DECISION

Background

By determination of the Management Board of 22 December 2011, ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) approved a draft decision on:

- the circumstances, format and procedures applicable to the requirements of reporting, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity with significant impact on the functioning of networks and services; and
- on the conditions by which ICP-ANACOM considers that there is public interest in public disclosure, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity with significant impact on the operation of networks and services.

In accordance with this determination, it was decided to submit this draft decision to the prior hearing of interested parties, pursuant to articles 100 and 101 of the *Código de Procedimento Administrativo* (Administrative Proceeding Code), as well as to the general consultation procedure laid down in article 8 and in paragraph 4 of article 54-C of *Lei das Comunicações Eletrónicas* (Electronic Communications Law - approved by Law no. 5/2004 of 10 February and subsequently amended by Decree-Law no. 176/2007 of 8 May, by Law no. 35/2008 of 28 July, by Decree-Law no. 123/2009 of 21 May, by Decree-Law no. 258/2009 of 25 September, Law no. 51/2011 of 13 September, by Law no. 10/2013 of 28 January and by Law no. 42/2013 of 3 July). A period of 20 working days was provided, under both procedures, for interested parties to comment - this period ended on 27 January 2012.

Following conclusion of the prior hearing and consultation processes, the corresponding report was prepared, which is given in annex to and is an integral part of the present Decision; this report presents a summary of the responses received and sets out the position taken by ICP-ANACOM, giving reasoning for the options taken in this decision.

Decision

Accordingly, bearing in mind the conclusions of the report on the prior hearing and consultation, and pursuant to the provisions of paragraph d) of article 9 of the Statutes, as in annex to Decree-Law no. 309/2001 of 7 December, in accordance with the powers and duties provided for in point b) of article 6 of the same Statutes and in point c) of paragraph 1 and in point f) of paragraph 4 of article 5 of the *Lei das Comunicações Eletrónicas* (Electronic Communications Law), and in the exercise of the powers set out in paragraph 2 of article 54-C and point b) of article 54-E of the same law, the Management Board of ICP-ANACOM decided to approve the decision on:

- the circumstances, format and procedures applicable to the requirements of reporting security breaches or loss of integrity with significant impact on the functioning of public communications networks and publicly available electronic communication services (ANNEX A); and

- public disclosure, by companies that provide public communications networks or publicly available electronic communication services, of security breaches or loss of integrity occurring on their networks and as part of their services (ANNEX B).

ANNEX A

Circumstances, format and procedures applicable to the requirements of reporting security breaches or loss of integrity with significant impact on the functioning of public communications networks and publicly available electronic communication services

I. Circumstances

1. Pursuant to article 54-B of Law no. 5/2004 of 10 February, as amended and republished by Law no. 51/2011 of 13 September (hereinafter the "Electronic Communications Law"), undertakings providing public communications networks or publicly available electronic communications services (hereinafter, the "undertakings") are required to notify ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) as to any breach of security or loss of integrity with a significant impact on the functioning of networks or services which they provide.

2. Undertakings are required to provide notification of all breaches of security or losses of integrity as cause a serious disturbance to the functioning of networks and services, with a significant impact on the continuity of this functioning, according to the circumstances and the rules laid down in the following paragraphs.

3. For the purposes of the preceding paragraphs, undertakings are required to notify ICP-ANACOM as to:

a) Any breach of security or loss of integrity whose impact is encompassed by the following criteria:

Duration and	**Number of affected subscribers or accesses (or, pursuant to point e) of paragraph 4 of Section I, geographic area affected)**
≥ 30 minutes	number of affected subscribers or accesses ≥ 500,000 (Or, pursuant to point e) of paragraph 4 of Section I, geographic area affected ≥3.000 km^2)
≥ 1 hour	500,000 > number of affected subscribers or accesses ≥ 100,000 (Or, pursuant to point e) of paragraph 4 of Section I, 3,000 km^2 > geographic area affected ≥ 2.000 km^2)
≥ 2 hours	100,000 > number of affected subscribers or accesses ≥ 30,000 (Or, pursuant to point e) of paragraph 4 of Section I, 2,000 km^2 > geographic area affected ≥

