

**DECREE**

of 7 December 2005

**on the extent of traffic and location data, the time of storage thereof and the form and method of the provision thereof to bodies authorised to use such data**

In accordance with Section 150(3) of Act No. 127/2005 on Electronic Communications and on Amendment to Certain Related Acts (the Electronic Communications Act), as amended in Act No. 290/2005 and Act 361/2005 (hereinafter referred to as the “Act”), the Ministry of Informatics in co-operation with the Ministry of Interior, seeking to implement Section 97(3) of the Act, lays down as follows:

## Section 1

For the purposes of this Decree, the following terms shall have the following meanings:

- a) BTS station means a base transceiver station of the public mobile telephone network;
- b) StartBTS station means the base station of the public mobile telephone network to which the subscriber is allocated when starting a communication;
- c) StopBTS station means the base station of the public mobile telephone network to which the subscriber is allocated when ending a communication;
- d) IMEI number means the International Mobile Equipment Identifier;
- e) MSISDN number means a subscriber number in the public mobile telephone network;
- f) IMSI number means the International Mobile Subscriber Identifier;
- g) Destination means identification of a foreign operator’s network;
- h) URI means the uniform resource identifier;
- i) The code of the juristic or natural person providing a public communication network or publicly accessible electronic communication service means the serial number of the authorisation contained in the businesses register based on Section 14 of the Act.

## Section 2

**Extent of Traffic and Location Data Storage**

(1) The juristic or natural persons providing a public communication network or publicly accessible electronic communication service (“operator“) shall submit the operation and location data defined herein (“data“) to the body authorised to request such submission (“authorised body“).

(2) For switched and fixed-connection electronic communication networks, the following data shall be maintained:

- a) data on the communication that has taken place, indicating the type of communication, the calling party’s and called party’s telephone number or identifier of the telephone card for use in the public pay phones, the communication start date and time, length of the communication and the status of the communication, where applicable;

- b) data on all the public pay phones, including their telephone numbers, registration numbers, geographical coordinates and verbal description of the location.

(3) For public electronic communications mobile telephone networks, the following data shall be maintained:

- a) data on the communication that has taken place, indicating the type of communication, the calling party's and called party's telephone number, the communication start date and time, length of the communication, the IMEI number, StartBTS station number and, where applicable, the StopBTS station, the destination, and additional information;
- b) data on the links between MSISDN numbers and IMEI numbers, jointly used in the network, identification of the BTS station and the IMEI number that made it possible to make a call without a SIM card to the emergency call number "112", the IP addresses of the terminals through which SMSs were sent via the Internet, the date and time of credit recharging for prepaid services, numbers of the recharging coupons in respect of a specific subscriber telephone number, and the subscriber telephone number in respect of a certain recharging coupon;
- c) data on all BTS stations with indication of their numbers, geographical coordinates, antenna azimuth and a verbal description of the location of the BTS station.

(4) For packet-switching electronic communication networks, the data on the communication that has taken place are maintained as follows:

- a) for the network access service – with indication of the type of connection, user account identifier, service user equipment identifier, connection start date and time, connection end date and time, identifiers related to the object of interest (e.g. IP address, port number), event status (success, failure, normal/abnormal end of connection), quantity of transmitted data (incoming / outgoing);
- b) for the mailbox access services – with indication of the equipment identifier of the user who is the object of interest, the user account identifier, e-mail server message identifier, communication start date and time, sender's e-mail address, recipients' e-mail addresses, e-mail protocol identifier, quantity of transmitted data and information about the use of secured communication;
- c) for the e-mail message transmission service – with indication of the equipment identifier of the user who is the object of interest, the e-mail server identifier, communication start date and time, sender's e-mail address, recipients' e-mail addresses, e-mail protocol identifier, quantity of transmitted data and information about the use of secure communication;
- d) for server services – with indication of the equipment identifier of the user who is the object of interest, the user account identifier, service request date and time, all server identifiers (including, but not limited to, the IP address, the fully qualified domain number FQDN), the required URI or service type identifiers, additional parameters of the URI or service identifiers, the services used, the quantity of transmitted data, and the service request method and status;
- e) for other electronic communication services (including, but not limited to, those of the type of chat, usenet, instant messaging and IP telephony) – with indication of all the identifiers of the communicating parties, the transport protocol, communication start date and time, communication end date and time, the service used and quantity of the transmitted data.

### Section 3 Method of Data Transfer

(1) An authorised body may, through its assigned contact workplace, ask the operator to make the stored information available. The operator shall immediately deliver the requested data through its assigned contact workplace. The data referred to in Section 2(3)(c) shall be handed over on a monthly basis in a summarised form up to date as at the handover date.

(2) Communication between the contact workplaces of the operator and the authorised body shall preferably be provided in a manner allowing for remote access. Requests and data shall preferably be delivered in a data file electronic format. Generally available technologies and communication protocols shall only be used in the contact workplaces' communication so as to avoid linking the solution to a specific manufacturer or supplier.

(3) Where it is impossible or unreasonable to use for communication a method allowing for remote access, an application or the requested data can be provided in paper form or in data files on a portable medium.

