Act No. 62, 25 June 2012 amending the Electronic Communications Act and the Act on the Post and Telecom Administration (CERT-IS, operating fee, etc.).

ACT

amending the Electronic Communications Act and the Act on the Post and Telecom Administration (CERT-IS, operating fee, etc.).

CHAPTER I

Amendment to the Electronic Communications Act, No 81/2003, with subsequent amendments

Article 1

In Article 2 of the Act, paragraphs 6 and 7 shall read as follows:

To serve as a forum for consultation and information exchange, the Minister may establish an Expert Group of representatives from the Post and Telecom Administration in Iceland, stakeholders and other actors in the field of electronic communications.

The Minister may issue a Regulation concerning the Expert Group's activities in the field of electronic communications.

Article 2

In Article 3 of the Act, the following definitions shall be added in the appropriate alphabetical order:

1. *CERT-IS*: A computer security and incident response team (CSIRT) operating under the aegis of the Post and Telecom Administration in Iceland for the protection of critical information infrastructure against cyber-attacks;

2. *Network and information security*: The ability of electronic communications networks to ensure that certain pre-determined safety margins are maintained when threats are imminent or if vulnerabilities arise, for instance through human error or sabotage, that compromise the confidentiality, integrity and availability of electronic communications network information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved;

3. *Constituency*: Stand-alone or, as the case may be, interconnected electronic communications systems and/or information systems under the aegis of CERT-IS constituents, among them critical information infrastructure operators who have entered into service contracts with CERT-IS for advice, assistance and preparedness for the purpose of resisting potential cyber-attacks intended to render the systems unresponsive, damage them or acquire illicit financial gain, such as by the theft of data or money;

4. *CERT-IS constituents or constituency members*: The constituency membership consists, on the one hand, of undertakings operating public communications networks and/or providing access to the internet and internet services, and, on the other hand, of critical information infrastructure operators joining the constituency under a service contract with CERT-IS. The constituents' networks concerned form what is known as a constituency, security incidents within which are given priority within the CERT-IS service portfolio;

5. *Critical information infrastructure*: The information systems of the important societal infrastructure which is to safeguard national security, the public interest and the procurement of various types of supplies in a developed and technologically advanced society. Critical information infrastructure involves the hardware and software necessary for the operation and functionality of the system, and the information stored by the system or transmitted over it. The National Commissioner of the Icelandic Police shall designate critical information infrastructure;

6. *Security event*: The occurrence of a system, service or network state indicating a possible breach of security policy or a failure of safeguards, or a previously unknown situation which may be security relevant;

7. *Security incident*: An incident 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;

8. *Anonymous real-time data*: Numerical information and codes providing traceability of electronic communications traffic on IP networks.

Article 3

In Article 6 of the Act, paragraph 2(e) shall be deleted.

Article 4

In Article 15 of the Act, a new paragraph shall be inserted after paragraph 1, reading as follows:

The Post and Telecom Administration in Iceland shall oversee a common number portability data base (NPDB) for looking up numbers and implementing number portability. The architecture of the NPDB, such as code registration and number sequence tagging, querying and dissemination options, and the design of common procedures for porting numbers shall be subject to the approval of the Post and Telecom Administration.

Article 5

Article 23 of the Act shall be amended as follows:

a. In paragraph 1, the words “PTA” (the Post and Telecom Administration in Iceland) shall be replaced by: “the Telecommunications Fund”.

b. In paragraph 2, after the words “as a rule be paid” the following shall be inserted: “from the Telecommunications Fund or, where applicable,”.

Article 6

The following three new paragraphs shall be added to Article 36:

In sparsely populated areas where distances are great, electronic communications undertakings may request joint utilisation of utility company earthmoving operations for the purpose of installing telecommunications facilities concomitantly with such operations, the telecommunications portion of the cost being calculated as the incremental cost of such operations only. Utility companies creating facilities for water and/or electric mains by earthmoving operations, including companies subject to paragraphs 1 and 2, may accept such requests, provided care is taken that competitive activities are not subsidised by activities enjoying exclusive rights or by protected operations.

Apportionment of costs pursuant to paragraph 3 shall be subject to the condition that electronic communications undertakings be offered open wholesale access to any telecommunications facilities thus constructed. Access charges shall be calculated based on cost plus a reasonable mark-up. Reasonable notice, not less than two months, shall be given of any planned operations, and public electronic communications network operators shall be given the option of putting in place their own telecommunications facilities on the same terms, if technologically feasible.

In the event of a dispute over how to calculate the telecommunications portion of the cost over and above the total cost of the operations, or concerning wholesale access charges pursuant to paragraphs 3 and 4, the Post and Telecom Administration in Iceland shall rule on the issue.

