CONSTITUTIONAL COURT

G 47/12-11
G 59/12-10
G 62,70,71/12-11
28 November 2012

DECISION

The Constitutional Court, chaired by President
Gerhart HOLZINGER,

in the presence of Vice-President
Brigitte BIERLEIN

and its members
Sieglinde GAHLEITNER,
Christoph GRABENWARTER,
Christoph HERBST,
Michael HOLOUBEK,
Helmut HÖRTENHUBER,
Claudia KAHR,
Georg LIENBACHER,
Rudolf MÜLLER,
Hans Georg RUPPE,
Johannes SCHNIZER, and
Ingrid SIESS-SCHERZ

as voting members, in the presence of the recording clerk
Gernot FRIEDL

has decided on the applications filed by

1. the GOVERNMENT OF THE PROVINCE OF CARINTHIA,

2. Michael S., (...) , 1030 Vienna, represented by Cabjolsky & Otto Rechtsanwälte OG, Biberstrasse 3, 1010 Vienna, and

3. Christof T., (...) , 1160 Vienna, Andreas K., (...) , 1070 Vienna, Albert S., (...), 1070 Vienna, Jana H., (...) , 1080 Vienna, Sigrid M., (...) , 1030 Vienna, Erich SCH., (...) , 1130 Vienna, Hannes T., (...) , 1030 Vienna, SCH. Rechtsanwalt GmbH, (...) , 1070 Vienna, Maria W.-T., (...) , 1130 Vienna, Philipp SCH., (...) , 2500 Baden, Stefan P., (...) , 1010 Vienna, and others, all represented by Scheucher Rechtsanwalt GmbH, Lindengasse 39, 1070 Vienna, firstly to repeal provisions of the Telecommunications Act ("*Telekommunikationsgesetz*") as amended by Federal Law Gazette *BGBl*. I 27/2011, and secondly and thirdly to also repeal provisions of the Code of Criminal Procedure ("*Strafprozessordnung*") as amended by Federal Law Gazette *BGBl*. I 33/2011 and of the Security Police Act ("*Sicherheitspolizeigesetz*") as amended by Federal Law Gazette *BGBl*. I 33/2011 in today's *in camera* meeting as follows:

I. The following questions are submitted to the Court of Justice of the European Union for a preliminary ruling according to Article 267 TFEU:

1. On the validity of acts of Union bodies:

"Are Articles 3 to 9 of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC compatible with Articles 7, 8 and 11 of the European Union Charter of Fundamental Rights?

2. On the interpretation of the Treaties:

2.1. In order to assess the permissibility of interferences, are Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data to be considered on an equal footing with the provisions of Article 8(2) and Article 52(1) of the Charter, in the light of the explanations on Article 8 of the Charter – drafted pursuant to Article 52(7) of the Charter as guidance on the interpretation of the Charter – which must be duly considered by the Constitutional Court?

2.2. What is the relation between "Union law" referred to in Article 52(3) last sentence of the Charter and the data protection Directives?

2.3. Given that Directive 95/46/EC and Regulation (EC) No 45/2001 lay down conditions and limitations on exercising the right to data protection set out in the Charter, should changes arising from later secondary law be considered when interpreting Article 8 of the Charter?

2.4. In consideration of Article 52(4) of the Charter, does the principle of providing more extensive protection laid down in Article 53 of the Charter in consequence mean that the relevant limits for permissible restrictions by secondary law should be drawn narrower?

2.5. In view of Article 52(3) of the Charter, paragraph 5 of the Preamble, and of the explanations on Article 7 of the Charter, according to which the rights they guarantee are the same as those laid down in Article 8 ECHR, is it possible that the case law of the European Court of Human Rights on Article

8 ECHR results in positions on the interpretation of Article 8 of the Charter which may influence the interpretation of the said Article?

II. The judicial review proceedings will be continued as soon as the Court of Justice of the European Union has handed down its ruling.

Reasoning

I.

1. According to its Article 1(1), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter referred to as Data Retention Directive) aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which is generated or processed by them, in order to ensure that the data is available for the purpose of the investigation, identification and prosecution of serious criminal acts, as defined by the national laws of each Member State. According to Article 1(2) of the Data Retention Directive, it shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications. Data is to be retained for periods of not less than six months and not more than two years from the date of the communication.