	1,500 km2)
≥ 4 hours	30.000 > number of affected subscribers or accesses ≥ 10.000 (Or, pursuant to point e) of paragraph 4 of Section I, 1,500 km^2 > geographic area affected ≥ 1,000 km^2)
≥ 6 hours	10.000 > number of affected subscribers or accesses ≥ 5.000 (Or, pursuant to point e) of paragraph 4 of Section I, 1,000 km^2 > geographic area affected ≥ 500 km^2)
≥ 8 hours	5.000 > number of affected subscribers or accesses ≥ 1.000 (Or, pursuant to point e) of paragraph 4 of Section I, 500 km^2 > geographic area affected ≥ 100 km^2)

b) Any breach of security or loss of integrity affecting delivery to Postos de Atendimento de Segurança Pública (Emergency Service Call Centres - 112 emergency calls), directly or indirectly, of calls to the single European emergency number 112, as well as calls to 115 (national emergency number), for a period equal to or exceeding 15 minutes;

c) Any recurrent breach of security or loss of integrity, where the cumulative impact of their occurrences over a four week period is covered by one of the conditions set out in the preceding paragraphs;

d) Any breach of security or loss of integrity which occurs on a date on which the normal and continuous functioning of networks and services is particularly relevant, under the terms of paragraph 5 of this Section I, where the occurrence:

   i) has a duration equal to or exceeding one hour; and

   ii) affects one thousand or more subscribers or accesses, or, under the terms of point e) of paragraph 4 of this section I, ii) affects a geographical area equal to or exceeding 100 km^2;

e) Any breach of security or loss of integrity which impacts the functioning of all networks and services offered by a company in the entire territory of an island of the Autonomous Region of the Azores or of Madeira, where the duration thereof is equal to or exceeds 30 minutes, regardless of the number of subscribers, number of accesses and geographic area affected;

f) Any breach of security or loss of integrity, detected by the undertakings or reported by customers, which impacts the functioning of networks and services through

which services with relevance to society and to citizens are provided, by public or private undertakings and at national or regional level, as set out in paragraph 6 of this Section I, where the occurrence is of a duration equal to or exceeding 30 minutes; and

g) Any breach of security or loss of integrity whose cumulative impact on a group of companies which are covered by the conditions laid down in paragraph 2 of article 3 of Law no. 19/2012 of 8 May is covered by the conditions laid down in point a), and, insofar as it refers to the present point, in point c), both of the present paragraph 3.

4. For purposes of the preceding paragraph:

a) The impact of a breach of security or loss of integrity is to be assessed by reference to all the networks and all the services of a company that are affected thereby;

b) The number of subscribers or accesses affected by a breach of security or loss of integrity corresponds to the sum of the number of subscribers or accesses which are so affected and as comprised by the various networks and services;

c) The number of subscribers to a service that is supported by another service will only be taken into account when the support is not affected;

d) The number of subscribers or accesses affected corresponds to the number of subscribers or accesses covered by the breach of security or loss of integrity, or where it is not possible to determine this number, to an estimate based on statistical data held by the undertaking; and

e) The criterion related to the affected geographical area is only to be applied in the event that the criterion on the number of affected subscribers or accesses is inapplicable or, in the specific case and on a reasoned basis, impossible to determine or estimate.

5. For the purposes of point d) of paragraph 3 of the present Section I, notwithstanding the identification of other dates by ANACOM, as duly notified to the undertakings a minimum of five working days in advance, the following dates are deemed relevant:

a) days on which national elections are held (parliamentary, presidential, European or local);

b) days on which national referendums are held;

c) days of national exercises involving electronic communications networks or services, pursuant to point c) of article 54-D of the Electronic Communications Law; and

d) days on which regional elections are held, where security breaches or losses of integrity occur in the region in question.