Article 7

Article 47 of the Act shall be amended as follows:

a. The following sentence shall be added to paragraph 10: Electronic communications undertakings shall adopt procedures for responding to requests for police access to users' personal data.

b. The following six new sentences shall be added to paragraph 11: The obligation of confidentiality shall remain in force even though employment may cease. Electronic communications undertakings shall request police security clearances for those of their employees making connections for telephone monitoring by police. In this context, the police are authorised, after obtaining the written consent of the individual concerned, to gather information on the background and any criminal history of the employee in question, such as from police records, criminal records or other public records. Before concluding their investigation, the police shall give the person under investigation the opportunity to express his or her views. He or she shall furthermore be entitled to the reasons, should the police decide to refuse him or her a security clearance. A police decision to refuse a security

clearance may be appealed to the Minister pursuant to the provisions of the Administrative Procedures Act.

c. The following paragraph shall be added:

The Minister may issue a Regulation concerning the obligations of electronic communications undertakings regarding the retention of information and police access to electronic communications transmissions and information pursuant to the present Article.

Article 8

At the end of Article 47 of the Act, the following new Article, Article 47(a), along with a heading, shall be inserted:

A Computer Security and Incident Response Team for the protection of critical information infrastructure.

The Post and Telecom Administration in Iceland shall operate cyber security team CERT-IS, which shall serve as a computer security and incident response team (CSIRT) for the protection of critical information infrastructure from cyber-attacks. Serving as a CERT-team for Iceland, CERT-IS shall participate and serve as the contact for the Icelandic authorities in national and international cooperation on incident response for network and information security. The aim of CERT-IS activities is to prevent and mitigate as much as possible the risk of cyber-attacks and other security incidents against its constituency, and to counteract and minimise any critical information infrastructure damage resulting from such attacks and incidents.

CERT-IS shall seek to identify security incidents at an early stage and to keep such incidents from spreading and damaging critical information infrastructure within its constituency. CERT-IS shall assist its constituency through prevention, advice and support for a rapid response to any impending danger. During any wide-spread security incidents, CERT-IS shall co-ordinate its constituents' measures to counter impending danger for the purpose of damage minimisation and the recovery of unresponsive systems. CERT-IS shall advise its constituency on prevention and preparedness, and shall communicate information to the public as may be deemed necessary.

CERT-IS is authorised to request from electronic communications undertakings anonymous real-time data on internet traffic volume, including at interconnection points between such undertakings and at international gateways. When a major cyber-attack is suspected, CERT-IS is authorised to scan the control information of electronic communications packets relating to possible security threats for more detailed information on their origin, destination, and technical properties. Information obtained in this way may be used for the purpose of security incident prevention or damage mitigation only. Information obtained pursuant to the present Article may not be personally identified and shall be deleted as soon as possible, yet in any event no later than six months form the date it was acquired. Electronic communications undertakings must house and interconnect with CERT-IS monitoring equipment free of charge.

Where there is reasonable suspicion that individual transmissions contain malicious code, CERT-IS is authorised, with the consent of individual critical information infrastructure operators, to analyse the content of individual electronic communication transmissions to and from the network concerned. This authorisation shall not, however, apply to inspection of transmissions on public electronic communications networks operated by electronic communications undertakings. The transmission's sender and recipient shall be notified that the transmission will be inspected and shall, if possible, be given the opportunity to be present during the inspection. In other respects, CERT-IS shall operate in accordance with any conditions for the processing to take place imposed by the Data Protection Authority of Iceland.

In cases where national security and the public interest are at stake, CERT-IS may notify the National Commissioner of the Icelandic Police of any major cyber-attacks against its constituency and of any serious or wide-spread security incidents which have caused damage or the risk of damage to critical information infrastructure. At the request of the Police Commissioner, CERT-IS shall engage in co-operation on prevention and response.

After receiving the comments of the Data Protection Authority, the Minister shall issue more detailed provisions on the operation of CERT-IS in a Regulation, which shall, inter alia, address:

a. the mission, organisation and tasks of CERT-IS;

b. co-ordination of intra-constituency collaboration and dissemination of information;

c. the appointment and eligibility of CERT-IS staff, including staff security clearances;

d. dissemination of information to foreign partners and the appropriate security measures pertaining thereto;

e. oversight arrangements for mechanical scanning of electronic communications traffic;

f. procedures for inspecting the content of electronic communications with the controller's consent;

g. measures to guarantee the security and deletion of data, and other measures to guarantee the right to privacy;

h. the duty of electronic communications undertakings and other stakeholders to report security incidents;

i. testing and auditing of network and information security and of information system resilience which CERT-IS may undertake;

j. the substance matter of service agreements CERT-IS enters into with critical information infrastructure operators;

k. reporting on CERT-IS activities.

Article 9

The following paragraph shall be added to Article 61 of the Act:

Manufacturing and marketing of hardware or software designed or adapted for the purpose of circumventing the rights of service providers providing services through conditional access systems is prohibited.

CHAPTER II

Amendment to the Electronic Communications Act No 69/2003,

with subsequent amendments

Article 10

In the opening sentence of Article 14(4) of the Act, “0.30%” and “0.25%” shall be replaced by: 0.38%; and: 0.34%, respectively.

CHAPTER III

Entry into force

Article 11

This Act shall enter into force immediately.