2. In its original version already, the federal law by which the Telecommunications Act was enacted (*Telekommunikationsgesetz 2003, TKG 2003*) contained provisions obliging telecommunications network operators to store certain data. The Data Retention Directive was transposed by the amendment Federal Law Gazette *BGBl*. I 27/2011, and the storage obligations were extended by a newly inserted section 102(a) *TKG* 2003 (see II.2. below).

This amendment entered into force on 1 April 2012, the implementation reference is contained in section 1 paragraph 4 subparagraph 5 *TKG* 2003.

3. Basing itself on its decision of 27 March 2012, the government of the Province of Carinthia (hereinafter: applicant province government) filed an application with the Constitutional Court on 6 April 2012 pursuant to Article 140 paragraph 1 of the Constitution (*Bundes-Verfassungsgesetz, B-VG*) seeking the annulment of explicitly listed provisions of the *TKG* 2003 (G 47/12), *inter alia* of section 102(a), which was inserted by the amendment Federal Law Gazette *BGBl*. I 27/2011.

4. On 25 May 2012 Michael S., an employee of (...), filed an application pursuant to Article 140 paragraph 1 of the Constitution, claiming that his rights were directly infringed i.a. by the unconstitutionality of section 102(a) *TKG* 2003. He maintained that he had four subscriber lines which he used for business as well as private purposes for voice telephony and internet access including email services. The challenged provision would require the operator of his communications network to store specified data of the applicant without cause, irrespective of technical requirements or billing purposes, and regardless of, or even against, his will. The applicant considered this *inter alia* a violation of Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter of Fundamental Rights).

5. Another application pursuant to Article 140 of the Constitution was received by the Constitutional Court on 15 June 2012, in which the applicants – 11,130 in total – equally maintained a direct infringement of their rights invoking the unconstitutionality of the data storage obligation laid down in section 102(a) *TKG* 2003, since all applicants had subscribed to (at least) one or several services enumerated in section 102(a) paragraphs 2 to 4 *TKG* 2003, and were therefore subject to data storage with their subscriber data (master data) in correlation with the respective traffic data. The applicants in these proceedings equally consider the storage of their data without any concrete suspicion or cause i.a. a violation of Article 8 of the Charter of Fundamental Rights.

II.

The relevant legislation is as follows:

1. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC reads as follows:

Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive

(a) ‘data’ means traffic data and location data and the related data necessary to identify the subscriber or user;

(b) ’user’ means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) ’telephone service’ means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) ’user ID’ means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) ’cell ID’ means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) ’unsuccessful call attempt’ means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly

available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;
(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and
(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10

Statistics

1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

- the cases in which information was provided to the competent authorities in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
- the cases where requests for data could not be met.

2. Such statistics shall not contain personal data

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks to be retained for the purposes referred to in Article 1 (1) of that Directive.

Article 12

Future measures

1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

3. Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14

Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007.

They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the Official Journal of the European Union.

Article 16

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 17

Addressees

This Directive is addressed to the Member States.

3. Section 102(a) of the Telecommunications Act 2003*, TKG* 2003*,* which obliges providers of public communication services to store explicitly listed data, reads as follows:

"Data retention

Section 102(a). (1) Beyond the authorisation to store or process data pursuant to sections 96, 97, 99, 101 and 102, providers of public communications services shall store data in accordance with paragraphs 2 to 4 from the time of generation or processing until six months after the communication is terminated. The data shall be stored solely for the purpose of investigating, identifying and prosecuting criminal acts whose severity justifies an order pursuant to section 135 paragraph 2(a) Code of Criminal Procedure.

(2) Providers of internet access services are obliged to store the following data:
1. the name, address and identifier of the subscriber to whom a public IP address was assigned at a given point in time, including an indication of the underlying time zone;
2. the date and time of the assignment and revocation of a public IP address for an Internet access service, including an indication of the underlying time zone;
3. the calling telephone number for dial-up access;
4. the unique identifier of the line over which Internet access was established.