6. For the purposes of point f) of paragraph 3 of the present Section I, and notwithstanding the possible identification of other bodies by ANACOM, as duly notified to the undertakings a minimum of five working days in advance, SIRESP - Sistema Integrado de Redes de Emergência e Segurança de Portugal (Integrated Security and Emergency Network System) is deemed a relevant body.

II. Format and Procedures

1. For every breach of security or loss of integrity that is subject to notification under the provisions of Section I, undertakings are required to submit the following to ICP-ANACOM:

a) an initial notification, pursuant to paragraphs 4 and 5 of the present Section II;

b) a final notification, pursuant to paragraphs 8 and 9 of the present Section II; and

c) whenever required, in accordance with the provisions of paragraph 6 of the present Section II, notice of the cessation of the breach of security or loss of integrity with significant impact, in accordance with paragraphs 6 and 7 of the present Section II.

2. In the circumstance detailed in point c) of paragraph 3 of Section I, undertakings are only required to submit a final notification to ICP-ANACOM, pursuant to paragraphs 8 and 9 of this Section II, *mutatis mutandis*.

3. In the circumstance referred to in point g) of paragraph 3 of Section I, a single series of notifications may be submitted to ICP-ANACOM, pursuant to paragraph 1 of this Section II, provided that said notifications:

a) cover the entire impact of the security breach or loss of integrity; and

b) are submitted on behalf of all the undertakings.

4. The initial notification is to be sent at the earliest opportunity and when the company is able to conclude that there is or will be significant impact, up to one hour subsequent to ascertaining the circumstance detailed in Section I as, in each specific case, determines the obligation of notification, whereas the undertaking, notwithstanding compliance with this deadline, is required to give priority to the mitigation and resolution of the breach of security or loss of integrity.

5. The notification referred to in the preceding paragraph is to include the following information:

a) Name, telephone number and email address of a representative of the undertaking for the purpose of any contact by ICP-ANACOM;
b) Date and time that the breach of security or loss of integrity took on significant impact or, where this cannot be determined, the date and time of its detection;
c) Date and time that the breach of security or loss of integrity ceased to have significant impact or, where impact persists, the date and time that it is estimated that significant impact will cease;

d) Brief description of the security breach or loss of integrity, including an indication of the category of the root cause and, as far as possible, the details;

e) Possible estimate of its impact in terms of:

   i) networks and services affected;

   ii) access to emergency services;

   iii) number of subscribers or accesses affected;

   iv) geographical area affected, in km^2; and

f) Observations.

6. After the breach of security or loss of integrity ceases to have significant impact, and whenever it has not already been reported in the initial notification, undertakings are required submit to ICP-ANACOM, at the earliest opportunity and within a maximum period of two hours after such impact ceases, notice that the breach of security or loss of integrity with significant impact has been resolved.

7. The notification referred to in the preceding paragraph must, as far as possible, include the following information:

a) An update to the information provided in the initial notification; and

b) A brief description of actions taken to resolve the breach of security or loss of integrity.

8. The final notification is to be sent within a period of twenty working days from the time that breach of security or loss of integrity ceases to have significant impact.

9. The notification referred to in the preceding paragraph must include the following information:

a) Date and time that the breach of security or loss of integrity took on significant impact or, where this cannot be determined, its detection;

b) Date and time that the breach of security or loss of integrity ceased to have significant impact;

c) Date and time that the security breach or loss of integrity commenced, or where this is not possible to determine, the date and time of its detection and date and time of cessation, where different from the dates and hours reported, respectively, in accordance with points a) and b);

d) Impact of the breach of security or loss of integrity in terms of:

   i) Networks (including national and international interconnections) and respective infrastructure (including systems) and affected services;

   ii) Access to emergency services using 112 (single European emergency number) (including access using the national emergency number 115);

   iii) Number of affected subscribers or accesses by network or service;

   iv) Percentage of affected subscribers or accesses as proportion of total subscribers or accesses by network or service access; and