(4) The following shall be used to prove the authenticity of the request and the data being transferred:

- a) guaranteed electronic signature, based on a qualified certificate issued by an accredited certification service provider<sup>1)</sup>; cryptographic standard format with the PKCS#7 public key shall be used to create and validate the signature;
- b) cover letter in paper form, containing the reference number or serial number of the request, the file name, the date, time and method of hand-over and possibly also the checksum or standard hash of the file (e.g. SHA-1), and signature of an authorised person;
- c) letter in paper form, containing the reference number and signature of an authorised person; or
- d) in the case of requests or data already transferred in an electronic format for a certain period, which as a rule is one week, for which no other authenticity proof has been used: a letter in paper form, which is sent subsequently, containing the reference number and signature of an authorised person.

(5) Data on the communication that took place under a certain identifier for a certain period of time shall be handed over by the operator to the authorised body as:

- a) fixed line communication dump, for data referred to in Section 2(2)(a);
- b) mobile communication dump, for data referred to in Section 2(3a);
- c) data communication dump, for data referred to in Section 2(4).

(6) The communication dumps referred to in Section 5 above shall be handed over to the authorised body in a structured text file, preferably with coding based on the CP-1250, UTF-8 or ISO 8859-2 character set. The files are prepared separately for each single telephone number or any other identifier indicated in the request. The names of the files being transferred are structured on the basis of the name convention given in the Annex.

---

<sup>1)</sup> Section 11 of Act No. 227/2000 on Electronic Signature as amended.

(7) The files have a uniform heading and a fixed structure, determined for the given type of network, or service, or request. The individual lines in the file are arranged chronologically, unless any other arrangement parameter is indicated in the request. The dump referred to in Subsection 5 above ends with the word “Konec” (End) in the last line.

(8) Within the line, the individual data elements are separated by the semicolon (code 0059 of the character set) or tabulator (code 0009 of the character set). The last item terminates with the CRLF character (codes 0013 and 0010 of the character set). If any of the data elements is not required or can be proved not to be identifiable with the technology used, its place in the structure shall be left empty.

(9) For information consisting of more than one data value, the individual values shall be separated by the “|” character (code 0166 of the character set). In the case that a character contained in the information being transferred is the same as any of the above separators, or if there is the character “\”(code 0092 of the character set), it must be prefixed with “\” (for example: “\;”, “\CR\LF”, “\|”).

(10) In justified cases and with the consent of an authorised body and the operator, it is possible to use a file format, structure and name different from the specification in Subsections 6 to 9.

#### Section 4 **Time of Data Storage**

(1) Data shall be stored for 6 months, unless otherwise provided in Subsection 2 below.

(2) Data indicated in Part 3 Points 3.3.4.5 and 3.3.4.6 of the Annex shall be stored for 3 months.

#### Section 5 **Effect**

This Decree shall come into effect as at the date of its promulgation, except Section 4(2) and except Part 3 of the Annex, which shall come into effect as at 1 December 2006.

Minister:  
Ing. **Bérová**

## Form of Data Transfer

### 1 Name Convention and the Structure of the Fixed Line Communication Dump

- 1.1 The name convention sets out the name of the file of the fixed line communication dump in the format of YYYY.txt, where YYYY indicates the request identifier.
- 1.2 Data transferred in a structured text file must be introduced by a header in the first three lines, the first line containing the following data:
  - 1.2.1 communication type requested;
  - 1.2.2 telephone number of the subscriber or the identifier of the telephone card for which the dump is requested;
  - 1.2.3 date and time from which the dump is requested;
  - 1.2.4 date and time until which the dump is requested;
  - 1.2.5 the character set used.The second line is empty and the third line contains the names of the information elements.
- 1.3 The introductory header is followed by lines in the following structure:
  - 1.3.1 call type (including, but not limited to, outgoing, incoming, SS7);
  - 1.3.2 telephone number of the calling party;
  - 1.3.3 telephone number of the called party;
  - 1.3.4 communication start date;
  - 1.3.5 communication start time;
  - 1.3.6 communication length in the format of HHH:MM:SS;
  - 1.3.7 communication status (indicated as a rule in the dump from SS7 signalling).

### 2 Name Convention and the Structure of the Mobile Communication Dump

- 2.1 The name convention sets out the name of the file of the mobile communication dump in the format of YYY...Y\_ZZZ.txt, where YYY...Y corresponds to the subscriber's telephone number or the IMEI number or the IMSI number<sup>2)</sup> or the number of the BTS station forat which the dump is being made. ZZZ is the serial number of the request.
- 2.2 Data transferred in a structured text file must be introduced by a header in the first three lines, the first line containing the following data:
  - 2.2.1 designation of the dump identifier (MSISDN/IMEI/IMSI/BTS);
  - 2.2.2 the MSISDN number, the IMEI number, the IMSI number or the number of the BTS station where the dump is requested;
  - 2.2.3 date and time from which the dump is requested;
  - 2.2.4 date and time until which the dump is requested;
  - 2.2.5 the character set used.

---

<sup>2)</sup> Recommendation ETSI EN 300 927.

