ACT

Of ….2014

On Cyber Security and Change of Related Acts (Act on Cyber Security)

The Parliament has resolved on the following Act of the Czech Republic:

PART ONE
Cyber Security

Chapter I
General provisions

§ 1

Subject of the Act

(1) This Act regulates rights and obligations of natural and legal persons and competence and power of public authorities in the field of cyber security.

(2) This Act shall not apply to information and communication systems handling classified information.

Basic periods

§ 2

For the purpose of this Act:

a) Cyber space means digital environment, enabling to create, process and exchange information, created by information systems and services and electronic communication networks[1],

b) Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems[2] within the field of cyber security,

[1] Act No. 127/2005 Coll. on Electronic Communications and on Amendment to certain related Acts (Electronic Communications Act)

[2] §2 of the Act No. 240/2000 Coll. on Crisis Management (the Crisis Act), as amended by Act No. 320/2002 Coll. and Act No. 430/2010 Coll.

c) Security of information means ensuring confidentiality, integrity and availability of information,

d) Important information system means an information system administrated by a public authority, that is not critical information infrastructure and which may endanger or noticeably limit the performance of public administration in case of information security breach,

e) Administrator of information system means a public authority or natural and legal person, which determine the purpose of the information processing and conditions for the information system administration,

f) Administrator of the communication system means a public authority or natural and legal person, which determine the purpose of the communication system and conditions for its administration and

g) Important network means electronic communication network**1** providing direct international interconnection to public communication networks or providing direct connection to critical information infrastructure.

§ 3

Liable public authorities and natural and legal persons in the cyber security field are as follows:

a) Electronic communication service provider and entity operating electronic communication network1, unless set out in b),

b) Public authority or natural and legal person administrating important network, unless being administrator of communication system as set out in d),

c) Administrator of critical information infrastructure information system,

d) Administrator of critical information infrastructure communication system and

e) Administrator of important information system.

Chapter II

System to ensure cyber security

Security measures

§ 4

(1) Security measures mean a complex of activities, with the purpose of ensuring the security of information in information systems and availability and reliability of services and networks of electronic communications in cyber space.

(2) Public authorities and natural and legal persons set out in § 3 c) to e) are obliged in the extent necessary for ensuring cyber security to determine and implement security measures for critical information infrastructure information system, critical information infrastructure communication system or important information system and to keep security measures record in security documentation

(3) The authorities and persons mentioned in § 3 c) to e) are obliged to take into consideration the security measures requirements during the provider selection of the critical information infrastructure information system, critical information infrastructure communication system or important information system. The security measures requirements considerations according to the first phrase here above shall not be considered as unlawful limitation of the competition or unjustified obstructions of the competition.

§ 5

(1) Security measures are as follows

a) Organisational measures and

b) Technical measures.

(2) Organisational measures are as follows

a) Information security management system,

b) Risk management,

c) Security policy,

d) Organisational security,

e) Security requirements on suppliers setting,

f) Assets management,

g) Human resources security,

h) Critical information infrastructure or important information system operation and communication management,

i) Access of persons to critical information infrastructure or to important information system management,

j) Acquisitions, development and maintenance of critical information infrastructure and important information systems,

k) Cyber security events and cyber security incidents management,

l) Business continuity management and

m) Critical information infrastructure and important information systems control and audit.

(3) Technical measures are as follows

a) Physical security,

b) Communication networks integrity protection tools,

c) Users' identity verification tools,

d) Access authorization management tools,

e) Counter malicious code protection tolls,

f) Critical information infrastructure and important information systems, their users and administrators activities recording tools,

g) Cyber security events detection tools,

h) Collection and evaluation of cyber security events tools,

i) Application security,

j) Cryptographic devices,

k) Tools for ensuring the levels of information availability and

l) Industrial and management systems security.

§ 6

Implementing legal regulation shall set out the following:

a) Security measures content,

b) Content and structure of security documentation and

c) Extent of security measures for public authorities and natural and legal persons set out in § 3 c) to e) and

d) Important information systems and their determinative criteria.

Cyber security event and cyber security incident

§ 7

(1) Cyber security event means an event which may cause security of information breach in information systems or security of services or security and integrity of electronic communication networks breach[1].

(2) Cyber security incident means information security breach in information systems or security of services breach or breach or integrity of electronic communication networks resulting from cyber security event.

