CONSTITUTIONAL COURT
G 47/2012-49, G 59/2012-38, G 62/2012-46,
G 70/2012-40, G 71/2012-36
27 June 2014

Translation in excerpts

# IN THE NAME OF THE REPUBLIC

The Constitutional Court, chaired by President
Gerhart HOLZINGER,

in the presence of Vice-President
Brigitte BIERLEIN

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

as voting members, in the presence of the recording clerk
Christian SIMON,

has decided on the applications filed 1. by the GOVERNMENT OF THE PROVINCE OF CARINTHIA to repeal specified provisions of the Telecommunications Act 2003 (*Telekommunikationsgesetz 2003*), Federal Law Gazette *BGBl*. I 70/2003 as amended by *BGBl*. I 27/2011 (recorded under G 47/2012), 2. by **** ******* **********, *****, represented by Brauneis Klauser Prändl Rechtsanwälte GmbH, Bauernmarkt 2, 1010 Vienna, to repeal specified provisions of the Telecommunications Act 2003 (*Telekommunikationsgesetz 2003*), Federal Law Gazette *BGBl*. I 70/2003 as amended by *BGBl*. I 102/2011, *in eventu* also provisions of the Code of Criminal Procedure 1975 (*Strafprozessordnung 1975*), Federal Law Gazette *BGBl*. 631 as amended by *BGBl*. I 35/2012, and of the Security Police Act (*Sicherheitspolizeigesetz*), Federal Law Gazette *BGBl*. 566/1991 as amended by *BGBl*. I 13/2012 (recorded under G 59/2012), and by 3. **** *** ******** *******, ********************, **** ****, represented by Scheucher Rechtsanwalt GmbH, Lindengasse 39, 1070 Vienna, to repeal specified provisions of the Telecommunications Act 2003 (*Telekommunikationsgesetz 2003*), Federal Law Gazette *BGBl*. I 70/2003 as amended by *BGBl*. I 102/2011, of the Code of Criminal Procedure 1975 (*Strafprozessordnung 1975*), Federal Law Gazette *BGBl*. 631 as amended by *BGBl*. I 53/2012, and of the Security Police Act (*Sicherheitspolizeigesetz*), Federal Law Gazette *BGBl*. 566/1991 as amended by *BGBl*. I 13/2012 (recorded under G 62,70,71/2012), as unconstitutional, after having referred questions to the Court of Justice of the European Union for a preliminary ruling pursuant to Article 267 TFEU, after having conducted a public oral hearing on 12 June 2014, after hearing the submissions of the rapporteur and the statements of the representative of the applicant province government Edmund Primosch, of the second applicant **** ******* *********, *****, and of his legal counsel Gerald Otto, LL.M., of the third applicant **** *** ****** ***** and his legal counsel Ewald Scheucher and of the representatives of the Federal Government Gerhard Hesse, Christian Pilnacek, Christian Singer and Verena Weiss, pursuant to Article 140 of the Constitution (*Bundes-Verfassungsgesetz, B-VG*) and declared on this day:

I. The following provisions in the Federal act by which a Telecommunications Act was enacted (*Telekommunikationsgesetz 2003, TKG 2003*), Federal Law

Gazette *BGBl*. I No 70/2003 as amended by *BGBl*. I No 27/2011, are repealed as unconstitutional:

– section 92 paragraph 3 subparagraph 6 point (b);

– in section 93 paragraph 3, the phrase "including retained data";

– in section 94 paragraph 1, the phrase "including information on retained data";

– in section 94 paragraph 2, the phrase "including information on retained data";

– in section 94 paragraph 4, the phrases "including the transmission of retained data," and "as well as further specifications regarding storage of the logs prepared pursuant to section 102c";

– in section 98 paragraph 2, the phrase ", even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose";

– in section 99 paragraph 5 subparagraph 2, the phrase ", even those stored as retained data pursuant to section 102a paragraph 2 subparagraph 1, paragraph 3 subparagraph 6 points (a) and (b) or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5 for a maximum of six months prior to the query";

– in section 99 paragraph 5 subparagraph 3, the phrase ", even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose";

– in section 99 paragraph 5 subparagraph 4, the phrases "even" and "in accordance with section 102a paragraph 2 subparagraph 1 or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5";

– section 102a;

– section 102b;

– section 102c paragraphs 2,3, and 6;

– in section 109 paragraph 3, subparagraphs 22, 23, 24, 25 and 26.