   v) Geographical area affected, in km^2;

e) Description of the security breach or loss of integrity, including indication of the category of the root cause and detail;

f) Indication of measures taken to mitigate the breach of security or loss of integrity;

g) Indication of measures adopted to resolve the breach of security or loss of integrity, including, in the event of breaches of security or loss of integrity with partial restoration, the chronology and detail of the stages of restoration;

h) Indication of the measures taken and/or planned to prevent or minimize the occurrence of similar security breaches or losses of integrity in the future (in terms of planning and/or operations, of contingency planning, of interconnection agreements, of service level agreements and other relevant areas) and the date on which they took or will take effect;

i) When appropriate, the information made available to the public regarding the breach of security or loss of integrity, including any updates to this information, and the date and time of such disclosure;

j) Other relevant information; and

k) Observations.

10. For the purposes of paragraphs 5, 7 and 9 of this Section II, the root causes of breaches of security or loss of integrity can have the following categories:

a) Accident/natural disaster;

b) Human error;

c) Malicious attack;

d) Hardware/software failure; or

e) Failure by an external party to supply goods or services.

11. Wherever possible, the information included in the notifications set out in the present Section II on the number of subscribers or accesses is to follow the definitions set out in the framework of obligations governing the periodic submission of information to ICP-ANACOM.

12. The notifications set out in the present Section II are to be performed using the following means:

a) as regards initial notifications and notifications of cessation of breaches of security or losses of integrity with significant impact, by email to notifica@anacom.pt and by telephone 214340899; and

b) as regards the final notification, by delivery in person or by registered mail.

13. Companies whose networks or services have their functioning impacted by such breaches of security or losses of integrity are to cooperate among themselves to ensure the proper detection of any breach of security or loss of integrity and to undertake assessment of its impact, and in the case referred to in point g) of paragraph 3 of Section I, for the respective notification.

14. With a view to the proper performance of the provisions of the present Annex A, it is incumbent upon the undertakings to deploy all the resources and procedures as are necessary to detect and evaluate security breaches or losses of integrity covered by the circumstances set out in Section I, assess their respective impact and undertake notification.

III. Entry into force and transitional provision

1. The undertakings are required to implement such measures as are necessary in order to comply with the provisions of the present Annex A, doing so no later than 12 June 2014, without prejudice to the following paragraph.

2. Based on available data and with reference to the circumstances described in Section I of the present Annex A and the requirements for the final notification given in paragraph 9 of Section II, undertakings are required to submit to ICP-ANACOM:

a) a report on the period starting on 1 January 2013 and ending on the date of approval of the present decision, which report is to be submitted no later than 12 January 2014; and

b) six monthly reports, covering the entire period specified in paragraph 1 of the present Section III, each report to be submitted no later than one month following the end of the period to which it relates.

ANNEX B

Public disclosure, by undertakings that provide public communications networks or publicly available electronic communication services, of security breaches or losses of integrity occurring on their networks and services

I. Conditions

1. Pursuant to point b) of article 54-E of Law no. 5/2004 of 10 February, as amended and republished by Law no. 51/2011 of 13 September (hereinafter "Electronic Communications Law"), it is incumbent upon ICP - Autoridade Nacional de Comunicações (ICP-ANACOM) to require undertakings which provide public communications networks or electronic communications services accessible to the public (hereinafter, the "undertakings") to inform the public, by appropriate means, of breaches of security or losses of network integrity, where deemed by ICP-ANACOM as being in the public interest.