(3) Public authorities and natural and legal persons set out in § 3 c) to e) are obliged to detect cyber security events in their important network, critical information infrastructure information system, critical information infrastructure communication system or important information system.

§ 8

Cyber security incident report

(1) Public authorities and natural and legal persons set out in § 3 b) to e) are obliged to report cyber security incidents in their important network, critical information infrastructure information system, critical information infrastructure communication system or important information system immediately after their detection; this shall not affect informational duty set out in other legal regulation[3].

[3] For example §98 paragraph 4 and §99 paragraph 4 of the Act No. 127/2005 Coll. , as amended by Act No. 153/2010 Coll. and Act No. 468/2011 Coll.

(2) Public authorities and natural and legal persons set out in § 3 b) shall report cyber security incidents to the administrator of national CERT.

(3) Public authorities and natural and legal persons set out in § 3 c) to e) shall report cyber security incidents to the National Security Authority (hereinafter referred to as the "NSA").

(4) Implementing legal regulation shall set out the following:

a) Cyber security incident's types and categories and

b) Cyber security incident report's requirements and form.

Record keeping

§ 9

(1) The NSA keeps cyber security incidents record (hereinafter referred to as "incidents record") which contains:

a) Cyber security incident report,

b) Identification data of a system where the cyber security incident occurred,

c) Cyber security incident source data and

d) Cyber security incident solving procedure, its outcome.

(2) The data set out in § 22 e) to g) may make part of the incidents record.

(3) The NSA provides incidents record data to the public authorities for the purpose of fulfilling tasks within their authority.

(4)The NSA may provide incidents record data to administrator of the national CERT, to bodies performing authority in the field of cyber security abroad and to other natural and legal persons acting in the field of cyber security in the extent necessary for ensuring protection of cyber space.

§ 10

(1) Employees of the Czech Republic working for the NSA, taking part in solving cyber security incident, are bound by confidentiality about incidents record data. Confidentiality lasts even after the termination of the labour law relationship towards the NSA.

(2) The director of the NSA may waive incidents evidence data confidentiality of persons set out in paragraph 1, together with determination of the data and waiver extent.

§ 11

Measures

(1) Measures mean the acts needed to protect information systems or services and electronic communication networks[1] from the threat in the cyber security field or from the cyber security incident or acts to solve already present cyber security incident.

(2) Measures are as follows:

a) Warnings,

b) Reactive measures and

c) Protective measures.

(3) Reactive measures are obligatorily carried out by:

a) Public authorities and natural and legal persons set out in § 3 a) and b) under the state of cyber emergency or under the state of emergency[4] in cases set out in §21 paragraph 6 and

b) Public authorities and natural and legal persons set out in § 3 c) to e).

(4) Protective measures are obligatorily carried out by public authorities and natural and legal persons set out in § 3 c) to e).

§ 12

Warning

(1) The NSA shall issue warning in case it finds out, particularly from its own action or on the initiative of the administrator of the national CERT or from foreign cyber security authorities, that the threat in the field of cyber security occurs.

(2) Warning shall be published by the NSA on its internet websites and shall be notified to public authorities and natural and legal persons set out in § 3 via contact details kept in the evidence as set out in §16 paragraph 4.

Reactive and protective measures

§ 13

(1) The NSA shall issue decision on reactive measures to solve cyber security incident or to secure information systems or networks and electronic communication services[1] from cyber security incident, which is the first legal act in re. If it is not possible to deliver the decision into the hands of the addressee within 3 days from the day of its issuance, it is enforceable upon publishing on the NSA's public notice board. The decision set out in the first sentence may be issued by the NSA on site according to Administrative Procedure Code.

(2) Appeal against decision according to paragraph 1 has no suspensory effect.

(3) If the reactive measure to solve cyber security incident or to secure information systems or networks and services in electronic communications from cyber security incident concerns unspecified group of public authorities and natural and legal persons, such reactive measure shall be issued by the NSA by a measure of general nature.

(4) Public authorities and natural and legal persons as set out in §3 are obliged to immediately inform the NSA about execution of the reactive measure and its result. Terms of the notice shall be set out in implementing legal regulation.

[4] Constitutional Act of Law No. 110/1998 Coll., on the Security of the Czech Republic, as amended by Act No. 300/2000 Coll.

§ 14

(1) The NSA shall issue protective measure by measure of general nature on the basis of an already solved cyber security incident analysis in order to increase protection of information systems or services or electronic communication networks1.

