting the interest of the citizens by ensuring a high protection level of personal data and privacy and the need to guarantee that they have all the necessary means to carry out their duties, including, in this case, 'comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised'.

To that end, the authorities need to monitor measures taken and, if they deem it appropriate, to disseminate best practices among providers.

In addition, controllers should maintain 'an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities'.

This means that the need to ensure the continuous improvement of the processes related to information security transcends the particular interest of the provider as such and becomes a common interest for all the stakeholders. Article 4(4) of the Directive [5][7] introduces that obligation, confirming the importance of the inventory of data breaches as a core element of the data breach notification scheme.

8.2 Identification of lessons learnt

Once a mitigation process has been implemented and the situation has been stabilised, it still remains vital to invest some time on lessons learnt. Those lessons should be focused on how to improve the information security system in terms of both technical and organisational measures, as well as on the breach management scheme, paying special attention to everything related to the notification process.

This effort should be carried out by all the parties involved and should cover the following questions:

13 'Recitals' in EU directives set out the reasons for the provisions that follow. Recital 58 states: 'The competent national authorities should promote the interests of citizens by, inter alia, contributing to ensuring a high level of protection of personal data and privacy. To this end, competent national authorities should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities.'

- Is there enough knowledge about the root causes of the breach?
- Is there enough knowledge about the particular technical or organisational weaknesses which facilitated the breach?
- Was the reaction to the breach quick enough?
- Were the consequences of the breach effectively limited / mitigated?
- Has all the evidence related to the breach been gathered /recorded?
- Have all the steps relating to the notification process to the competent authority been followed?
- If so, is it reasonable to expect that all the affected individuals have been properly informed and advised about the breach?
- Is there a need for additional technical or organisational resources or actions that can prevent similar breaches?
- Is there a need for additional training or awareness efforts?
- Is there a need for third-party feedback and / or support?

The depth of the analysis must be in proportion to the severity of the breach. However, there is a clear benefit in paying some attention to all detected incidents; a serious breach could have its source in a chain of minor vulnerabilities.

8.2.1 Improvements to information security measures and controls

Apart from the regular processes of monitoring and reviewing the information security measures and controls in place, a review of the measures directly related to a particular breach should be part of the follow-up activities. The need for new or updated technical and / or organisational measures as a result of the analysis should lead to proper planning and implementation of the changes. If necessary, a global analysis of the information security system should be conducted.

8.2.2 Improvements to data breach management and notification scheme

Ensuring proper feedback also implies reviewing both the internal data breach management scheme and all the processes related to the notification to the competent authority as well as to individuals.

Relevant findings need to be shared with all the parties involved and, when appropriate, trigger relevant changes. Any event or finding deemed useful to improve the working of the system should also be shared with the competent authority responsible for the smooth functioning of the system.

An initial approach to this review would imply, at least, the analysis of the following aspects:

- Whether the relevant procedures of the notification system work as expected;
- The process of obtaining relevant information about the breach;
- If necessary, further improvement of the indicators used to evaluate the severity of the breach;

- Whether the information provided in the notification complies with the expectations of both the authority and the controller;
- Unnecessary delays in the notification;
- Accuracy of the information provided;
- The possible lack of procedures or tools aiming to enhance the quality of the notification process;
- The usefulness of the communications channel in place and the identification of any procedure or tool allowing for a better notification process; and
- Any observation or recommendation made by the competent authority or by individuals involved in the breach.

8.3 Data Breach Inventory

Article 4(4)[14] of the ePrivacy Directive makes provision for an obligation for the controllers to maintain a register of the facts regarding breaches, as well as information on the known effects and remedial actions taken. The information included in the inventory should be sufficient to enable the competent national authorities to fulfil their tasks related to the verification of compliance by the controllers. The article also states that the information included in the inventory should be only that necessary to achieve that purpose.

To properly understand the significance of this provision, it is necessary to take into account what recital 58 stands for; i.e. the need for the competent authorities to have adequate means to carry out their duties, *inter alia,* monitoring measures taken in response to security breaches as well as disseminating best practices.

A register of security incidents is a common tool in business continuity plans or Information Security Management System (ISMS). It has also been adopted by some Member States[15] when developing security rules to be adopted by data controllers. In some cases, there is also a requirement to make its contents available to the competent authorities. But the ePrivacy Directive goes beyond this by creating a specific link between the obligation assumed by the controller and the task assigned to the competent authorities.

However, the Directive is not very specific on what an inventory of data breaches should look like or how its content could be released to the competent authorities by controllers who may be reluctant to disclose certain information to third parties due to the technical and even commercial implications associated with an uncontrolled dissemination of the information. To complete the picture, there is also a need to make clear which information may be deemed necessary

14 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. The inventory shall only include the information necessary for this purpose.'

15 In Spain, Article 90 of the Regulation implementing Data Protection Law states: '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 occurred or, if appropriate, was detected, the person making the notification, to whom it was communicated, the effect arising from it and the corrective measures applied.'

to be included, as the last sentence of the article indicates that excessive information should not be provided.

8.3.1 Content of the inventory

The content of the inventory is based on the content requirements for a notification set out in section 7.1.2 of this report. It is recommended that the inventory should include, apart from the notification itself, information as well as factual and documentary evidence supporting what has been provided in the notification, namely:

- Time references;
- The nature and the subject of the breach;
- Individuals involved, if any;
- Type of data involved in the breach;
- The assessment on the severity of the breach;
- Measures – both technical and organisational – applied;
- Person or department responsible for the breach to be addressed by the competent authorities;
- Information on when and how individuals have been notified; and
- Other technical and administrative information deemed necessary by the controller.

The main beneficiary of the content is of course the competent authority, presenting the information in this way has many benefits for the controller. The inventory can be seen as a valuable internal source for enhancing technical measures and organisational proceedings.

8.3.2 Access to the content of the inventory

By its very nature, the inventory has certain characteristics that should prevent widespread access to it. This is because, first, it includes technical information – including processes and instructions – about both the information system and the breaches and, second, because of the personal data that could be included in the notification files as part of the elements of analysis or notification efforts. From this standpoint, a certain level control over the access and use of the information should be an integral part of the system.