The second line is empty and the third line contains the names of the information elements.

2.3 The introductory heading is followed by lines in the following structure:

- 2.3.1 communication type (including, but not limited to, outgoing call, incoming call, outgoing SMS message, incoming SMS message);
- 2.3.2 telephone number of the calling party;
- 2.3.3 telephone number of the called party;
- 2.3.4 communication start date and time in the format DD.MM.RRRR HH:MM:SS (“R” being “year”);
- 2.3.5 length of communication (call time in seconds);
- 2.3.6 IMEI number of the mobile telephone set of the object of interest;
- 2.3.7 number of the StartBTS station;
- 2.3.8 number of the StopBTS station;
- 2.3.9 destination;
- 2.3.10 additional information (setting additional services).

### **3 Name Convention and the Structure of the Data Communication Dump**

3.1 The name convention sets out the name of the file of the data communication dump in the format of XXX\_RRMMDD\_ZZZZ.txt, where XXX is the operator code; RRMMDD is the date of hand-over of the dump in the format of year (“R” being “year”), month, day; and ZZZZ is the numerical identifier of the request.

3.2 Data transferred in a structured text file must be introduced by a header in the first three lines, the first line containing the following data:

- 3.2.1 name of the dump file;
- 3.2.2 dump type (service used);
- 3.2.3 identifier, for which the dump is requested (for example, IP address, the subscriber’s telephone number, e-mail address);
- 3.2.4 date and time from which the dump is requested;
- 3.2.5 date and time until which the dump is requested;
- 3.2.6 character set used;
- 3.2.7 identification of the time zone, related to the zero meridian in the format of GMT ± HH:MM).

The second line is empty and the third line contains the names of the information elements.

3.3 The introductory heading is followed by information in the sequence indicated in the heading:

- 3.3.1 Access to the network
  - 3.3.1.1 access connection type (including, but not limited to, dial-up, ADSL, GPRS, cable modem, LAN);
  - 3.3.1.2 user account identifier;
  - 3.3.1.3 service user equipment identifier (including, but not limited to, the MAC, the subscriber’s telephone number, for the dial-up access connection);
  - 3.3.1.4 access connection start date and time;
  - 3.3.1.5 access connection end date and time;

- 3.3.1.6 identifiers related to the object of interest (including, but not limited to, IP address, and – if the IP address does not provide clear identification of the terminal equipment – also the number of the port, for example, PAT);
  - 3.3.1.7 event status;
  - 3.3.1.8 quantity of transmitted data in kilobytes [kB].
- 3.3.2 Access to mailboxes
- 3.3.2.1 user equipment identifier of the object of interest (including, but not limited to, the IP address and port number);
  - 3.3.2.2 user account identifier;
  - 3.3.2.3 identifier of the message on the mail server (ID Message);
  - 3.3.2.4 communication start date and time;
  - 3.3.2.5 sender's e-mail address;
  - 3.3.2.6 recipients' e-mail addresses;
  - 3.3.2.7 e-mail protocol identifier (e.g. POP3, IMAP);
  - 3.3.2.8 quantity of transmitted data in kilobytes [kB];
  - 3.3.2.9 use of secured communication (Yes – No; and also the way of use of secured communication, if appropriate).
- 3.3.3 Electronic mail message transmission
- 3.3.3.1 user equipment identifier of the object of interest (including, but not limited to, the IP address and port number);
  - 3.3.3.2 identifier of the server for electronic mail message transmission;
  - 3.3.3.3 communication start date and time;
  - 3.3.3.4 sender's e-mail address;
  - 3.3.3.5 recipients' e-mail addresses;
  - 3.3.3.6 identifier of the electronic mail protocol;
  - 3.3.3.7 quantity of transmitted data in kilobytes [kB];
  - 3.3.3.8 use of secured communication (Yes – No; and also the way of use of secured communication, if appropriate).
- 3.3.4 Server services
- 3.3.4.1 user equipment identifier of the object of interest;
  - 3.3.4.2 user account identifier;
  - 3.3.4.3 date and time of the request for service;
  - 3.3.4.4 server identifiers;
  - 3.3.4.5 requested URI identifier or any other service identifier;
  - 3.3.4.6 URI or service identifier parameters;
  - 3.3.4.7 The service used (for example, ftp, http);
  - 3.3.4.8 quantity of transmitted data in kilobytes [kB];
  - 3.3.4.9 request method (for example, POST, GET, DEL);
  - 3.3.4.10 request status (for example, success, failure, time-out, status code).
- 3.3.5 Other electronic communication services (including, but not limited to, services of the type of chat, usenet, instant messaging and IP telephony)
- 3.3.5.1 identifier of the object of interest;
  - 3.3.5.2 source equipment identifier (for example, IP address and port number);
  - 3.3.5.3 target equipment identifier (for example, IP address and port number);
  - 3.3.5.4 transport protocol;

- 3.3.5.5 communication start date and time;
- 3.3.5.6 communication end date and time;
- 3.3.5.7 services used;
- 3.3.5.8 quantity of transmitted data in kilobytes [kB].