(2) The NSA shall determine the method of increasing protection of information systems or services and electronic communication networks1 and deadline for its execution to public authorities and natural and legal persons set out in § 3 c) to e) by a measure of general nature.

§ 15

(1) Measures of general nature according to § 13 or § 14 come into force upon publishing on the NSA's public notice board; provision § 172 of the Administrative Procedure Code shall not be used. Public authorities and natural and legal persons as set out in § 3 shall be notified about the issuance of the measure of general nature via contact details in the evidence according to § 16 paragraph 4.

(2) The comments to the measure of general nature issued according to § 13 or § 14 may be applied within 30 days upon its publishing on the NSA's public notice board. The NSA may change or repeal the measure of general nature in line with applied comments.

§ 16

Contact details

(1) The contact details mean:

a) As for legal person, the trading company or the name, address of the seat, identification number of the person or similar number assigned abroad,

b) As for natural person pursuing business, the trading company or the name including differentiating amendment or other marking, address of the seat and identification number of a person,

c) As for public authority, its name, address of the seat, person registration number, if assigned and the public authority identification, when the person registration number is not assigned,

and the natural person's data, who is authorized to act on behalf of the public authority or natural or legal person in issues provided for by this Act ; name, surname, telephone number and electronic mail address.

(2) Contact details and their changes shall be announced by

a) Public authority or natural and legal persons set out in § 3 a) and b) to the administrator of the national CERT and

b) Public authority or natural and legal persons set out in § 3 c) to e) to the NSA.

(3) Public authority or natural and legal persons set out in § 3 c) to e) shall immediately announce changes only of the details set out in paragraph 1, which are not referential details kept in the basic registers.

(4) The NSA shall keep contact details evidence, which contains details set out in paragraph 1.

(5) The NSA is authorized to require contact details collected by the administrator of the national CERT according to paragraph 2 a) under the state cyber emergency.

(6) Contact details notice template and its form shall be set out in the implementing legal regulation.

§ 17

National CERT

(1) National CERT ensures under the provisions of this Act information sharing on national and international level in the field of cyber security.

(2) Administrator of the national CERT shall

a) Accept the contact details notice from public authorities or natural and legal persons set out in § 3 a) and b), keep record of and store them,

b) Accept cyber security incidents reports from public authorities or natural and legal persons set out in § 3 b), keep record of, store and protect them,

c) Evaluate cyber security incidents as for public authorities or natural and legal persons set out in § 3 b),

d) Provide public authorities or natural and legal persons set out in §3 a) and b) with methodical support, help and cooperation when cyber security incident occurs.,

e) Act as point of contact for public authorities or natural and legal persons set out in §3 a) and b),

f) Carry out vulnerability analysis in the cyber security field,

g) Transmit to the NSA the cyber security incident data without disclosing the announcer of the cyber security incident and

h) Under the state of cyber emergency and on the NSA's request, transmits contact details of public authorities or natural and legal persons set out in §3 a) and b).

(3) Administrator of national CERT may, on its own behalf and responsibility, perform also other business activity in the field of cyber security unspecified by this Act, in case such an activity does not harm the duties fulfilment set out in paragraph 2.

(4) Administrator of national CERT shall coordinate its activities with the NSA while fulfilling its duties set out in paragraph 2.

(5) Administrator of national CERT shall act inpartially when fulfilling the duties according to paragraph 2.

§ 18

Administrator of national CERT

(1) Administrator of national CERT may be only a legal person

a) Who fulfils conditions set out in paragraph 2 and

b) Who was concluded a public-law contract with the NSA according to § 19.

(2) Administrator of national CERT may be only a legal person who

a) Does not carry out any activities against the interests of the Czech Republic according to Act on Protection of Classified Information and has never done so,

b) Operates or administrates information systems or services and electronic communication networks[1] or participates in their operation and administration, at least for the time period of 5 years,

c) Has technological prerequisites for the field of cyber security,

d) Is a member of a multinational organisation operating in the field of cyber security,

e) Has no record of arrears in the evidence of taxes by the financial and customs authorities of the Czech Republic, nor in the evidence of taxes, nor in the evidence of social insurance, nor in the evidence of health insurance and

f) Has not been sentenced for committing any crime set out in §7 of the Act No. 418/2011 Coll., on the criminal responsibility of legal persons and proceedings against them.

g) Is not a foreign person accordin to another legal prescription and hasn´t been created solely to gain profit; therefore the National CERT´s operator ability to perform according to§ 17 paragraph 3.