According to Article 4(4) of the Directive [5][6] the natural users of the inventory are the officials of the competent authorities, who are usually subject to a duty of professional secrecy; the same should apply to the staff members of the controllers. Finally, access by third parties must be preceded by the signing of a confidentiality agreement and compliance with all legal obligations. As a best practice, all the accesses to the inventory should be properly recorded.

8.3.3 Security measures

The controller should guarantee the implementation of technical and organisational measures aimed at creating a sound security schema for the inventory to ensure the

confidentiality and the integrity of the information as well as the availability of the inventory. For possible controls, see section 5.2 this report on appropriate technological and organisational measures.

8.3.4 The inventory as personal data processing

As stated previously, the inventory can store personal data related either to the breaches or to the notification to the individuals. Depending on the source – system images, logs, database content, personal records – and the format, the data can have varying degrees of sensitivity and can be accessed with a greater or lesser degree of difficulty.

The inventory should be seen as personal data processing that is legally subject to the obligations laid down by data protection legislation, including information to individuals, notification to the competent authorities and proper security measures.

8.3.5 Data retention

The Directive does not make any provision for a data retention period applicable to the information included in the inventory of data breaches. However, taking into account the statutes of the competent authorities, it could be considered that a retention period might apply based on the statute of limitations period associated with the breaches, or on the possibility that the competent authorities may start investigations or enforcement actions. The same could apply with regard to possible responsibilities with respect to the civil, criminal or administrative law.

Upon expiry of that period the controller can keep the technical information according to its own policy and depending on its usefulness. However, personal data should be kept only on the proviso that, according to data protection legislation, it must be in a form that permits the identification of individuals for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Therefore, the use of a dissociation procedure to render the data anonymous is strongly recommended as a best practice.

8.3.6 Further use of the inventory

The inventory of data breaches can be considered as a high-value asset for the controller as far as it represents a relevant source of information for analysis in order to identify trends and patterns and specific areas of concern for the controller, as well as a way to identify areas where action is needed in order to prevent breaches. To that extent, the information included in the inventory should be organised in a way that allows for effective analysis in order to gain relevant information that can be shared inside the company as well as with relevant third parties.

9. Roles and responsibilities

Three main entities participate in the notification process: the data controller (and / or the data processor), the competent authority, and the individual(s) affected. This chapter provides a high-level overview of their responsibilities, especially within the organisation of the data controller. It is noted that existing roles of an incident response team, etc., are assumed.

Data Controller

At the Data Controller level the actions may be performed by the following roles:

- Employees / users
- Data Protection Officer [DPO]
- Chief Information Security Officer [CISO]
- Information security incident response team [IRT]
- IT operations team [IT]
- Legal department [LD]
- Dedicated ad-hoc personal data breach response team [DBRT]. Ideally members of this team should be the CISO and the representatives of IRT, IT and LD.
- Senior management [MGT]

Specific responsibilities include:

- Perform risk management of the organisation with the focus on the impact on the individual [MGT, CISO, DPO]
- Implement appropriate technological and organisational measures in order to prevent personal data breaches, based on the results of the risk management [MGT, IT, DPO, CISO]
- Develop and document procedures for responding to personal data breaches [LD, DPO, IRT]
- Detect the personal data breach [user, IRT, IT, external party detecting a breach]
- Perform the initial and detailed assessments of a breach once it has been detected [DBRT, IRT, IT, DPO]
- Notify the competent authority without undue delay , i.e. 24 hours after having become aware of a personal data breach breach [DBRT, DPO, LD]
- Notify the individual or individuals affected by the personal data breach without undue delay and inform them of proactive measures they can undertake to appropriately protect themselves [DPO, LD]. Perform the recovery after the breach [DPO, CISO, IT]
- Identify the lessons learnt and implement improvements [DPO, ISIRT, IT, LD, DBRT, MGT]
- Maintain inventory of data breaches [DPO, DBRT]

Competent authority

- Provide data controllers with clear guidelines regarding data breach notification process and issue instructions on the data breach notification process
- Collect information about data breaches from data controllers
- Specify and endorse appropriate technological measures that render the data unintelligible to any person who is not authorised to assess it
- Interact with data controllers after a personal data breach has been reported and provide possible support
- Perform audits to check data controllers' compliance with their notification obligations and impose appropriate sanctions in the event they fail to do so
- Maintain a repository of data breaches notifications

Individual(s)

- Notify the data controller and/or the competent authority in case (s)he detects a personal data breach
- Interact with both data controller and competent authority if needed, and provide necessary support and information
- Follow the instructions provided by the data controller and the competent authority to contain or mitigate the personal data breach and refrain from providing information to any third parties until the personal data breach has been contained. They should also follow any proactive recommendations the data controller provides, to avoid the recurrence of the personal data breach.

10. Conclusions and final remarks

This study has provided specific guidelines for the process of handling personal data breaches, as provided for by Article 4 of the ePrivacy Directive. It has also taken account of the European Commission Communication entitled *A comprehensive approach on personal data protection in the European Union [8].*

In a nutshell, the following remarks and recommendations are made with regard to the implementation of the Article 4 provisions on personal data breach notification:

- **Importance of being proactive and prepared –** It is crucial that data controllers be proactive and well prepared to respond to potential personal data breaches. To this end, the data controller must have a risk management framework in place, identifying the risks of potential personal data breaches and identifying and adopting appropriate controls / measures;
- **Distinction between information security incident and personal data breach** – A personal data breach can be the result of a security incident, but also of loss of user control. An information security incident does not necessarily entail a personal data breach and vice versa;
- **Integration of the data breach notification scheme with existing procedures** – It is very important to integrate the personal data breach management activities with existing information security incident and risk management procedures in the data controller's environment. It is at any rate essential that the data controller has established and follows efficient incident handling and risk management procedures;
- **Two-phased assessments** – We recommend having two stages in the assessment: the initial one, where the data controller will need to determine as soon as possible the circumstances of the personal data breach and make a first impact assessment of the personal data breach, and a more detailed assessment, where the overall impact of the breach will be assessed. This will enable the data controllers to make the notifications in two stages as well;
- **Two-phased notifications** – According to the Directive, the data controller is obliged to notify the competent authority without undue delay. To facilitate early notification of the personal data breach, while giving the data controller enough time to perform the appropriate investigations and assessments, we propose also a two-phased approach in notifications. The first notification would ideally take place immediately after the initial assessment (within 24 hours), while the detailed one can follow later. The thresholds for the detailed one depend on the severity / impact of the personal data breach;
- **Test and improve the proposed process and particularly the impact assessment approach** – Since the procedures of handling and notification of personal data breaches are still in an early stage of development, the proposed approach, and particularly the severity assessment methodology proposed, should be tested in practice, ideally using real cases. This would help to identify any shortcomings and to update the process appropriately, especially with regard to:

- Appropriateness of the criteria and the evaluation proposed
- Possible differentiations in the steps of the severity / impact assessment of the personal data breach that the data controller and the competent authority may need to follow
- Although this approach intends to be technology-neutral, there might be a need to consider specific examples for some special and important technological platforms, such as cloud computing, and identify any need for updating the approach appropriately to address any gaps or difficulties in implementing this approach in such platforms.

