CERT participation in incident handling related to Article 4 obligations

Handbook, Document for teachers

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

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

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Copyright Notice

Table of Contents

1 Introduction

Goal

This exercise provides students with information about rules, procedures and best practices in incident handling related to personal data breaches. It is based on data breach notification requirements for the electronic communication sector introduced by the review of the ePrivacy Directive.[1] The process of notification is parallel to normal incident handling process and it is part of it.

Target audience

Incident handlers and CERT managers responsible for incident handling procedures within an organisation.

Course Duration

2 hours

Frequency

Once for each new CERT member

Structure of this document

	Task	Duration
	Introduction to the exercise – data breach terminology and processes	20 min
	Task 1: Data breach incident severity evaluation	35 min
	Task 2**:** Data breach notification to data controller and individuals	25 min
	Summary of the exercise	40 min

2 General Description

The purpose of this exercise is to familiarise participants with set of activities which are characteristic for events involving personal data breaches. The 'data breach' term is understood as a security

[1] *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*

incident related to personal data[2]. These events are usually related to breaches of national law on personal data protection.

Specifically, during the exercise participants will learn:

- the terminology related to data breach notification as well as to personal data protection;
- how to evaluate the severity of the data breach incident;
- how to prepare notifications for different kinds of receivers – competent national bodies (data protection authorities) and individuals;
- how to conduct some specific parts of incident handling process – severity evaluation and incident notification.

3 EXERCISE COURSE

The course of this exercise is as follows. All assumptions and discussions should be moderated by the trainer.

3.1 Introduction to the exercise

At the beginning of the exercise you have the task of presenting to the participants terminology related to the data breach and personal data.[3]

3.1.1 Terminology

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Union.[4] 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.[5]

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 or her physical, physiological, mental, economic, cultural or social identity.[6] In our study we considered the analysis performed by the Art. 29 WP on the explanation of the 'personal data' regarding the four main 'building blocks' that can be

---

[2] See definition of personal data breach in the terminlogy part of the exercise – 'Introduction to the exercise'

[3] The terminology is from the ENISA publication 'Recommendations on technical implementation guidelines of Article 4' (http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech)

[4] Amendment by Directive 2006/24/EC and Directive 2009/136/EC of Directive on Privacy and electronic communications 2002/58/EC: (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML)

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

[6] Article 2(a) of Directive 95/46/EC: (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML)

distinguished in the definition of 'personal data': i.e. 'any information', 'relating to', 'an identified or identifiable', 'natural person'.[7]

Individual – any living natural person affected by the personal data breach. This includes users and subscribers, for private or for business purposes, without their necessarily having subscribed to the service that is affected by the breach.[8]

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).[6]

Data controller – the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of personal data (Article 2(d) of Directive 95/46/EC).

Data processor – the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller (Article 2(e) of Directive 95/46/EC).

3.1.2 Describe the general workflow of the personal data breach handling procedure

Present the following workflow[9] (see below) and explain the particular phases of the process. Place special attention on those parts that are dedicated to incident handling procedures themselves and will be part of the further exercise activities, which are the parts of this exercise e.g.:

- initial assessments;
- preliminary notification;
- detailed notification.

Explain to participants that CERT participation is especially important in the particular parts of the process.

- **Initial assessment:** This is the most important parts of the process in terms of CERT participation. CERT staff, with their experience and knowledge of various incidents, are able to make the best initial assessment. This assessment has a big influence on further incident processing. Thus, CERT technical skills allows for the proper identification of the circumstances and severity of the breach and the immediate response measures.
- **Collection of evidence and forensics analysis:** This is the second most important part of the process from the point of view of CERT participation. It is especially important because of CERT staff has technical knowledge on evidence collection and forensics analysis. Even if CERT staff is not able to physically collect the evidence they can provide practical recommendations and advice on how to do it.

For better and easier presentation use the description of the process from the ENISA document.