(3) Providers of public telephone services, including Internet telephone services, are required to store the following data:
1. the subscriber number or other identifier for the calling line and the line called;
2. for additional services such as call forwarding or call diverting, the subscriber number to which the call is forwarded/diverted;
3. the name and address of the calling subscriber and of the called subscriber;
4. the start date and time as well as the duration of communication, with an indication of the underlying time zone;
5. the type of service used (calls, additional services, messaging and multimedia services).
6. in the case of mobile networks, the following additional data is to be stored:
a) the international mobile subscriber identity (IMSI) of the calling line and the

line called;
b) the international mobile equipment identity (IMEI) of the calling line and the line called;
c) in the case of anonymous prepaid services, the date and time of the initial activation of the service and the cell ID at which the service was activated;
d) the location label (cell ID) at the start of the communication;

(4) Providers of e-mail services are obliged to store the following data:
1. the identifier assigned to a subscriber;
2. the name and address of the subscriber to whom an e-mail address was assigned at a given point in time;
3. when an e-mail is sent, the e-mail address and the public IP address of the sender as well as the e-mail address of each recipient of the e-mail;
4. when an e-mail is received and delivered to an electronic mailbox, the e-mail address of the message sender and recipient as well as the public IP address of the last communications network facility involved in the transmission;
5. when a user logs in and out of an e-mail service, the date, time, identifier and public IP address of the subscriber, including an indication of the underlying time zone.

(5) The storage obligation pursuant to paragraph 1 applies only to those data pursuant to paragraphs 2 to 4 which are generated or processed in the course of providing the relevant communications services. In connection with unsuccessful call attempts, the storage obligation pursuant to paragraph 1 only applies to the extent that these data are generated or processed and stored or logged in the course of providing the relevant communications service.

(6) The storage obligation pursuant to paragraph 1 does not apply to those providers whose undertakings are exempt from the financing contribution requirement pursuant to section 34 *KommAustria Act*.

(7) The content of communications and in particular data on addresses retrieved on the Internet is not to be stored on the basis of this provision.

(8) Without prejudice to section 99 paragraph 2, once the retention period has ended, the data to be stored pursuant to paragraph 1 are to be deleted without delay, at the latest within one month after the end of the retention period. The provision of information after the end of the retention period shall not be permissible.

(9) With regard to retained data transmitted in accordance with section 102(b), the claims to information on this use of data shall be based solely on the provisions of the Code of Criminal Procedure".

Pursuant to section 102(b) *TKG* 2003, information on retained data may be provided solely on the basis of a court-approved order from the public prosecutor's office for the investigation and prosecution of criminal acts whose severity justifies an order pursuant to section 135 paragraph 2(a) of the Code of Criminal Procedure 1975 (admissibility of providing information on retained data at specified conditions if the provision of such information is likely to help the investigation of a wilfully committed criminal act for which the sentence is more than six months or more than one year, or if it can be expected based on given facts that the whereabouts of a fugitive or absent accused who is strongly suspected of having wilfully committed a criminal act which carries a sentence of more than one year can be established). The data is to be stored in such a way that it can be transmitted without delay to the authorities competent to provide information on communications data pursuant to the Code of Criminal Procedure. The data is to be provided in an "appropriately protected form" via the technical means to be provided for according to section 94 paragraph 4 *TKG* 2003.

Section 102(c) *TKG* 2003 contains provisions on data security, logging and statistics. For instance, appropriate technical and organisational measures shall be taken to ensure that retained data can be accessed only by authorised persons with due adherence to the principle of dual control. Logs on every request for, or information provided on, retained data, which have to be kept by providers under a data retention obligation, must be stored for a period of three years after the end of the retention period for the respective retained data item. The Austrian Data Protection Commission shall be responsible for monitoring compliance with these provisions.

Section 109 paragraphs 22 to 26 *TKG* 2003 contains administrative penal regulations according to which any person violating the provisions of sections 102(a) to 102(c) of the above Act shall be guilty of an administrative offence and shall be punished by a fine of up to EUR 37,000.

4. Section 135 of the Code of Criminal Procedure (*Strafprozessordnung, StPO)* Federal Law Gazette, *BGBl*. 631/1975 as amended by Federal Law Gazette *BGBl*. I 33/2011, reads as follows:

"Seizure of letters, information on communication data, information on retained data, and surveillance of communications

Section 135. (1) The seizure of letters shall be admissible if necessary to investigate a wilfully committed criminal act which carries a sentence of more than one year and if the accused has been detained for such an act or his arraignment or arrest has been ordered for such reason.

(2) The provision of information on communication data shall be admissible,

1. if and as long as there is a strong suspicion that a person affected by such information has kidnapped or in any other way taken possession of another person, and if the provision of data is limited to communications which are expected to be transmitted, sent or received by the accused during the time such deprivation of liberty is taking place,
2. if the provision of such information is expected to help investigate a wilfully committed criminal act carrying a sentence of more than six months and the owner of the technical device which was or will be the source or target of data communication explicitly consents to such information being provided, or
3. if the provision of such information is expected to help investigate a wilfully committed criminal act carrying a sentence of more than one year and it can be assumed based on given facts that the provision of such information will allow to ascertain the data about the accused;
4. if, based on given facts, it is to be expected that the whereabouts of a fugitive or absent accused who is strongly suspected of having wilfully committed a criminal act which carries a sentence of more than one year can be established.