It should be noted that, since ENISA intends to perform such pilots in 2012, the proposed severity assessment methodology, as well as other parts of the recommendations made in this report, may be updated as appropriate to reflect the results of the pilot.

11. References

[1] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, adopted on 20th June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[2] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', 00264/10/EN, WP 169, adopted on 16 February 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[3] Article 29 Data Protection Working Party, Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments, 00683/11/EN, WP 184, adopted on 5 April 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13/04/2006 P. 0054 – 0063. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

[7] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal L 337, 18/12/2009 P.11. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF

[8] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

[9] European Commission, Proposal for a Regulation of the European Parliament and

of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25.1.2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[10] International Organization for Standardization (ISO), Information technology — Security techniques — Information security risk management, International Standard, ISO/IEC 27005:2011(E)

[11] International Organization for Standardization (ISO), Information technology — Security techniques — Information security incident management, International Standard, ISO/IEC 27035:2011-09(E)

[12] International Organization for Standardization (ISO), General requirements for the competence of testing and calibration laboratories, International Standard, ISO/IEC 17025:2005.

[13] European Network and Information Security Agency, 'Securing Europe's Information Society', Work Programme 2011. http://www.enisa.europa.eu/media/news-items/work-programme-2011

[14] European Network and Information Security Agency, Data breach notifications in the EU, 2010. http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn

[15] European Network and Information Security Agency, ENISA's Clearinghouse for Incident Handling Tools. http://www.enisa.europa.eu/act/cert/support/chiht

[16] European Network and Information Security Agency, Good Practice Guide for Incident Management, December 2010. http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management

12. APPENDIX A – Example template of a data breach notification form to the competent authorities

As discussed in this report, the notification is an ongoing process which evolves in line with the findings of the forensic analysis. Because the data controller will probably not know all the details in his first notification, it is quite normal procedure that the follow-up notifications result in a change of answers that were given at the first notification. For this reason, only a few fields of the form must be marked as 'required', namely the fields 1, 2, 3, 4 and 5. The rest of the fields should be optional. The system on the website of the competent authority should log the history of the answers to the questions.

It is important to note that the example template presented below is recommended to be used as an electronic form (e.g. XML) in the competent authority's website to facilitate submission by the data controllers.

Some questions, e.g. '*What is the content of the notification to the individuals?*' may require multiple answers. This might be the case when the data controller informs the individuals in multiple instances, at each instance presenting more information (even though we consider this undesirable). Or some individuals may be affected differently by the data breach compared to other individuals, requiring different messages to be sent to different groups of individuals. Therefore the electronic form on the website should enable some questions to be answered in multiple instances.

Example template of a data breach notification form to the competent authority	
System data	
1. **Unique notification number** *[automatically generated]*	
2. **Notification date and time** *[automatically generated]*	
Notification data	
3. **Information on organisation notifying the data breach:**	
a. Name organisation: *[Name of organisation]*	
b. Notified by: *[name of person]*	
c. Job title: *[job title]*	
d. Email: *[email address]*	
e. Telephone: *[land line number]*	
f. Mobile phone: *[mobile phone number]*	

4. **The notification is a:** [choose between the following options]
a. Initial notification **(go to 7)**
b. Follow-up / detailed notification **(go to 5)**
5. **The follow-up notification serves the following purpose:** *[choose between the following options]*
a. Adding additional information to notification *[notification number]* **(go to 7)**
b. Withdrawal of notification *[notification number]* **(go to 6)**
6. **The reason for the withdrawal of this notification is:**
[Free text] <**end of script**>
7. **Contact persons for more information about this notification** *[only if different from 3]*
If applicable contact details of one or more persons:
a. Name: *[name of person]*
b. Job title: *[job title]*
c. Email: *[email address]*
d. Telephone: *[land line number]*
e. Mobile phone: *[mobile phone number]*
8. **Summary of the incident that caused the data breach:** *[Only a short summary is needed here; the details will be addressed in the other questions]*
[Free text]
9. **When did the actual data breach take place?** *[choose among the following options]*
a. At *[date + time]*
b. Between *[date + time]* and *[date + time]*
c. Has not been determined yet
d. Has not been determined yet and the breach is (possibly) still ongoing
10. **The type of exposure is:**
Breach type: *[choose one or more applicable options]*

a. Reading (only reading, an attacker does not have data)
b. Copying (data still exist in the controller's system)
c. Alteration (data exist but their integration was breached)
d. Removal (data do not exist in the controller's system; attacker does not have them either)
e. Theft (data do not exist in the controller's system, an attacker has them)
Breach subject: *[choose one or more applicable options]*
a. A computer
b. A mobile device
c. A paper document
d. A file or part of a file
e. A backup electronic mean
f. A network
11. **How many individuals are affected by the data breach?** *[choose one or more applicable options]*
a. A (yet) unknown quantity of people
b. *[exact number]* people
c. An estimated *[give approximate number]* people
d.At least *[x]* but certainly no more than *[y]* people
12. **What type of data are involved in the data breach?** *[choose one or more applicable options]*
a. (Yet) unknown
b. Name and address data
c. (Mobile) phone numbers
d. Email address / other electronic communication addresses
e. Access and identifying data (choose one or more applicable options: user name, password, customer ID, other [free text])
f. Payment data (choose one or more applicable options: account number, credit card details, other [free text])