---

[7] *Opinion 4/2007 of the Article 29 Data Protection Working Party*
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
[8] ENISA's 'Recommendation on technical implementation guidelines of Article 4'
http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech
[9] The workflow is part of the ENISA document: 'Recommendations on technical implementation guidelines of Article 4' (http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech)

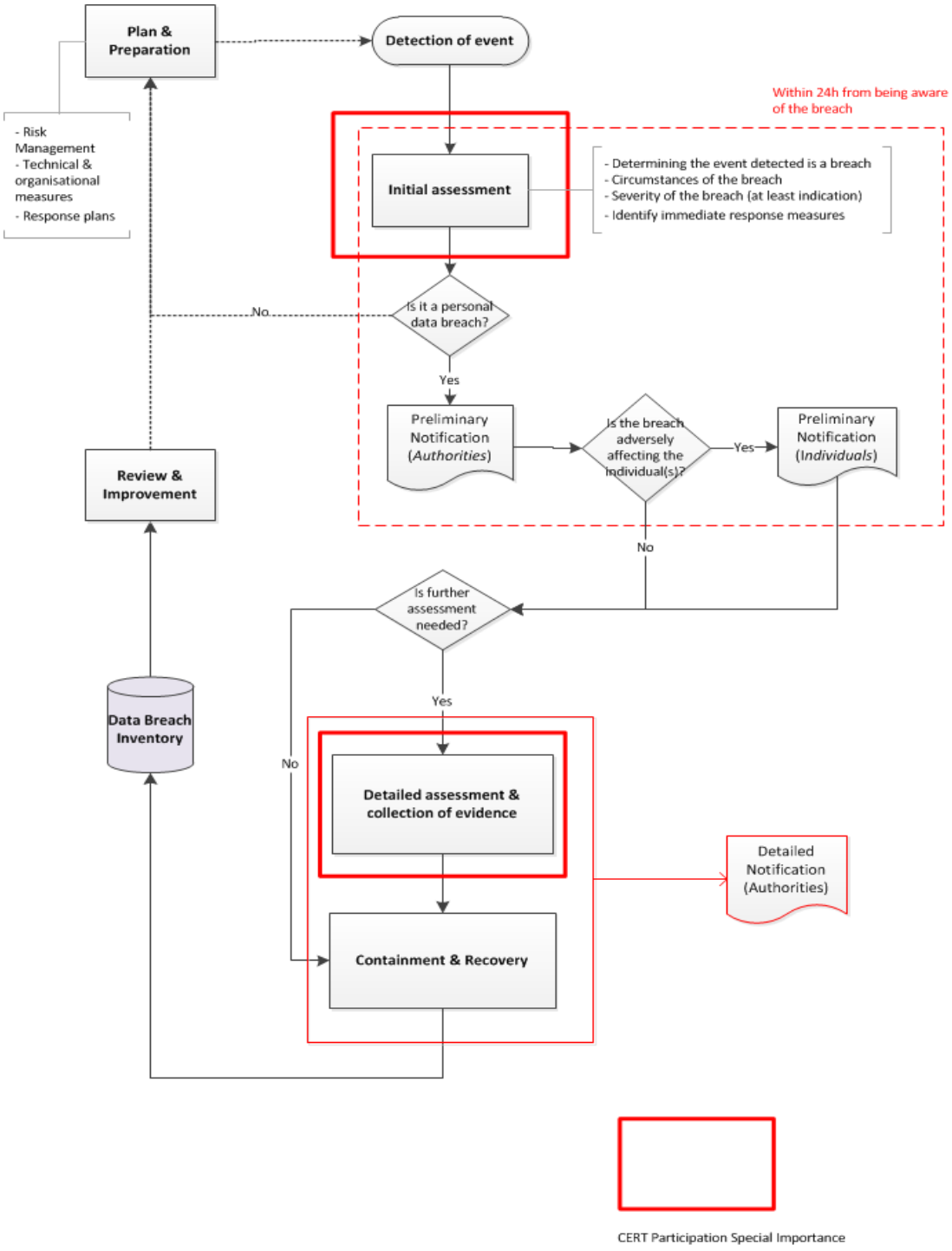

Figure 1 Personal Data Breach Management Procedure[10]

3.2 Task 1: Data breach incident – severity evaluation

After the introduction to the exercises, participants start to work with the particular case. They will receive information about the case. Form groups of two or three people and give them five minutes

[10] From ENISA 'Recommendation on technical implementation guidelines of Article 4' http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

to learn about the case; then present it with your own words. Then give participants a chance to ask questions and clarify all doubts related to the case. It is worth mentioning at this point that generally the assessment of an incident that involves personal data should always start with the notification of the competent authority. The case is presented here.