II. Section 134 subparagraph 2a and section 135 paragraph 2a of the Code of Criminal Procedure 1975 (*StPO*), Federal Law Gazette *BGBl*. No 631 as amended by *BGBl*. I No 33/2011, are repealed as unconstitutional.

III. The following provisions of the Security Police Act (*Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei, [Sicherheitspolizeigesetz, SPG]*), Federal Law Gazette *BGBl*. No 566/1991, are repealed:

– In section 53 paragraph 3a subparagraph 3 as amended by Federal Law Gazette *BGBl*. I No 33/2011, the phrase "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 4 in conjunction with section 102a *TKG* 2003,";

– in section 53 paragraph 3b as amended by Federal Law Gazette *BGBl*. I No 13/2012, the phrase ", even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 3 in conjunction with section 102a *TKG* 2003,";

IV. Earlier legal provisions do not re-enter into force.

V. The Federal Chancellor shall immediately promulgate these dictums in the Federal Law Gazette *Bundesgesetzblatt I*.

VI. The application filed by the GOVERNMENT OF THE PROVINCE OF CARINTHIA under G 47/2012 is rejected on substantive grounds.

[…]

## Reasoning

## I. Applications and Preliminary Proceedings

1. The application G 47/2012:

1.1. Following its resolution of 27 March 2012, the Government of the Province of Carinthia (hereinafter: the applicant province government) has filed an application pursuant to Article 140 paragraph 1 of the Constitution (*Bundes-Verfassungsgesetz, B-VG*) in conjunction with section 62 et seqq. of the Constitutional Court Act (*Verfassungsgerichtshofgesetz, VfGG*) seeking to

"repeal the provisions of […]
section 90 paragraph 6, paragraphs 7 to 8,
section 92 paragraph 3 subparagraphs 2a to 2b, paragraph 3 subparagraph 3 points (a) to (c), paragraph 3 subparagraphs 6a to 6b, paragraph 3 sub-paragraph 8, paragraph 3 subparagraph 8a,
section 93 paragraph 5,
section 94 paragraphs 1 to 2, paragraph 3, paragraph 4,
section 98 paragraph 2,
section 99 paragraph 1, paragraph 5 subparagraphs 1 to 4,
section 102a paragraphs 1 to 7, paragraph 8,
section 102b paragraph 1, paragraph 2, paragraph 3,
section 102c paragraph 1, paragraph 2
*TKG* 2003 as amended by Federal Law Gazette *BGBl*. I 2011/27 in their entirety."

[…]

2.4. The Federal Government has filed an application seeking to reject the application as inadmissible on substantive grounds, *in eventu* to dismiss it as unfounded.