(2a) The provision of information on retained data (sections 102(a) and 102(b) *TKG*) shall be admissible in the cases enumerated in paragraph 2, subparagraphs 2 to 4.

(3) Surveillance of communications shall be admissible,

1. in the cases of paragraph 2 subparagraph 1

2. in the cases of paragraph 2 subparagraph 2 if the owner of the technical device which was or will be the source or target of communications agrees to such surveillance,
3. if such surveillance appears necessary to investigate a wilfully committed criminal act which carries a sentence of more than one year or if the investigation or prevention of punishable criminal acts that have been committed or planned within the framework of a criminal or terrorist association or criminal organisation (sections 278 to 278(b) Criminal Code *[Strafgesetzbuch*, *StGB]*) would otherwise be severely impeded, and
   a) if the owner of the technical device which was or will be the source or target of data communications is strongly suspected of having committed a criminal act which carries a sentence of more than one year, or of a criminal act pursuant to sections 278 to 278(b) Criminal Code, or
   b) if it can be assumed based on given facts that the person strongly suspected of having committed a criminal act (letter a) will use the technical device or establish a connection with such device;

4. in the cases of paragraph 2 subparagraph 4."

5. Having constitutional status, section 1 of the Federal Act on the Protection of Personal Data (Data Protection Act 2000 [*Datenschutzgesetz*, *DSG* 2000]), Federal Law Gazette *BGBl*. I 165/1999 as amended by Federal Law Gazette *BGBl*. I 112/2011, reads as follows:

"(Constitutional Provision)

Fundamental Right to Data Protection

Section 1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject.

(2) Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Article 8(2) of the European

Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions the interference with the fundamental right shall be carried out using only the least intrusive of all effective methods.

(3) Everybody shall have, insofar as personal data concerning him are destined for automated processing or manual processing, i.e. in filing systems without automated processing, as provided for by law,

1. the right to obtain information as to who processes what data concerning him, where the data originated, for which purpose they are used, as well as to whom the data are transmitted;
2. the right to rectification of incorrect data and the right to erasure of illegally processed data.

(4) Restrictions of the rights according to paragraph 3 are only permitted under the conditions laid out in paragraph 2.

(5) The fundamental right to data protection, except the right to information, shall be asserted before the civil courts against organisations that are established according to private law, as long as they do not act in execution of laws. In all other cases the Data Protection Commission shall be competent to render the decision, unless an act of Parliament or a judicial decision is concerned."

III.

1. In the applications pending with the Constitutional Court it is maintained on different grounds not only that section 102(a) *TKG* 2003 violates the fundamental right to data protection (section 1 paragraph 1 *DSG* 2000, Article 8 ECHR, Article 8 Charter of Fundamental Rights), but also that the Data Retention Directive violates Article 8 of the Charter of Fundamental Rights. While the applicant province government claims that the Data Retention Directive is incompatible with Article 8 of the Charter of Fundamental Rights, the applicant in the proceedings case no. G 59/12 complains that the Data Retention Directive as such is in violation of Articles 7, 8, 11 and 20 of the Charter of Fundamental Rights.

1.1. Application G 47/12:

In the view of the applicant province government, the provisions of the *TKG* 2003 enacted to implement the Data Retention Directive concerning the storage of communication data irrespective of any suspicion constitute a massive interference with explicitly stated fundamental rights. The applicant province government holds in particular that the generalised storage of all traffic and location data while knowing the addressees, the frequency and the time of contacts in many cases allows inferring the contents of communications and that knowing that the data will be logged suffices to alter communication behaviour. Moreover, given the unreliable validity of the information deduced from the data and easy circumvention (e.g. by the use of prepaid cards for mobile telephones), and in light of the purpose of investigating, identifying and prosecuting serious criminal acts which the Data Retention Directive is aimed at, these provisions are – as is maintained – largely unsuitable and the inference with fundamental rights is therefore disproportionate. The applicant province government moreover claims a violation of Article 8 of the Charter of Fundamental Rights. Especially from its wording it would result that every individual enjoys a right to data protection also vis-à-vis the European Union. As regards the principle of proportionality, it is being complained that neither investigations as to the need for, nor on the likely success of, such a measure in terms of investigating, identifying and prosecuting serious criminal acts were carried out neither before nor when the Data Retention Directive was adopted.