(3) The interested applicant proves the fulfilment of conditions stated above via presentation of

a) Statutory declaration in case of paragraph 2 a) to d), g) and h) and

b) Confirmation by the financial and customs authorities of the Czech Republic in case of paragraph 2 a).

(4) From the content of the statutory declaration according to paragraph 3 a) it must be clear that the applicant fulfils relevant prerequisites. Confirmation according to paragraph 3 b) that applicant does not have in the evidence of taxes of financial and customs authorities of the Czech Republic nor in the evidence of taxes nor in the evidence of social insurance and public health insurance, has no record of arrears. This confirmation must not be older than 30days.In order to prove conditions stated in paragraph 2 f), the NSA shall require criminal record according to different legal regulation.[5]

(5) Administrator of the national CERT proceeds its activities according to §17 paragraph 2, a), b), c), e), g) and h free of charge.

(6) The NSA shall publish the administrator of the national CERT's data; the trading company or name, address of seat, identification number of person, identification of data box and address of the internet pages.

§ 19

Public-law contract

(1) The NSA concludes a public-law contract (hereinafter referred to as „contract") with a legal person chosen by the selection procedure in line with § 163 paragraph 4 of the Administrative Procedure Code in order to cooperate in the field of cyber security and ensure activities set out in § 17 paragraph 2. The selection procedure shall be published by the NSA.

(2) The contract contains at least

a) Indication of contracting parties,

b) Definition of the subject of the contract,

c) Rights and obligations of the contracting parties,

d) Cooperation conditions of the contracting parties,

e) Terms and conditions of the parties' withdrawal from the contract,

f) Notice period and notice reasons,

g) Ban on misuse of data acquired while performing activities set out in §17 paragraph 2,

h) Terms of national CERT activities according to § 17 paragraph 3 and

i) Terms of handover and extent of data handed over to the NSA if the contract loses effect.

(3) The contract concluded according to paragraph 1 shall be published in the NSA's Bulletin, except for the parts of the contract, whose publishing is not allowed by other legal regulation.

(4) If the contract is not concluded according to paragraph 1, or if the contract loses effect, the activity of the national CERT shall be fulfilled by the NSA.

§ 20

Governmental CERT

Governmental CERT, as a part of the NSA

a) Receives the contact details notice from public authorities and natural and legal persons set out in § 3 c) to e),

b) Receives cyber security incidents reports from public authorities and natural and legal persons set out in § 3 c) to e),

c) Evaluates cyber security events and cyber security incidents data from critical information infrastructure, from important information systems and from other information systems of the public administration,

d) Provides methodical support and help to public authorities and natural and legal persons set out in § 3 c) to e)

e) Provides cooperation to public authorities and natural and legal persons set out in §3 c) to e) during cyber security incidents and cyber security events,

f) Receives impulses and data from public authorities and natural and legal persons set out in §3 and from other public authorities and natural and legal persons, and analyses these impulses and data,

g) Receives data from the administrator of the national CERT and analyses this data,

h) Receives data from bodies, performing authority in the field of cyber security abroad, and analyses this data,

i) Provides according to §9 paragraph 4 to the administrator of the national CERT, entities performing authority in the field of cyber security abroad and other entities acting in the field of cyber security with incidents record data and

j) Performs vulnerability analysis in the field of cyber security.

Chapter III

State of cyber emergency

§ 21

(1) State of cyber emergency means a state, during which information security in information systems or security and integrity of services or electronic communication networks is seriously endangered and the interests of the Czech Republic may thus be violated or endangered according to the law on protection of classified information.

(2) State of cyber emergency shall be declared by the Director of the NSA. The decision on the state of cyber emergency declaration shall be announced on the NSA's public notice board. Information on the state of cyber emergency declaration shall be published in communication mass media. The provider of the television or radio broadcasting is obliged to announce the information on the state of cyber emergency declaration without cost reimbursement, on request of the NSA, without delay and with no content and meaning adjustment.

(3) Decision on the state of cyber emergency declaration enters into force at the moment stipulated in the decision. State of cyber emergency shall be declared for a necessary period of time, for a maximum of 7 days. The period given may be prolonged; total period of a declared state of cyber emergency shall not exceed 30 days.