2. ICP-ANACOM determines that it is in the public interest that undertakings inform the public as to any breach of security or loss of integrity whose impact on the functioning of their networks and services is encompassed by the following criteria:

Duration and	**Number of subscribers or accesses affected** **(or, pursuant to point e) of paragraph 3 of Section I, geographic area affected)**
≥ 30 minutes	no. of subscribers or accesses affected ≥ 500,000 (or, pursuant to point e) of paragraph 3 of Section I, geographic area affected - 3,000 km^2)
≥ 1 hour	500.000 > number of affected subscribers or accesses ≥ 100,000 (or, pursuant to point e) of paragraph 3 of Section I, 3,000 km^2 > geographic area affected ≥ 2,000 km^2)
≥ 2 hours	100.000 > number of affected subscribers or accesses ≥ 30,000 (or, pursuant to point e) of paragraph 3 of Section I, 2,000 km^2 > geographic area affected ≥ 1,500 km^2)
≥ 4 hours	30.000 > number of affected subscribers or accesses ≥ 10,000 (or, pursuant to point e) of paragraph 3 of Section I, 1,500 km^2 > geographic area affected ≥ 1,000 km^2)

3. For the purposes of the preceding paragraph:

a) The impact of a breach of security or loss of integrity is to be assessed by reference to all the networks and all the services of a company that are affected thereby;
b) The number of subscribers or accesses affected by a breach of security or loss of integrity corresponds to the sum of the number of subscribers or accesses which are so affected and as comprised by the various networks and services;
c) The number of subscribers to a service that is supported by another service will only be taken into account when the support is not affected;
d) The number of subscribers or accesses affected corresponds to the number of subscribers or accesses covered by the breach of security or loss of integrity, or where it is not possible to determine this number, to an estimate based on statistical data held by the undertaking; and
e) The criterion related to the affected geographical area is only to be applied in the event that the criterion on the number of affected subscribers or accesses is inapplicable or, in the specific case and on a reasoned basis, impossible to determine or estimate.

4. Notwithstanding the provisions of the present Annex B, ICP-ANACOM may, pursuant to paragraph b) of article 54 of the Electronic Communications Law, including in circumstances not provided for in paragraph 2 of the present Section I, order undertakings to inform the public as to other breaches of security or losses of integrity occurring on their networks and as part of their services.

II. Contents, means and timing of disclosure

1. In their disclosure to the public of breaches of security or losses of integrity referred to in Section I, undertakings are required to:

a) Ensure that the content of the disclosure is clear, accessible and as precise as possible and includes, among other relevant information:

i) Indication of the networks and services affected; and

ii) The length of time it is expected to take to resolve the occurrence or, if applicable, the date of resolution;

b) Provide, as a minimum, information on their respective web sites, as used in their relationship with users, through a hyperlink posted on the homepage of the website, which hyperlink shall be immediately visible and identifiable without scrolling;

c) Provide the information at the earliest opportunity and within four business hours following the deadline of the initial notification to ICP-ANACOM[1],for this purpose, working hours means time elapsing between 09.00 and 19.00 on a working day;

d) Update the information whenever a significant alteration occurs and immediately after the breach of security or loss of integrity ceases; and

e) Ensure that the information provided on the Internet remains accessible to the public, in the same locations as referred to in point b), for a period of one month following the date on which the breach of security or loss of integrity ceases.

2. Companies are required to notify ICP-ANACOM, upon commencing their activity, as to the URL addresses[2] of web pages which, for the purposes of point b) above, they will use to provide public disclosure of security breaches or losses of integrity occurring on their networks and as part of their services, and notify ICP-ANACOM as to any subsequent amendments thereto within a minimum of 5 working days subsequent to such amendments being implemented.

3. With a view to the proper performance of the provisions of this Annex A, it is incumbent upon the undertakings to implement all the means and procedures as are necessary to detect and evaluate security breaches or losses of integrity covered by the circumstances set out in Section I, assess their respective impact and undertake notification.

III. Entry into force and transitional provision

1. The undertakings are required to implement such measures as necessary in order to comply with the provisions of the present Annex B, doing so no later than 12 June 2014.

---

[1] In accordance with the provisions of Section II of Annex A.

[2] Uniform Resource Locator.

2. Undertakings are required to notify ICP-ANACOM, a minimum of 15 working days prior to the expiry of the period specified in the preceding paragraph, as to the URL addresses referred to in paragraph 2 of Section II.