g. (Other) personal data (choose one or more applicable options: sex, date of birth/age, maiden name, [free text]), special categories of data (choose one or more applicable options: racial or ethnic origin/ criminal data/political opinions/religious or philosophical beliefs/trade-union membership/data concerning health or sex life)
h. Other, namely *[free text]*
13. Estimated severity of the data breach (see chapter 4, assessing a data breach and its consequences)
a. Low / Negligible b. Medium c. High d. Very high
14. **Technical and organisational measures applied on the affected data**
[Free text]
15. **Have the individuals been notified?** *[choose one or more applicable options]*
a. Yes, they have been notified at [date] **(go to 15)**
b. No, but they will be notified at [date] **(go to 16)**
c. No, but they will be notified if the ongoing investigation shows it is necessary **(go to 16)**
d. No, they will not be notified because the data have been adequately secured **(go to 16)**
e. No, they will not be notified because [free text] **(go to 16)**
16. **What is the content of the notification to the individuals?** *[Copy text of notification]*
[Free text]
17. **Which communication channel is used for the notification to the individuals?**
[Free text]
18. **What technological and organisational measures have been taken to address and contain the data breach and prevent similar future data breaches?**
[Free text]
19. **Does the data breach involve individuals in other EU countries?** *[choose between the following options]*
a. No **<end of script>**

b. Yes
20. **Have you notified the competent authority in one or several other EU countries?** *[choose between the following options]*
a. No **<end of script>**
b. Yes
21. **Which authorities have you informed?** *[choose one or more options from the menu]*
[dropdown list competent authorities in the EU]
ANNEX: Attach the report on the impact assessment conducted for the personal data breach.

13. APPENDIX B – Assessing the impact of a personal data breach [Informative]

As discussed in section 6.3 of this report, in order to assess the impact/severity of a detected personal data breach, we need to consider two main criteria.

We hereby provide a possible approach that can be used to assess the impact of a personal data breach.

To facilitate the assessment, the competent authorities can provide a calculator of the severity of the breach, taking into account all circumstances and their own methods of calculation. For specific cases, the data controller could adjust the result obtained from the calculator by one grade (up or down).

The evaluation will be performed with the pre-defined scale presented in section 6.3: Very Low/Negligible, Medium, High, Very High, corresponding to values of 1, 2, 3, 4.

The final value of the impact / severity assessment table will be estimated based on the table below (see also section 6.3).

Impact assessment – Calculation of impact				
A. Identifiability / **B. Level of exposure**	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**
2	**2**	**3**	**4**	**5**
3	**3**	**4**	**5**	**6**
4	**4**	**5**	**6**	**7**

In order to give more information on how to evaluate each criterion, we provide explicit examples and values. However, it should be noted that this does not aim to be an exhaustive list of all the possibilities for each criterion and parameter, but rather to provide a clearer idea of how the assessment should be conducted, by providing concrete examples and possible values that could assigned for each one. The evaluation of the criteria would also need to be based on professional experience, since the approach is chiefly qualitative.

A. Identifiability

Identifiability is a very important criterion for assessing a personal data breach since it concerns the ability to identify a person from the personal data that have been breached (according to the Directive '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').

As mentioned in the main part of the report (section 6.3), in order to assess this criterion, the various types of personal data need to be considered, namely:

- **National identifiers (ID cards, passports)**
- **Sensitive data:** sexual orientation, trade-union membership, racial origin, political opinions
- **Financial data**
- **Health / medical data:** e.g. health cards, doctors' notes on disabilities, diseases, medical exams results etc.
- **Location data**
- **Pictures & videos**
- **Criminal conduct records or similar**
- **Email address / telephone**
- **IP address**

If more than one types of personal data are involved, e.g. medical and location data, or national identifiers and picture, then the final value should be the maximum of the individual values estimated. Also, it is possible that the combination of personal data may increase the impact of the breach (e.g. by increasing identifiability). It is thus important to consider this, when evaluating this criterion.

In the table below we provide an indicative way of evaluating this criterion based on the type of personal data breached. The scale used to evaluate is 1 to 4.

Evaluation of identifiability	
Scenarios / Examples	**Value [1 to 4]**
I**mpossible or very difficult:** it is almost impossible to identify the persons with the data that are compromised (e.g. first name within a database of 60 million people)	**1**
Possible: e.g. name & first name	**2**
Easy: e.g. name & first name & data of birth	**3**
Certain: e.g.name & first name & address & zip code & date of birth & tax or social security number or name & first name & address & picture	**4**

B. Level of exposure

Once the identifiability and type of personal data breached have been determined and evaluated, then the data controller needs to identify and evaluate the particular circumstances of the breach and its levels of exposure. In general, the data controller should consider the following parameters to determine what exactly happened and to assess this criterion:

B1. Nature of data breach, the type of exposure accomplished (i.e. the breach action), namely:

- unauthorised or unlawful access (read access only)
- loss or destruction
- alteration / modification
- transmission, processing, storing
- disclosure (e.g. to public or unauthorised third parties)

Also, and in order to better determine this, the **asset (e.g. device, systems)** that was subject to the breach should be identified, e.g.:

- PC / server
- Mobile device, e.g. laptop
- Network
- Data file
- Paper document
- Backup electronic mean, e.g. DVD, CDs

For the actions above it should be considered whether it was **internal** (within the data controller, e.g. an employee) or **external** (e.g. an attacker). This is important because of the amount of information that is known to the person responsible for the personal data breach (an employee has higher levels of access than an external attacker).

For the assessment of this criterion the data controller should consider that the **higher the type of exposure, the greater the impact.** As an indication, we provide the following table:

Nature of data breach / type of exposure	
Type	**Exposure**
Unauthorised or unlawful access (read access only)	1
Loss or destruction	2
Minor alteration / modification of personal data	3

Nature of data breach / type of exposure	
Type	**Exposure**
Transmission	**3**
Major alteration / modification of personal data	**4**
Disclosure (e.g. to public or unauthorised third parties)	**4**

B2. Implemented controls (esp. data unintelligibility)

This parameter has to do with the controls / measures that the data controller has implemented in order to protect the personal data. Ideally these controls should have been identified as a result of a risk management exercise. What is of interest here is particularly to consider whether data have been rendered unintelligible or not, so in case they are stolen it would be impossible to render them with the current technological knowledge. A definition of unintelligible data is included in section 5.2.2 of this report.