1.2. Application G 59/12:

In the individual application G 59/12 it is equally maintained that the obligation to store data allows to draw inferences on the behaviour, habits and whereabouts of the users of communications services and therefore to draw up “movement profiles“. The applicant complains that according to the Data Retention Directive operators of non-public communications services and networks (such as corporate networks) are not subject to the obligation of storing data and that it is – still – possible for operators of public internet access services to allow for an anonymous use of their services and that operators of public telephone services are able to offer prepaid cards without having to record user data. The applicant maintains that the Data Retention Directive is

unlawful because it violates Articles 7, 8, 11 and 20 of the Charter of Fundamental Rights and does not have any direct legal effects, respectively, hence the Austrian legislator is not under an obligation to implement the Directive and a primacy of application of these rules over Austrian constitutional law is not to be assumed. The applicant is therefore suggesting that the Constitutional Court bring the issue before the Court of Justice of the European Union seeking a preliminary ruling according to Article 267 TFEU, asking whether the Data Retention Directive is valid.

5.2. Application G 62, 70, 71/12:

The applicants first point out that personal data has already been recorded and processed at various instances under Austrian law to date, but that this data was generally used in individual cases to investigate and prosecute committed crimes, to perform a contract, or to furnish various general-interest services to society. The implementation of the Data Retention Directive, on the other hand, would provide for preventive data recording and processing in order to investigate, identify and prosecute criminal acts without concrete suspicion. In essence, the applicants argue, this constitutes a "change of paradigm that cannot be justified in the light of fundamental rights". The applicants in case no G 62, 70, 71/12 maintain that they are directly affected by the implementation of the Data Retention Directive through the loss of the "feeling to be able to live in a free, self-determined and unobserved manner and of not being bothered if and when, to the extent and as long as they adhered to and complied with the laws of the state and did not become delinquent". The applicants invoke i.a. a violation of Articles 7 and 8 of the Charter of Fundamental Rights, as well as of section 1 *DSG* 2000, which they mainly justify by reference to the case law handed down by the European Court of Human Rights on Article 8 ECHR. In the opinion of the applicants, the interference brought about by the obligation to store data is disproportionate, especially given a lack of legal remedies.

III.

The Constitutional Court has considered the applications which have been joined for deliberation applying section 187 of the Code of Civil Procedure in

combination with section 35 of the Constitutional Court Act *(Verfassungs-gerichtshofgesetz, VfGG*) *mutatis mutandis*:

1. The Constitutional Court has jurisdiction to decide on the applications for judicial review which have been filed.

Pursuant to Article 140 paragraph 1, second and fourth sentence, of the Constitution *(Bundes-Verfassungsgesetz, B-VG*), the Constitutional Court shall decide on the unconstitutionality of a federal act i.a. on application of a province government or of an individual claiming that his or her rights are directly infringed by this unconstitutionality (individual application), if the act entered into effect without a court judgment having been rendered, or without an official administrative notice (*Bescheid*) having been issued in respect of that person.

1.1. For the purpose of judicial review proceedings, the Constitutional Court will provisionally presume that the application by the government of the province of Carinthia file no. G 47/12 and the individual applications files no. G 59/12 and G 62, 70, 71/12 are admissible.

1.2. According to the Constitutional Court‘s case law, the rights guaranteed by the Charter of Fundamental Rights constitute a standard of review in judicial review proceedings within the scope of application of the Charter of Fundamental Rights (Article 51(1) Charter of Fundamental Rights), in particular in proceedings according to Article 139 and 140 of the Constitution. This shall apply in any case when the said guarantee in the Charter of Fundamental Rights is equivalent in terms of wording and determination to constitutionally guaranteed rights laid down in the Austrian Federal Constitution (*cf. VfGH 14.3.2012, U 466/11 et al.)*.

In keeping with established procedure (*cf. VfSlg. 15.450/1999, 16.050/2000, 16.100/2001*), the Constitutional Court will bring a matter before the Court of Justice of the European Union for a preliminary ruling if it has doubts on the interpretation of a provision of Union law, i.e. including the Charter of Fundamental Rights, or if it has doubts on the validity of a provision of secondary law.