3. The application G 59/2012:

3.1. The applicant under G 59/2012 (hereinafter: second applicant) has filed an application pursuant to Article 140 paragraph 1 of the Constitution in conjunction with section 62 et seqq. of the Constitutional Court Act seeking to repeal provisions of the *TKG* 2003 as amended by Federal Law Gazette *BGBl*. I 102/2011 as unconstitutional, maintaining that section 102a *TKG* 2003 should be repealed because it violates the constitutionally guaranteed right to respect for private and family life, to the protection of personal data, to the freedom of communication and equality of all citizens before the law. Section 1 paragraph 4 subparagraph 5 (probably to mean section 1 paragraph 4 subparagraph 7), section 92 paragraph 3 subparagraph 6b, in section 93 paragraph 3 the phrase "including retained data", in section 94 paragraph 1 the phrase "including information on retained data", section 94 paragraph 4, section 99 paragraph 5 subparagraphs 2, 3, and 4, section 102b, section 102c, section 109 paragraph 3 subparagraphs 22 to 26 *TKG* 2003 are, it is argued, inseparably linked to section 102a *TKG* 2003 and therefore also to be repealed. As regards section 94 paragraph 4 and section 99 paragraph 5 subparagraphs 2, 3 and 4 *TKG* 2003, the second applicant has applied to repeal *in eventu* certain phrases as being unconstitutional. Equally, the second applicant has also applied to repeal *in eventu* as unconstitutional the provisions of section 53 paragraphs 3a and 3b *SPG* and – again *in eventu* – certain phrases in these provisions, respectively, for being inseparably linked to section 102a *TKG* 2003, and for the same reason section 134 subparagraph 2a *StPO* and section 135 paragraph 2a *StPO*.

[…]

4.4. The Federal Government has applied that the application filed by the second applicant be rejected as inadmissible on substantive grounds, *in eventu* that it be dismissed as unfounded.

5. The application G 62,70,71/2012:

5.1. In an application based on Article 140 paragraph 1 of the Constitution (*B-VG*) filed with the Constitutional Court as a "collective individual application", the third applicant and 11,129 other persons have requested the Constitutional Court to repeal provisions of the *TKG* 2003 as amended by Federal Law Gazette *BGBl*. I 102/2011, of the *SPG* as amended by Federal Law Gazette *BGBl*. I 13/2012, and of the *StPO* as amended by Federal Law Gazette *BGBl*. I 53/2012 as unconstitutional. The application by the 11,129 other persons was rejected on substantive grounds in a decision handed down by the Constitutional Court on 10 June 2014 (G 62/2012-36, G 70/2012-30, G 71/2012-26).

It has been applied to repeal section 102a *TKG* 2003 and furthermore, for being inseparably linked to this provision, section 102b, section 102c, in section 99 paragraph 5 subparagraph 2 the phrase ", even those stored as retained data pursuant to section 102a paragraph 2 subparagraph 1, paragraph 3 subparagraph 6 points (a) and (b) or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5 for a maximum of six months prior to the query", in section 99 paragraph 5 subparagraph 3 the phrase ", even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose", in section 99 paragraph 5 subparagraph 4 the phrases "even" and "in accordance with section 102a paragraph 2 subparagraph 1 or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5", section 92 paragraph 3 subparagraph 6 point (b) in its entirety, in section 93 paragraph 3 the phrase "including retained data", in section 94 paragraph 1 the phrase "including information on retained data", in section 94 paragraph 2 the phrase "including information on retained data", in section 94 paragraph 4 the phrases "including information on retained data" and "as well as further specifications regarding storage of the logs prepared pursuant to section 102c", in section 98 paragraph 2 the phrase ", even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose", and subparagraphs 22, 23, 24, 25 and 26 of section 109 paragraph 3 *TKG* 2003 for infringing the right to respect for private and family life and the protection of correspondence pursuant to Article 8 ECHR

and Article 7 of the Charter of Fundamental Rights respectively, the right to data protection pursuant to section 1 of the Data Protection Act 2000 (*Datenschutzgesetz, DSG 2000*) and Article 8 of the Charter respectively, the right to freedom of expression and information pursuant to Article 10 ECHR and Article 11 of the Charter respectively, the right to freedom of assembly and association pursuant to Article 11 ECHR and Article 12 of the Charter respectively, the right to the protection of the telecommunications secret pursuant to Article 10a of the Basic State Law (*Staatsgrundgesetz, StGG*), and the right to the presumption of innocence in criminal law cases pursuant to Article 6 ECHR and Article 48 of the Charter respectively.