This parameter is considered in association with the previous one in the sense that it may decrease the previous parameter: even if the type of exposure is very serious, if appropriate technological measures have been implemented, then the overall level of exposure is diminished. In particular, the data controller should consider the following:

Nature of data breach / type of exposure	
Type	**Exposure**
Data have been stored or transferred in plain text format, standardised formats, proprietary formats, • No backups of data kept / no backup policy	**Very High** *(increasing the severity of the previous parameter: +2)*
• Data stored in hashed format or is password-protected (with no key) • Short password based encryption • Backups taken, but are not taken often	**High** (increasing the severity of the previous parameter: +1)
• Weak encryption • Non-secure deletion • Full backups are taken but not every day	**Medium** (decreasing the severity of the previous parameter: -1)
• Encrypted data with strong key/password • Hashed data with a 128-bit key • Destruction, degaussing or secure deletion • Full daily backups	**Low / very low:** Data can be considered unintelligible – in this case, the data controller is also exempt from notifying the individual (decreasing the severity of the previous parameter: -2)

In the table above we mainly consider aspects of data encoding and measures regarding availability of data (e.g. backup). The data controller should always consider the maximum impact, even if the measures taken for the availability of data are better than those regarding encoding (e.g. full daily backups are taken but the data are stored in hashed format, in which case level 2 of exposure should be considered, namely increasing the severity of the previous parameter +1).

B3. Delay in identifying the breach

The delay in identifying the breach is a parameter worth considering, because the longer the delay the greater the possibility that the exposure levels have increased, and the more difficult it will be to respond to the data breach. For example, in the case of a stolen laptop with sensitive HR data that are weakly encrypted or hashed, a delay in detection of one week or more could give the attackers valuable time to crack through the encryption and gain access to the data. Hence, **the longer it takes to detect the personal data breach, the higher the potential exposure.** Indicatively:

Delay in identifying the breach	
Possibilities / Examples	**Exposure**
<24 hours	Decreasing severity of first parameter -1
2-5 days	No increase / decrease
5-10 days	Increasing severity of first parameter +1
>10 days	Increasing severity of first parameter +2

B4. Evaluation of overall level of exposure

Based on the three parameters above, the data controller would need to estimate the total level of exposure. It should be noted that the evaluation is based on a scale from 1 to 4, which means that if the increases or decreases from the last two parameters on the value of the first parameter result in a value above 4 or below 1, then the maximum (4) or the minimum (1) value would still be indicated.

The table below shows possible ways of evaluating various scenarios.

Evaluation of level of exposure	
Possible scenarios / Examples	**Value [1 to 4]**
Personal data intact (e.g. due to data being appropriately encrypted with a 128-bit key); or accidental read-only access accomplished; no disclosure of data; data have been lost or destructed, but full daily backups are taken.	1
An attacker stole a laptop and successfully accessed the data, but was not able to modify or copy them or otherwise transmit them (due to access controls in place protecting the data); also the breach was detected within 24 hours so data could not be disclosed.	2
An attacker sniffed personal data transmitted through the network; he/she has been able to copy them but has not been able to modify them or transmit them and process them.	3
Personal data have been accidentally disclosed to unauthorised recipients (e.g. via a wrongly addressed email); the data have been sent in read-only format, so cannot be modified, but they can be re-transmitted and processed.	3
DVDs storing personal data have been stolen; the data have been successfully accessed and disclosed in a public website.	4
Attacker successfully gained access to the database server, modifying HR personal data of employees. The data have also been copied and transmitted to third parties.	4