Hence, the Constitutional Court is under an obligation to bring such matter before the Court of Justice of the European Union under the terms of Article 267(3) TFEU (*cf. VfGH 14.3.2012, U 466/11 et al*.) not only as regards the interpretation of the Charter of Fundamental Rights, but also when the question of conformity of secondary law with the Charter of Fundamental Rights and hence the validity of secondary law is raised in pending proceedings.

2. The Constitutional Court has been led both by doubts on the interpretation of the Charter of Fundamental Rights and by concerns on the validity of Directive 2006/24/EC on data retention to submit a request for a preliminary ruling to the Court of Justice of the European Union.

3. For a request for a preliminary ruling to be admissible according to Article 267 TFEU, the requesting court must consider the ruling on validity necessary, i.e. relevant for its own decision. The requesting court shall decide thereon within its own discretion. *(ECJ 27/06/1991, C-348/89, Mecanarte [1991], I-3277 [para. 47]).*

Both the question as to the validity of the Data Retention Directive and the questions on the interpretation of Article 8 of the Charter of Fundamental Rights are relevant for the decision.

3.1. Section 102(a) *TKG* 2003 was enacted in implementation of the Data Retention Directive as is shown in the implementation reference and the legislative materials. In essence, this legislative provision fully transposes the contents of the Directive. Implementing Article 3 of the Data Retention Directive, section 102(a) paragraph 1 of the above act lays down a general obligation to store data and, basing itself on the minimum period contained in Article 6 of the Data Retention Directive, provides for a retention period of six months. Implementing Article 5 of the Data Retention Directive, paragraphs 2 and 3 define the category of data to be stored.

In the Austrian legal order, this provision meets with specific constitutional requirements. Federal constitutional law separately lays down a fundamental right to data protection that is independent of Article 8 ECHR. The constitutional provision laid down in section 1 *DSG* 2000 grants every natural and legal person a right to secrecy of the personal data concerning them, provided there is an

interest meriting such protection (section 1 paragraph 1 *DSG* 2000, see II.4. above).

Section 1 paragraph 2 *DSG* 2000 contains a statutory reservation which draws the limits for interference with the fundamental right narrower than Article 8(2) ECHR. Apart from personal data being used in the vital interest of the person concerned or with his or her consent, restrictions to the right to secrecy are admissible only to safeguard an overwhelmingly justified interest of another person, and in the case of interferences by state authorities only on the basis of the law, if necessary for the reasons set out in Article 8(2) ECHR.

For any such interference to be deemed based on the law, section 1 paragraph 2 *DSG* 2000 stipulates, going beyond Article 8(2) ECHR, that the use of data which, by its nature, deserves specific protection shall be allowed only to safeguard substantial public interests and that suitable safeguards for the protection of the data subjects' interest in secrecy are to be concurrently provided for by law. This provision explicitly stipulates that, even in the case of permitted restrictions, any interference with the fundamental right shall be carried out using only the "least intrusive of all effective methods". Based on the Constitutional Court's case law it follows from this provision that a stricter measure must be applied to the proportionality of the interference with the fundamental right to data protection than results from Article 8 ECHR *(VfSlg. 16.369/2001, 18.643/2008).*

3.2. The applications challenge the proportionality of the obligation to store data for at least six months set out in the Data Retention Directive in the light of Article 8 of the Charter of Fundamental Rights.

Should these reservations against the obligation to store data in itself be found pertinent, Union law would require the implementation of a directive which, being part of secondary law, takes precedence (also) over constitutional law *(VfSlg. 15.427/1999*) and hence over the fundamental right according to section 1 *DSG* 2000, provided the Austrian legislator had no other possibility than to implement the Directive in a manner that violates such fundamental right. Since, in such a case, the legislator would not have any leeway to implement the Directive in conformity with the Constitution, the Constitutional Court would be barred from reviewing section 102(a) *TKG* 2003 using section 1 *DSG* 2000 as a

standard of review, given the primacy of the Directive over the nationally implemented fundamental right to data protection.

3.3. And even the substance of the fundamental right laid down in Article 8 of the Charter of Fundamental Rights, which also falls under the Constitutional Court's standard of review, depends not only on the content of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, but also on the validity of the Data Retention Directive inasmuch as the Directive is itself a factor in determining, under the terms of Article 52(3), last sentence, Charter of Fundamental Rights, whether Union law affords more extensive protection which would have to be considered when defining the relevance and scope of the fundamental right to data protection. It does not require further justification that the answer to the questions of interpretation on Article 8 Charter of Fundamental Rights directly affects the decision of the Constitutional Court.