(4) During the state of cyber emergency the NSA Director shall inform the government about the procedure of the state of cyber emergency solving and about current state of threats, which led to the state of cyber emergency declaration. Under the state of cyber emergency and under the state of emergency in cases set out in paragraph 6, the NSA is entitled to issue decisions or measures of general nature according to §13 also to public authorities and natural and legal persons set out in §3 a) and b).

(5) State of cyber emergency shall not be declared in case when the threat to security of information in the information systems or security of services or security and integrity of electronic communication networks[1] threat may be averted by the NSA's activities according to this Act.

(6) If it is not possible to avert the threat to information security in information systems or to security of services or security and integrity of electronic communication networks[1] within the framework of the state of cyber emergency, the NSA Director shall immediately ask the government to declare state of emergency. Decisions and measures of general nature issued by the NSA according to §13 before the state of emergency declaration remain effective as long as such measures do not contradict the emergency measures declared by the government.

(7) State of cyber emergency shall terminate after the given period, unless the NSA Director decides to terminate it earlier or by declaration of state of emergency[4].

Chapter IV

State administration performance

§ 22

(1) State administration in the field of cyber security is carried out by the NSA, unless otherwise stipulated by the law.

(2) The NSA

a) Determines security measures,

b) Issues countermeasures,

c) Ensures the activities of the National Cyber Security Centre,

d) Keeps records according to this Act,

e) Imposes fines for administrative offences according to this Act,

f) Acts like a coordination body during the state of cyber emergency,

g) Cooperates with public authorities and natural and legal persons, which work in the field of cyber security, especially with public-law corporations, research and development units and other units of CERT type,

h) Ensures international cooperation,

i) Negotiates and concludes agreements on international cooperation,

j) Ensures prevention, education and methodical support in the field of cyber security,

k) Ensures research and development in the field of cyber security,

l) Concludes public-law contract with the national CERT administrator,

m) According to Emergency law, it sends to the Ministry of Interior proposals of critical infrastructure elements in the area of communication and information systems in the field of cyber security, the administrator of which is an organisational state body,

n) Determines elements of critical infrastructure in the area of communication and information systems in the field of cyber security according to Emergency law, except elements set out in m) and

o) Fulfils other tasks in the field of cyber security set out by this Act.

Chapter V

Control, supervision and administrative offences

§ 23

Control

(1) The NSA shall perform control in the field of cyber security. While performing control, the NSA determines how public authorities and natural and legal persons set out in §3 fulfil duties set by this Act and decisions and measures of general nature issued by the NSA, and how they respect the implementing legal regulations in the field of cyber security.

(2) The NSA controls

a) Public authorities and natural and legal persons set out in § 3 a) and b), whether they fulfil duties assigned by the NSA via decision or measure of general nature according to §13under the state of cyber emergency,

b) Public authorities and natural and legal persons set out in § 3 c) to e), whether they fulfil duties set out in §4 paragraph 2, §8 paragraph 3 and §16 paragraph 2 b) and duties assigned by the NSA via decision or measure of general interest according to §13 or §14.

§ 24

Corrective measures

(1) In case the NSA ascertains any deficiencies during control, it assigns the controlled public authority or natural and legal persons to rectify them in a specified period of time and possibly to determine in which way.

(2) In case the critical information infrastructure information system, critical information infrastructure communication system or important information system is immediately endangered by cyber security incident, which can significantly damage or destroy it, the controlling body may prohibit the controlled public authority or natural and legal persons from using this system or its parts until the ascertained deficiency is eliminated.

Administrative offences

§ 25

(1) Legal entity or natural entity pursuing business set out in § 3 a) or b) commits administrative offence in the following cases:

a) Does not implement duties assigned by the NSA via decision or measure of general nature according to § 13, or

b) Does not fulfil some of the obligations imposed by the corrective measure according to § 24.

(2) Legal entity or natural entity pursuing business set out in § 3 c) to e) commits administrative offence in the following cases:

a) Does not implement security measures contrary to § 4 paragraph 2 or does not keep security measures record,

b) Does not notify cyber security incident according to § 8 paragraphs 1 and 3,

c) Does not implement duty assigned by the NSA via decision or measure of general nature according to §13 or §14,

d) Does not notify contact details or their changes to the NSA according to § 16 paragraph 2 b) or

e) Does not fulfil some of the obligations imposed by the corrective measure according to § 24.