14. APPENDIX C – Information security event and incident flow diagram [ISO/IEC 27035:2011]

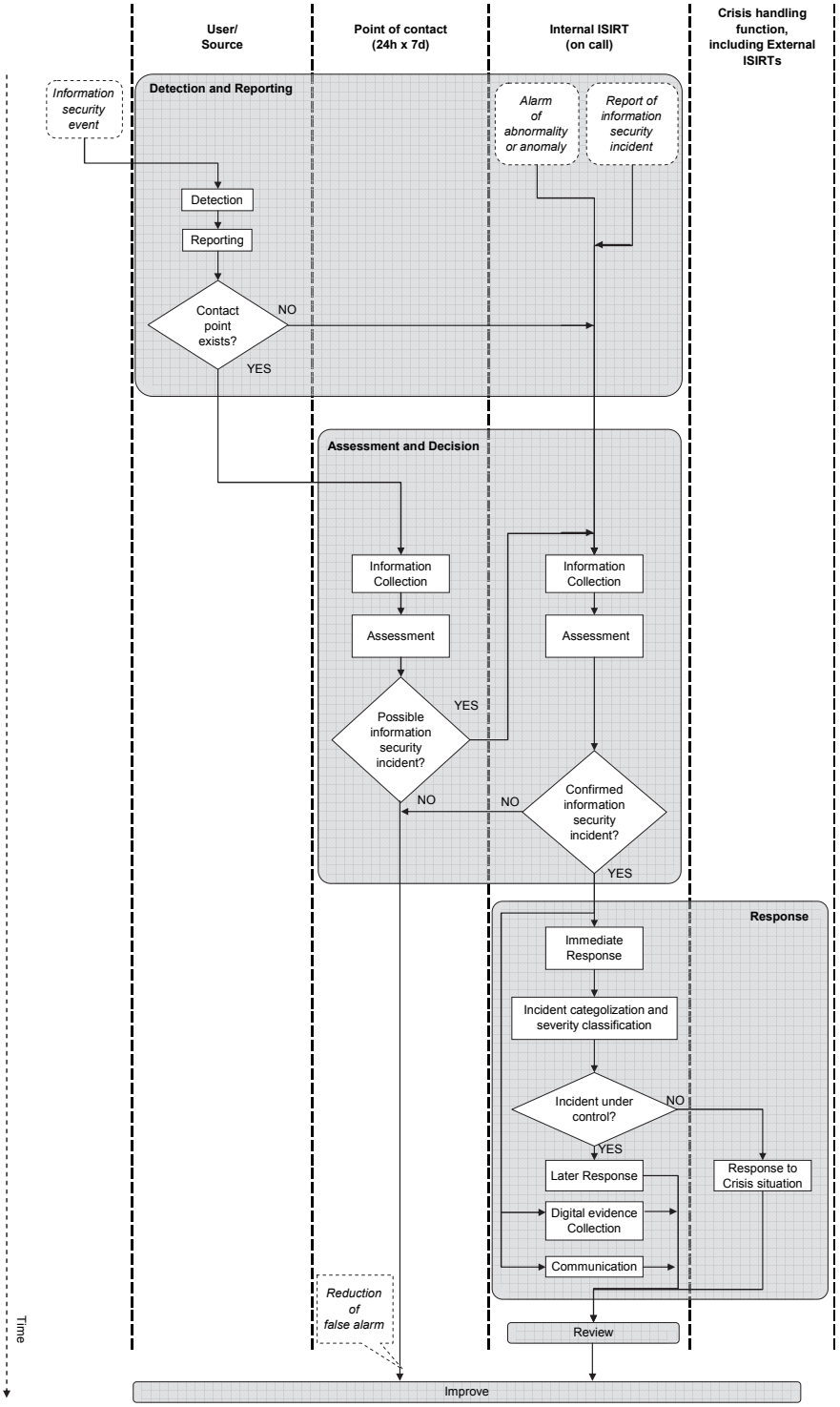


Figure 3 — Information security event and incident flow diagram

NOTE False alarm is an indication of an unwanted event, but is found not to be real or of any consequence.

15. APPENDIX D – Elements of a personal data breach response plan

1. Identification of appropriate roles and responsibilities within the organisation

- appropriately define the roles and responsibilities of parties involved in responding to and reporting personal data breaches, to facilitate personal data incident management;
- identify the members of a personal data breach management team (if different from an incident response team), which should be composed of a limited number of people (e.g. one representative of the top-level management, the IT and risk managers, data protection official).
- formalise the responsibilities of the person in charge of compliance with the data protection law (e.g. data protection official).

2. Identification and documentation of procedures: the procedures for reporting potential personal data breaches should be documented and should be in line with the internal security incident management procedure, so as to facilitate their implementation. Specifically, at least the following should be properly documented:

- classification of a security incident as a personal data breach
- estimation of the severity of the personal data breach
- any escalation procedures (e.g. based on the severity of the breach), as well as response and internal and external notification plans.

3. Response and collection of evidence procedures

For each severity level, the procedures to react to personal data breaches should be defined, in order to contain such breaches and limit their consequences. For a high level of severity, such procedures should include scenarios for which business operations will be temporarily stopped to avoid greater consequences of personal data breaches. Providers might consider, to the extent that this is possible,[16] including the following actions in their response plan:

- the establishment of a call centre to provide the users with a number to call in order to get more information on the details of the breach
- provide access to services and information to help those affected by the breach via a toll free number
- prepare spokesperson(s) to respond to media inquiries to ensure that potential data breach victims receive high quality and useful information
- prepare material such as web pages, form templates, phone scripts and frequently asked questions (FAQs) drafted and ready for posting
- consider the need for extra staff to deal with the increased call volumes
- consider steps to minimise hold times of the telephone lines

16 For example, if the organisation is big enough and the breach is of high or very high severity.

- consider whether multi-lingual support is needed
- collect evidence on the causes and the consequences of the breach. If the severity of the breach is high, a more thorough analysis will be necessary.

4. Notification to competent authorities and individuals

- Directive 2002/58, as amended in 2009 [7], identifies two types of external notifications: to national competent authorities and to individuals (when the personal data breach is likely to adversely affect personal data or privacy).
- The response plan should provide the contact details of national competent authorities and forms to be used when external notifications are required. Preferred and backup communication channels to competent authorities and persons should be identified; preferred channels should be used unless they have been compromised by the breach.
- Concerning notifications to individuals, the response plan should distinguish several notification channels depending on the severity of the breach, the number of people involved and whether the people involved can be contacted directly. Different scenarios can be envisaged involving, for instance, one or a combination of the following: a written notification to people, phone calls, articles in the press, information on the website.

16. APPENDIX E – Options for exercising personal data breach plans

Tabletop Exercises

A tabletop exercise involves assembling the key stakeholders in a single place and walking through a scripted exercise. The exercise coordinator slowly releases information concerning the incident, and each stakeholder plays the role they would play in a real incident.

This type of exercise is an efficient way of conducting an exercise. It is good at uncovering broad issues with a response plan and educating participants. However, the complexities of an actual breach, including issues such as communications problems or complex investigation issues, will not be addressed.

Functional Open Knowledge Exercises

Unlike a tabletop exercise, a functional exercise involves the participants functionally performing each step of the plan as if it were a real incident. The participants are aware that it is a test, but attempt to stay true to enacting a real response. This may involve conducting a forensics exercise, generating necessary notifications, legal consultation, law enforcement involvement, writing public press briefs, and conducting operational security for the response effort.

Functional Blind Exercise

The blind exercise is considered a 'live fire' exercise, much like a functional open knowledge exercise, except that those involved in the response are unaware that it is an exercise. Generally only organisations that have mature response capabilities undertake these exercises due to the complexity of managing and containing such an exercise. However, this exercising gives the most realistic view of the effectiveness of the response and is considered the best training beyond real experience.

Exercise Results

Once an exercise has been concluded it is important that the exercise and any lessons learned are documented and fed back into planning. This normally comes in the form of a post-mortem document that should cover the following points as a minimum:

1. What worked well during the exercise. Where did the team do well, which pieces of the plan were useful.
2. What didn't work during the exercise. Include documentation that was missing or incomplete and tools or processes that created failures or inefficiencies in executing the plan.
3. A list of action items and assigned people to improve the plan or the response next time.
4. When the next test will occur.

Results should be distributed to key stakeholders, and, depending on the scope of the test, it is advisable to conduct a post-mortem meeting to discuss it.

17. APPENDIX F – Collecting evidence from computing resources

Generally collecting evidence starts with choosing the right containment strategy, i.e. containing the area, shutting down a system, disconnecting it from a wired or wireless network, or disabling certain functions. Ideally, containment strategies and procedures should have been predetermined based on acceptable risks in dealing with incidents and they should include methods of gathering all possible evidence during an incident as well as after it.