3.4. The conformity of the Directive with the Charter of Fundamental Rights and the questions on the interpretation of Article 8 Charter of Fundamental Rights have not yet been resolved by the case law of the Court of Justice of the European Union. The latter was already called upon to rule on the validity of the Data Retention Directive. That complaint, however, related only to the choice of the legal basis, and not to a possible violation of fundamental rights in connection with the Data Retention Directive (*ECJ 10/02/2009, case C-301/06, Ireland/European Parliament and Council, [2009], I-00593*).

4. The following considerations have led the Constitutional Court to bring a request for a preliminary ruling before the Court of Justice of the European Union:

4.1. According to Article 8(1) Charter of Fundamental Rights, every person has a right to their personal data being protected. According to Article 8(2) of the Charter, such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Inasmuch as the Charter of Fundamental Rights contains rights which correspond with the rights

guaranteed in the ECHR, their meaning and scope shall be the same as those laid down by the said Convention pursuant to Article 52(3) of the Charter of Fundamental Rights.

The Constitutional Court does not fail to recognise the importance and weight of the goal of harmonising the duties of service providers and network operators regarding the retention of defined data and ensuring the availability of this data for the purpose of investigating, identifying and prosecuting serious criminal acts, which the Data Retention Directive aims at. Moreover, the Constitutional Court draws attention to the fact that Article 4 of the Data Retention Directive requires Member States to define the procedures to be followed and the conditions to be fulfilled in due consideration of i.a. the ECHR.

4.2. This notwithstanding, concerns prevail regarding the retention of data without cause as such and the related consequences. The applicants' concerns are largely based on the high degree of interference of data retention, and that for several reasons. First, the Directive sets out a retention period ranging from six months to two years. This timeframe is to be assessed in consideration of the data volume to be stored. It is the preliminary view of the Constitutional Court that this retention period gives rise to serious concerns.

4.3. Second, the scope of data retention raises concerns as to its conformity with the Charter of Fundamental Rights. The Directive allows for the large-scale collection of data in terms of the *category of data*, even though there is a limitation by a catalogue of traffic data, the non-limited *group of persons,* and in terms of the state *tasks* for which it is ordered. The "spread" of the interference goes beyond that of interferences with the fundamental right to data protection which the Constitutional Court had to rule on in its case law to date, whereby the possibility of interlinking data recorded in different contexts must also be taken into account *(Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, Gutachten, 18. Österreichischer Juristentag, 2012, 76 and 111 et seq.).*

4.4. Moreover, data retention almost exclusively affects persons who do not give cause for their data being stored. At the same time, they will necessarily be subject to a higher risk, regardless of any concrete modalities of data use defined

in national law, namely that the authorities will record their data, become aware of their content, inform themselves of the private behaviour of such persons and then further use this data for other purposes (e.g. as a consequence of an accidental presence in a given radio cell at a given moment that is relevant for official investigations).

4.5. In addition, there is a heightened risk of *abuse*. Here, one should note in particular that the obligation to store personal data set out in the Data Retention Directive – and such also in section 102(a) *TKG* 2003 that was enacted in implementation of the Data Retention Directive – goes beyond the former permission to store traffic data for billing retail or wholesale charges. Given the multitude of telecommunications services providers which exist and, as a consequence, the large number of those obliged to store data, an incalculable group of persons has access to traffic data which must be retained for at least six months according to the Data Retention Directive. Regardless of efforts undertaken by the national legislator, preventing abuse is likely to reach "structural limits", since smaller providers would also have to be included which, if only for their small size, have a limited capacity to prevent abuse *(explicitly BVerfG, 2.3.2010, 1 BvR 256/08 et al., paragraph 212).*

The related interference appears disproportionate, not least because of prevailing doubts as to its suitability for reaching the intended purpose.

5. Induced by the main proceedings, the Constitutional Court also had to refer questions on the interpretation of Article 8 of the Charter of Fundamental Rights to the Court of Justice of the European Union (*cf. VfGH 14.3.2012, U 466/12 et al*.). These concern the relation of the fundamental right to Union law including secondary law, to the ECHR, and to the constitutions of the Member States.