1. *The company database administrator notices that access to the database has been made late at night. He/she investigates the case and decides that it is probably an attack from outside the company. The company cooperates with banks and in its business contracts to process the personal data of banks' customers.*

2. *The administrator reports the fact to the company security team. The team plays the role of the internal CERT. They have specialists on network and computer forensics and some have participated in events organised by the CERT community – for example, the FIRST Conference. Currently, they are trying to convince company management that their team should become an official CERT team and join the European CERT community – TERENA TF-CSIRT.*

3. *The security team contacts the company network and system administrator to explain the case. They explain the possible scenario of a data breach and recommend some control activities to further investigate the case. It is recommended inter alia to check network connections to the database server, authorisation logs in the local network and remote connections to the company's network.*

4. *The network and system administrator discovers a new unauthorised account that was created three days ago with administrative privileges on the database server. During this investigation he/she also discovers that the host intrusion detection system was not active for almost one week. There is no clear evidence why it was deactivated. Was this intentional or was it a system failure?*

5. *Further investigation shows the copying from the company's database server of more than 10,000 records (including such personal data as names of company customers, their credit card data as well as postal addresses and authorisation data) to the online service (online shop). The system administrators assure the company that data was encrypted with AES 256 algorithm.*

6. *The customer list includes citizens from Germany, The Netherlands, Poland, Greece and the United States*

Based on these facts, participants – working in groups – should prepare their own evaluation of the incident severity. To calculate the potential impact of the data breach, they should estimate two main factors: identifiability and level of exposure.

Identifiability is understood as 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').

Level of exposure can be evaluated as the result of a few important factors; the most important are the nature of the data breach, the implemented controls, and the delay in identifying the breach (see

the tables below). There are no simple, unambiguous values. An evaluation comes from users' knowledge and experience. One possible method is presented below.

Nature of data breach/type of exposure	
Implemented controls	**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*)

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

3.2.1 Initial assessment

During the initial assessment, participants will propose their calculation of identifiability and level of exposure. Both can be scored between 1 and 4. A value of 1 is the least identifiable and the least exposed. A value of 4 represents the most identifiable and exposed asset.

Ask participants to prepare their own calculation of incident severity in the groups. In order to make this task more creative and provoke discussion within the groups as well as between all participants in the summary part of the exercise, do not provide any specific concrete models of calculation.

The final evaluation is the results of the mentioned factors and can be determined with the following table. Depending on the final position of the case assessment, the case can be considered to be a dangerous one with a high impact on personal data safety, or it can have a low impact because of the low values of the identifiability and level of exposure.

This table assists in the calculation of the impact schema.[11]

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**

3.3 Task 2: Data breach notification to data controller and individuals

3.3.1 Preliminary notification

Students should prepare two notification report schemas. One for data controllers and the second for individuals who have been victims of data breach notification. For this purpose, provide them the table from the Appendix ('Sample template of a data breach notification form to the competent authority'). You can present them with one example of notification (to the competent authority) as below:

[11] Article 2(a) of Directive 95/46/EC: (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML)

Sample template of a data breach notification form to the competent authority	
System data	
1. **Unique notification number**	Automat#0001
2. **Notification date and time**	10/01/2013
Notification data	
3. **Information on organisation notifying the data breach**:	
a. Name organisation:	YOUR JOB KEEPER Limited
b. Notified by:	John Smith
c. Job title:	IT Security Officer
d. Email:	John.Smith@yourjobkeeper.com
e. Telephone:	+00 111 111 00
f. Mobile phone:	+00 111 111 01
4. **The notification is a/an**: [*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:	
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: *Jonathan First*	
b. Job title: *Personal Database Administrator*	
c. Email: *Jonathan.First@* yourjobkeeper *.com*	
d. Telephone: +00 111 111 02	
e. Mobile phone: +00 111 111 03	
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]*	