When the system is shut down, it needs to be put into a state in which the evidence cannot be accidentally modified. This generally includes removing the power cable and taping up the power receptacle. In many instances the hard drive can be removed to serve as evidence. In other cases, such as when the system cannot be shut down, a forensic copy of the hard drive, memory collection or pertinent files can be collected using industry standard tools.[17]

There are various containment strategies based on the type of incident. For example, the overall strategy for containing an email-borne virus infection is quite different from that of a network-based distributed denial of service attack. Organisations should create separate containment strategies for each typical incident. Criteria should be documented clearly to facilitate quick and effective decision-making, including (but not limited to) potential damage, need for evidence preservation, IT service availability, or duration of the solution.

In certain cases, organisations tend to delay the containment of an incident so that they can monitor the attacker's activity, usually to gather additional evidence. However, a delayed containment strategy poses a high risk because an attacker could escalate unauthorised access or compromise other systems in the meantime.

Collecting evidence is not necessary for every incident that occurs. For example, most malicious code incidents do not merit evidence acquisition. Also, computer forensics is not needed for most incidents.

Evidence from computing resources includes the following:

- System information such as location, serial number, model number, hostname, MAC address, and IP address.
- Capture of volatile information such as current network connections, processes, login sessions, open files, network interface configurations, and the contents of memory.
- System image containing all data on the disk, including deleted files and file fragments.
- Registry data, if applicable.
- Copies of supporting log files from affected systems as well as other re-

17 See http://www.forensicswiki.org/wiki/Tools

sources, i.e. firewall logs that show keywords, URLs and IP addresses used by an attacker.

- Time and date stamps (including time-zones) of each occurrence of evidence for forensic timeline analysis.

Good practices and guidelines for the management of network and information security incidents, including collecting of evidence, can be found in ENISA's Good Practice Guide for Incident Management [16].

18. APPENDIX G – Forensic analysis

The basic forensic analysis procedure

As with any other important process, the forensic analysis should be performed according to the approved procedure. The most important steps of it are:

STEP 1 – Organise a team

Gather all specialists who are needed during an analysis. Contact with the Legal Department, the Law Enforcement Agencies and external forensic experts should also be established, if and when needed.

STEP 2 – Determine objects

Decide what objects will be analysed. If some of them are not part of the infrastructure, external parties, e.g. ISP, should be contacted.

STEP 3 – Collect tools

Based on the information from the Step 2, tools that will be needed to successfully perform the forensic analysis should be collected.

STEP 4 – Gather data

According to what it was decided in Step 2, collect data from all sources.

STEP 5 – Archive data

In the forensic process the proper data archiving is not the final process. The work should be performed on replicated data. The original should remain unchanged to allow for an integrity check and to repeat or confirm the analysis process if needed.

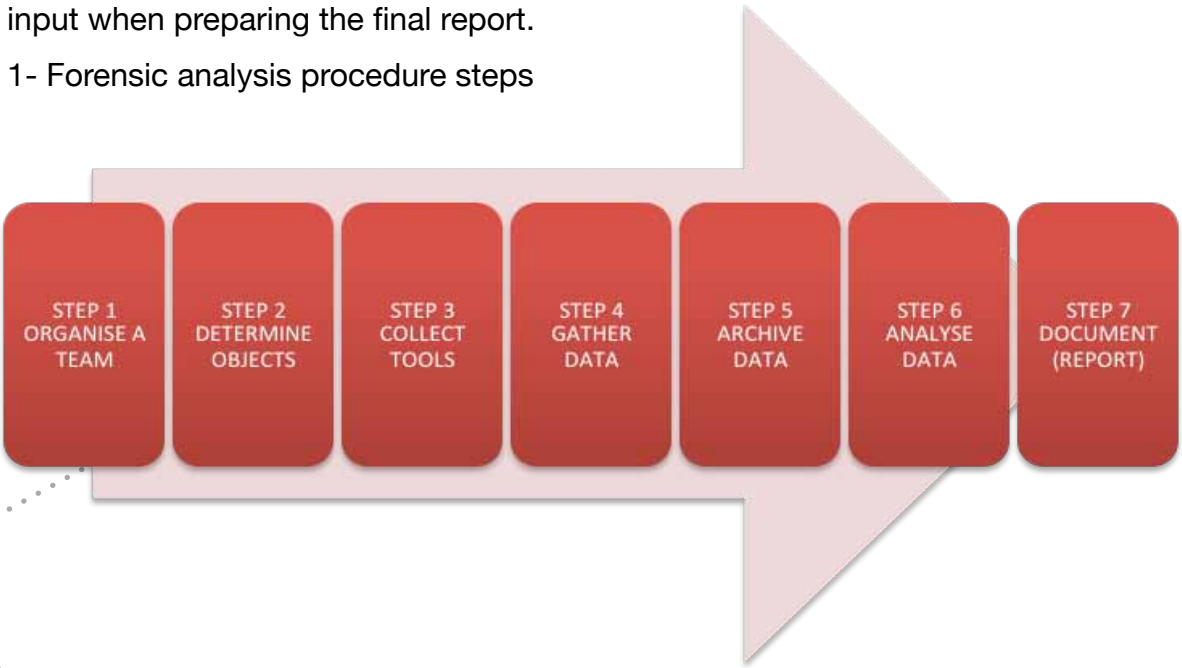
STEP 6 – Analyse data

Perform all planned analysis. This is the most important part of the process. Especially in this step, it is very important to document the work. Sometimes this step requires a lot of interaction among the different experts participating in the exercise and repetition of activities.

STEP 7 – Document (report)

The whole process should be documented. This documentation will be the major input when preparing the final report.

1- Forensic analysis procedure steps



Forensics Tools

There are plenty of forensic tools for both kind of analysis – computer and network forensics. The choice of tool is determined by three main factors: their cost and available specialists able to use them and – the most important one – the needs of the data controller. Besides the available multi-functional tools (toolkits), there are tools with very narrow functionality; both solutions are helpful. The natural approach is to use toolkits at the beginning followed by more precise analysis with other tools if needed, unless it is clear from the outset that some of the specific tools will need to be used.

The forensics tools can be divided according to the objects that are analysed with these tools: [18]

- Data Recovery
- File Analysis
- Document Metadata Extraction
- Memory Imaging
- Memory Analysis
- Network Forensics
- Logfile Analysis

Additionally these tools can be classified in terms of operational systems as well as their market availability – commercial vs. open-source tools.[19]

Forensic analysis objects

There are two main objects which can be analysed – computers (including PC computers, servers, laptops and other mobile devices) and networks, and interviews with the relevant people / individuals.