5.1. Article 52(7) of the Charter of Fundamental Rights stipulates that the Union courts must also consider the explanations. The explanations on Article 8 Charter of Fundamental Rights state that it is based on Article 286 EC-Treaty and on Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, on Article 8 ECHR, and on the Convention of the Council of Europe of 28 January 1981 for the Protection of Individuals with regard to

Automatic Processing of Personal Data, which was ratified by all member states, and that Article 286 EC-Treaty was replaced by Article 16 TFEU and by Article 39 TEU. Moreover, there is a reference to Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data. The Directive and the Regulation set forth conditions and limitations for exercising the right to the protection of personal data (c.f. Explanations Relating to the Charter of Fundamental Rights, OJ 2007 C 303, 20).

It is not obvious to the Constitutional Court what the relation between the secondary law that is explicitly referred to in the explanations and the limitations set out in Article 8(2) and in Article 52(1) and (3) of the Charter of Fundamental Rights (question 2.1.) and Directives in the same field of regulation is (questions 2.2. and 2.3.).

5.2. Similar to the constitutions of other Member States, Austrian Federal Constitutional Law contains a separate provision that guarantees the fundamental right of data protection in section 1 *DSG* 2000. According to Article 53 of the Charter of Fundamental Rights, the constitutions of the Member States determine, amongst others, the level of protection under the Charter of Fundamental Rights. Question 2.4. is to clarify whether these rights take precedence over the limitations that result from the Charter of Fundamental Rights itself in the event that they afford more extensive protection than Article 8 of the Charter of Fundamental Rights when assessing actions of Member States in implementing Union law and the validity of secondary law, respectively. The Constitutional Court presumes in the scope of application of the Charter of Fundamental Rights that, while no one single fundamental right in the constitution of one individual Member State can set the standard and remove the unlimited applicability of the fundamental right enshrined in the Charter (*cf. SA Bot, 02/10/2012, case C-399/11, Melloni, paragraph 96 et seq.*), if a comparative legal study of the constitutions of the Member States revealed that they provided a more extensive protection than that of the Charter of Fundamental Rights, such fact may well be relevant and compel Union courts to interpret the said guarantee as laid down in the Charter of Fundamental Rights in such a way that the fundamental rights standard of the Charter will in no case be lower than that afforded by the constitutions of the Member States.

Ultimately, this assumption is corroborated by Article 52(4) of the Charter of Fundamental Rights, which explicitly stipulates that the fundamental rights which are recognised in the Charter as they result from the constitutional traditions common to the Member States shall be interpreted in harmony with these traditions (cf. also Article 6(3) TEU). While not every Member State's constitution contains a separate right to data protection, it is still to be assumed – not least with regard to the case law of the constitutional courts of the Member States – that the fundamental right to data protection is not only part of the constitutional traditions of the Member States, but also part of the human rights and fundamental freedoms within the meaning of Article 53 of the Charter of Fundamental Rights, which are recognised by the constitutions of the Member States (in addition to section 1 *DSG* 2000 see e.g. also Article 51(2) of the Polish Constitution, or the right to informational self-determination that is derived from Article 2(1) of the German Basic Law).

5.3. The last question of the Constitutional Court (question 2.5.) seeks to clarify the role of the case law of the European Court of Human Rights on Article 8 ECHR, which comprises a number of judgments on data protection. However, the explanations on Article 8 of the Charter of Fundamental Rights do not refer to Article 8 ECHR. The explanations on Article 7 of the Charter of Fundamental Rights ("Respect for private and family life") state that the latter corresponds to Article 8 ECHR. In accordance with Article 52(7) of the Charter of Fundamental Rights, the explanations are to be duly considered by the courts as guidance for interpretation. Paragraph 5 of the Preamble not only refers explicitly to the Explanations of the Praesidium of the European Convention, but also to the case law of the European Court of Human Rights. This being the case, the extent to which the case law on Article 8 ECHR is to be considered in the interpretation not only of Article 7, but also of Article 8 of the Charter of Fundamental Rights, needs to be clarified. 1

IV.

1. On these grounds, the Constitutional Court has decided to refer the question as to the validity of Articles 3 to 9 of the Data Retention Directive as well as the questions stated in the outset of this decision on the interpretation of Article 8 of

the Charter of Fundamental Rights to the Court of Justice of the European Union for a preliminary ruling.

2. With the exception of actions, decisions and dispositions of section 19(a) paragraph 1 of the Constitutional Court Act, the proceedings will be continued once the Court of Justice of the European Union has handed down its ruling.

3. Pursuant to section 19 paragraph 4, first sentence, Constitutional Court Act, this decision was taken in private without the need for an oral hearing.

Vienna 28 November 2012
The President:
HOLZINGER

Recording clerk:
FRIEDL