We have experienced data leakage via our website. There was unauthorised connection to our service. Intruders crafted an SQL query to our database and due to some configuration mistakes they were able to get access to personal data records of approximately 4,000 people.
9. When did the actual data breach take place? [*choose among the following options*]
a. At *[date + time]*
b. Between *10/01/2013 around 11:00 AM and 10/01/2013 around 05:00 PM*
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 means of electronic backup
f. A network
11. How many individuals are affected by the data breach? *[choose one or more applicable options]*
a. A (currently) unknown quantity of people
b. *[exact number]* people
c. An estimated *4,000* 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. (Currently) 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
f. Payment data (choose one or more applicable options: account number, credit card details, other
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: job status, current and past employees, education
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
There is a Personal Database Policy, rules of limited computer access, network separation for database server, auditing policy of the database, encryption channel for exchanging personal data with outside parties, database server operation system policy, backup policy.
15. Have the individuals been notified? *[choose one or more applicable options]*
a. Yes, they have been notified on [date] **(go to 15)**
b. No, but they will be notified on [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]*
Dear [Insert customer name]:[12] We are contacting you regarding a data security incident that has occurred at Your Job Keeper Limited. This incident involved your personal data (name, address, mobile phone number, email address, job status, current and past employees, education). As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

[12] *The template is based on the proposal from the Experian Data Breach Response Guide (*http://www.experian.com/assets/data-breach/brochures/response-guide.pdf*)*

Your Job Keeper takes this incident seriously and is committed to ensuring the security of your data. To help protect your identity, we will provide you in the following days with the specific information about this concrete case as well as information for assuring protection of your data in the future. It will help you to improve the protection of your in a systematic way.
17. Which communication channel is used for the notification to the individuals?
Email-addresses
18. What technological and organisational measures have been taken to address and contain the data breach and prevent similar future data breaches?
Database server hardening, audit of website interface, suspension of website online service
19. Does the data breach involve individuals in other EU countries? *[choose between the following options]*
a. No
b. Yes
20. Have you notified the competent authority in one or several other EU countries? *[choose between the following options]*
a. No
b. Yes
21. Which authorities have you informed?
ANNEX: Attach the report on the impact assessment conducted for the personal data breach.

According to the proposed law, these notifications should include very concrete fields and information but it is participants' tasks to propose their own solutions.

The notification content is described in Art. 4(3), of the ePrivacy Directive as follows:[13]

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.

[13] *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.*
*(*http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML*)*

Participants should prepare their own list of information, taking into consideration the purpose of this notification, especially regarding victims who should not only have learnt about the fact of their personal data breach but also learnt about consequences and possible next steps.

Paricipants work on their own proposal; after they finish their work you can present them with a notification template, which should include the following fields:[14]

- contact details (e.g. name, postal address, email address) for the organisation and the reporting person;
- information about contact person for this notification (if different from the one who is reporting);
- data controllers involved (for large global organisations, a breach can occur across more than one entity);
- date and time of notification;
- date and time when the data breach was established;
- (estimated) date and time of occurrence of the data breach;
- type of personal data breached;
- a short summary of the event (when, why, who, what happened, etc.);
- the results of the impact / severity assessment performed, including the way this was calculated, based on the calculation criteria from Task 1;
- the number of individuals impacted or likely to be impacted;
- actions taken or services offered to the individual;
- 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:

- 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);
- communication channels used to notify the affected individuals (if applicable);
- cross-border data breach (if applicable), e.g. competent authorities that have been informed;

[14] *the list originates from „ENISA Recommendations on technical implementation guidelines of Article 4' (*http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech*)*

4 Summary

The exercise ends with a summary, which mainly consists of a presentation of the results of group work and discussion between groups with your moderation.

Firstly, the results of the breach severity evaluation should be presented. To facilitate the discussion and to present the proper approach to the problem, you can use materials from the ENISA document *Recommendations on technical implementation guidelines of Article 4*. Especially helpful could be the tables included in the appendix:

- table for evaluating the identifiability;
- table for evaluating the level of exposure;
- table for evaluating the nature of data breach and type of exposure;
- table presenting the influence of delay in identifying the breach on the severity.

5 REFERENCES

1. ENISA *Recommendations on technical implementation guidelines of Article 4* (http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech)
2. ENISA, *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
3. ENISA, Data breach notifications in the EU, 2010. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn/at_download/fullReport

6 APPENDIX

Table for evaluating identifiability:

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

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

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

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