(3) The penalty in case of administrative offence reaches up to:

a) 100 000 CZK in case of administrative offence set out in paragraph 1 a) or b) or paragraph 2 a) to c) or e),.

b) 10 000 CZK in case of administrative offence set out in paragraph 2 d).

§26

(1) Natural person commits offence in the case he/she does not fulfil duty set out in §10 paragraph 1.

(2) The penalty for the offence set out in paragraph 1 is 50 000 CZK.

§ 27

(1) Legal person is not responsible for the administrative offence in case it can prove having made every effort, which was possible to demand, to prevent the breach of the legal obligation.

(2) The responsibility of legal person for an administrative offence ceases to exist if the NSA has not launched the proceedings within 1 year from the day this offence was discovered, but no later than3 years from the day the administrative offence was committed.

(3) While determining the penalty assessment of a legal entity, the gravity of the administrative offence shall be taken into account, especially the way of its committing and the consequences and circumstances of its committing.

(4) Administrative offences set out by this Act shall be debated by the NSA.

(5) Responsibility for actions during the natural person’s entrepreneurship or in direct connection with it is regulated by provisions on responsibilities and legal person’s penalty of this Act.

(6) The penalties shall be collected by the NSA. The income from these penalties shall be public revenue.

(7) The penalty is due 30 days from the day of entering into force of the decision of its imposition.

Chapter VI

Final provisions

§ 28

Enabling provisions

(1) The NSA and the Ministry of Interior shall stipulate important information systems and their determinative criteria according to §6 d) by the implementing legal regulation.

(2) The NSA shall stipulate by the implementing legal regulation the following:

a) Content and structure of the security documentation, content of security measures and extent of security measures according to§6 a) to c),

b) Types and categories of cyber security incidents and requirements and form of cyber security incident report according to 8§ paragraph 4,

c) Requirements on implementation and result of a reactive measure notice according to § 13 paragraph 6,

d) Contact details notice template and its form according to §16 paragraph 6.

Transitional provisions

§ 29

(1) Public authorities and natural and legal persons set out in § 3 a) and b) shall notify contact details according to § 16 within 30 days from entering into force of this Act.

(2) Public authorities and natural and legal persons set out in § 3 b) are obliged to implement duty set out in §8 paragraph 1 and 2no later than 1 year from entering into force of this Act.

§ 30

Public authorities and natural and legal persons set out in § 3 c) and d) are obliged to

a) Notify contact details according to § 16 within 30 days from the day of determination of their information system or communication system as critical information infrastructure,

b) Fulfil duty set out in § 8 paragraph 1 and 3 no later than 1 year from the day of determination of their information system or communication system as critical information infrastructure at the latest and

c) Implement security measures according to § 4 paragraph 2 within 1 year from the day of determination of their information system or communication system as critical information infrastructure.

§ 31

Public authorities and natural and legal persons set out in § 3 e) are obliged to

a) Notify contact details according to § 16 within 30 days from the day of fulfilment of determinative criteria of the important information system,

b) Implement duties set out in § 8 paragraph 1 and 3 no later than 1 year from the day of fulfilment of determinative criteria of the important information system and

c) Implement security measures according to § 4 paragraph 2 within 1 year from the day of fulfilment of determinative criteria of the important information system.

§ 32

Until the time when a public-law contract concluded according to § 19 comes into force, the activity of the National CERT shall be performed by the entity, which carried out activities that are to be carried out by the national CERT according to this Act before this Act entered into force, for no longer than 2 years from the day of entering into force of this Act.

§ 33

Common provisions

(1) This Act refers only to information or communication systems of intelligence services, which fulfil conditions for determination of critical information infrastructure, as set out in § 12 and § 16; the provision § 4 applies to such systems proportionately and the NSA does not propose these as elements of critical infrastructure according to § 22 paragraph 2 m).

(2) This Act applies to information system of the Police of the Czech Republic for analytical activity in penal proceedings only within §12 and §16; the provision § 4 applies to such systems proportionately. This is not valid if this system is critical information infrastructure.