Concerning computers, both the operating systems logs as well as logs from software installed on computers should be analysed. Concerning the networks, logs from network devices and also logs from the communication between these devices should be analysed.

Computer and network logs may be collected as a matter of routine, and can also be collected during live capturing of interesting data. This capturing is based on the initial information which is available to the data controller and it is especially related to network data.

Last but not least, data can be retrieved by following a data recovery process. It is very important to have such a capacity as intruders usually try to hide any evidence related to a breach. Also, breached data itself can be deleted and its recovery process is the only solution to resolve a problem.

18 Based on Forensic Wiki: http://www.forensicswiki.org/wiki/Tools

19 A practical guide to many helpful tools is available on ENISA's website at Clearinghouse for Incident Handling Tools [15]

During the forensics analysis the relevant sources should be analysed. They may include:

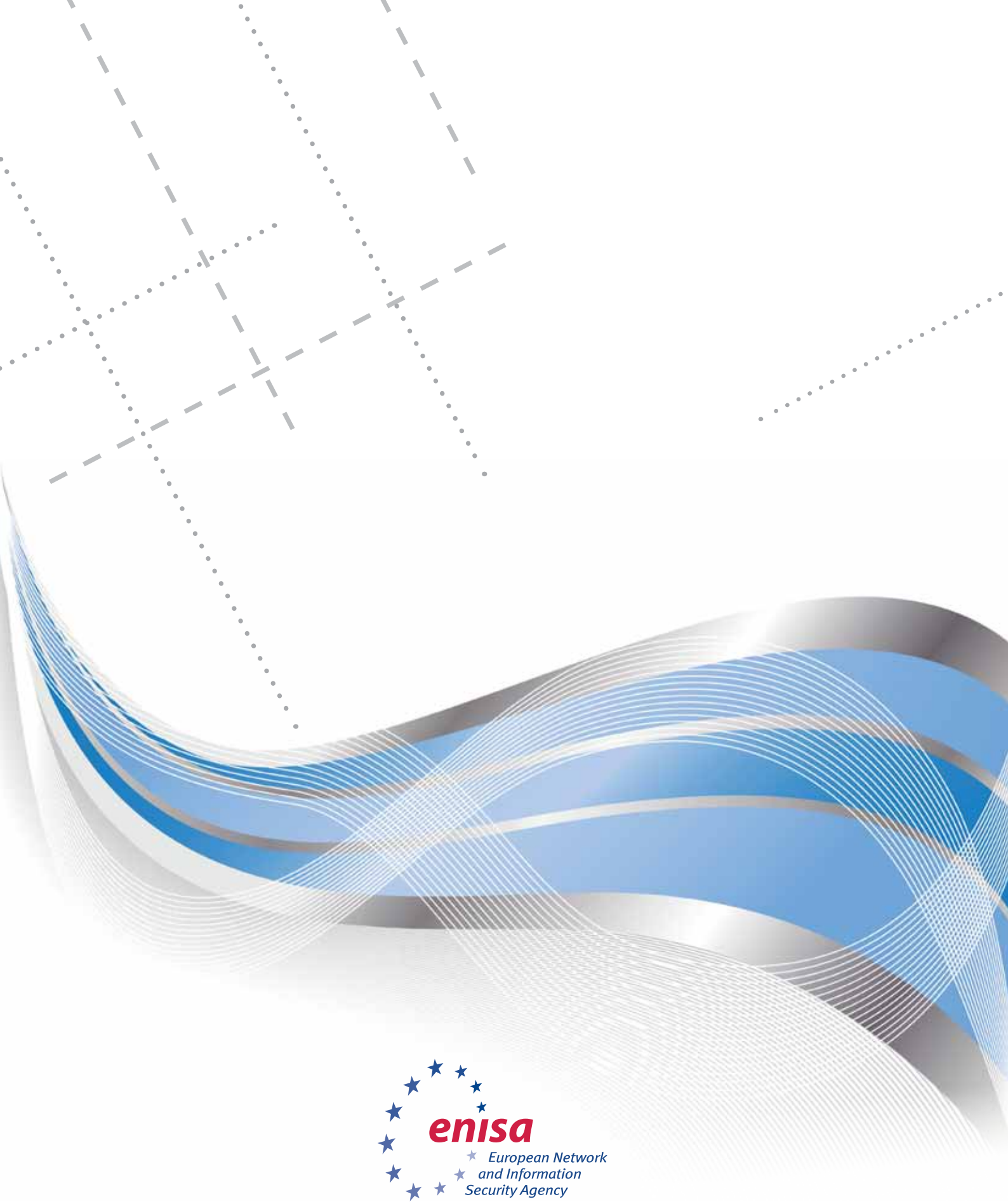
- Personal computers including laptops (files, file systems, hard drives, RAM)
- Servers (files, file systems, hard drives, RAM)
- Mobile devices (mobile phones, smart phones, PADs, USB sticks)
- Network devices (routers, switches, WiFi Access Points, firewalls, intrusion detection systems, honeynets)

Devices may be owned by the data controller as well as other parties involved in the data breach, especially data processors (e.g. which process data according to an agreement with data controller) and internet service providers serving network services to a data controller (e.g. internet access).

Legal aspects of forensic analysis

It is very important to process all activities related to forensic analysis in a way that ensures the results of this analysis can be used as legal evidence. To do this, the following steps should be taken:

- Incorporating data controller's legal department into the data breach investigation process – By this they can advise and control the process from the legal point of view; however the involvement of the legal department in such an analysis should be formalised.
- Delegate professional staff to this activity – That means specialists in forensic analysis, no matter whether they are internal company staff or external experts. However, special precautions should be taken when involving external people. In addition, special requirements may also be specified if sensitive data are involved.
- Professional archiving of all data and results from the analysis – Badly maintained data, for example data that are not kept in a secure place which ensures their integrity, can easily be rejected as legal evidence.
- Cooperation with Law Enforcement Agencies – It may be an obligation in some data breach cases to report a crime. Cooperating with law enforcement authorities significantly improves the likelihood of capturing an offender. Inform the competent authorities and the individuals, as appropriate.



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