PART TWO

Change of the Act on the Protection of Classified Information and Security Eligibility

§ 34

Act No. 412/2005 Coll., on Protection of Classified Information and Security Eligibility, as amended by Act No. 119/2007 Coll., Act No. 177/2007 Coll., Act No. 296/2007 Coll., Act No. 32/2008 Coll., Act No. 124/2008 Coll., Act No. 126/2008 Coll., Act No. 250/2008 Coll., Act No. 41/2009 Coll., Act No. 227/2009 Coll., Act No. 281/2009 Coll., Act No. 255/2011

Coll., Act No. 420/2011 Coll., Act No. 458/2011 Coll., Act No. 167/2012 Coll. and Act No. 303/2013 Coll., will change in the following way:

1. In § 145 at the end of paragraph 5, a full stop shall be replaced by a comma and letter f) shall be added in the following way:

   „f) Following request notice about respective cyber security incidents from critical information infrastructure."

2. In § 146 paragraph 1, the wording "or within the administrative procedure on issuance of countermeasures according to the Act on Cyber Security" shall be inserted behind the wording "security procedure".

3. In § 146 paragraph 2, the wording "or according to the Act on Cyber Security" shall be inserted behind the wording "according to this Act".

PART THREE

Change of the Electronic Communications Act

§ 35

Act No. 127/2005 Coll., on Electronic Communications and on Amendment to certain related Acts (the Electronic Communications Act), as amended by Act No. 290/2005 Coll., Act No. 361/2005 Coll., Act No. 186/2006 Coll., Act No. 235/2006 Coll., Act No. 310/2006 Coll., Act No. 110/2007 Coll., Act No. 261/2007 Coll., Act No. 304/2007 Coll., Act No. 124/2008 Coll., Act No. 177/2008 Coll., Act No. 189/2008 Coll., Act No. 247/2008 Coll., Act No. 384/2008 Coll., Act No. 227/2009 Coll., Act No. 281/2009 Coll., Act No. 153/2010 Coll., Constitutional Court judgement promulgated under No. 94/2011 Coll., Act No. 137/2011 Coll., Act No. 341/2011 Coll., Act No. 375/2011 Coll., Act No. 420/2011 Coll., Act No. 457/2011 Coll., Act No. 458/2011 Coll., Act No. 468/2011 Coll., Act No. 18/2012 Coll., Act No. 19/2012 Coll., Act No. 142/2012 Coll., Act No. 167/2012 Coll., Act No. 273/2012 Coll., Act No. 214/2013 Coll. and Act No. 303/2013 Sb. will change in the following way:

1. In § 89 paragraph 4 shall be added, including footnote No. 62:

   „(4) Entrepreneur administrating a public communication network or providing publicly accessible electronic communications service is obliged, on the participant's request free of charge and in the form enabling further electronic data processing, to provide operational and localization data, available on the basis of this Act, in case when the participant was not able to collect or save them because of his/her device failure in consequence of a cyber security incident[5].The entrepreneur shall transmit the

[5] § 7 paragraph 2 of the Act No. …/2014 Coll., on Cyber Security and on Amendment to related Acts (Act on Cyber Security)."

data, if technically possible, immediately, however, no later than 3 days from the day of the delivery of the request or in the case of an ongoing communication from the day of its realization.

2. In § 118 paragraph 14 y) the word “or” shall be cancelled.

3. In § 118 at the end of paragraph 14 a full stop shall be replaced by the word “or” and letter ad) shall be added:

„ad) contrary to § 89 paragraph 4 does not provide data or provides them late.”

4. In § 118 paragraph 22 a), the word “or” shall be replaced by a comma and at the end of the text of 22 a) the wording “or of the paragraph 14 letter ad)”shall be added.

PART FOUR

Change of the Act on Freedom of Information

§ 36

In § 11 paragraph 4 of the Act No. 106/1999 Coll., on Freedom of Information, as amended by the Act No. 61/2006 Coll. the full stop at the end of the letter e) shall be replaced by a comma, and the letter f) shall be added as follows:

„f) data kept in the evidence of incidents according to the Act on Cyber security, from which it was possible to identify public authority or person, who announced the security incident or whose providing would endanger efficiency of reactive or protective measure according to the Act on Cyber security.”

PART FIVE

Change of the Act on Radio and Television Broadcasting

§ 37

In § 32 paragraph 1 k) of the Act No. 231/2001 Coll. on Radio and Television Broadcasting and on Amendment to Other Act, as amended by the Act No. 274/2003 Coll., the words “state of cyber emergency” are added behind the words “state of war.”

PART SIX

Entering into force

§ 38

This Act shall enter into force on 1st January 2015.