For the same reasons, the third applicant has filed an application seeking to repeal section 135 paragraph 2a and section 134 subparagraph 2a of the Code of Criminal Procedure as unconstitutional. Finally, the third applicant has applied to repeal the phrase "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 4 in conjunction with section 102a *TKG* 2003," in section 53 paragraph 3a subparagraph 3 *SPG* and the phrase "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 3 in conjunction with section 102a *TKG* 2003," in section 53 paragraph 3b *SPG*. The principal claim stated by the third applicant is followed by extensive alternative claims.

The third applicant moreover suggests that the Constitutional Court seek a preliminary ruling from the Court of Justice of the European Union as to the compatibility of the Data Retention Directive with the rights enshrined in the Charter of Fundamental Rights.

[…]

6.3. The Federal Government has filed an application seeking to reject the application G 62,70,71/2012 as inadmissible on substantive grounds, and *in eventu* to dismiss the application as unfounded.

7. Applying section 187 of the Code of Civil Procedure (*Zivilprozessordnung, ZPO*) in conjunction with section 35 of the Constitutional Court Act (*VfGG*) *mutatis*

*mutandis*, the Constitutional Court has joined the applications for joint deliberation.

8. By way of decision of 28 November 2012, G 47/12-11, G 59/12-10, G 62,70,71/12-11 (= *VfSlg. 19.702/2012*), the Constitutional Court stayed the judicial review proceedings and referred the following questions to the Court of Justice of the European Union for a preliminary ruling pursuant to Article 267 TFEU:

"1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3-9 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. Concerning the interpretation of the treaties:

2.1. In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Constitutional Court, must 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 be taken into account, for the purpose of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

2.2. What is the relationship between "Union law", as referred to in the final sentence of Article 52(3) of the Charter, and the Directives in the field of the law on data protection?

2.3. In view of the fact that Directive 95/46/EC and Regulation (EC) No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments arising from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

2.4. Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

2.5. Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the ECHR, can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of the latter article?" (quote without the highlightings in the original)

9. The Court of Justice of the European Union joined the request for a preliminary ruling submitted by the Constitutional Court with a corresponding request from the Irish High Court. In a judgment by the Grand Chamber in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* of 8 April 2014, the Court of Justice of the European Union declared the Data Retention Directive to be invalid.

9.1. In its judgment of 8 April 2014, the Court of Justice of the European Union answered the first question referred to it by the Constitutional Court in essence as follows:

It would be appropriate to examine the validity of the Directive in the light of Articles 7 and 8 of the Charter (CJEU, 8 April 2014 [GC], Joined Cases C-293/12, C-594/12, *Digital Rights Ireland and Seitlinger and Others* [paragraph 31]). The duty imposed on providers of publicly available electronic communications services and on public communications network operators in the Data Retention Directive to retain data on the private life of a person and his or her communications during a defined period constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 34). Moreover, the access by the competent national authorities to the retained data, it reasoned, constitutes an additional interference with this fundamental right (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 35 with references from the case law of the ECtHR). Equally, the Data Retention Directive interferes with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter, as it provides for the processing of personal data (CJEU, *Digital Rights Ireland and*

*Seitlinger and Others,* paragraph 36). The Court takes the view that the interference with the fundamental rights laid down in Articles 7 and 8 of the Charter related to the Data Retention Directive is wide-ranging and particularly serious.

In the following, the Court of Justice of the European Union examined whether the interference with the rights guaranteed by Articles 7 and 8 of the Charter is justified (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 38 et seqq.). In this context, it noted that the Data Retention Directive must lay down clear and precise rules governing the scope and application of the measure in question and impose minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risks of abuse and against any unlawful access and use of that data (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 54, referring to the case law of the ECtHR).

In its judgment of 8 April 2014, the Court of Justice of the European Union subsequently elaborated at length on whether the Data Retention Directive would satisfy the requirements set out in paragraph 54 of the judgment (CJEU, *Digital Rights Ireland und Seitlinger and Others*, paragraph 56 et seqq.). Finally it concluded that, by adopting the Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter (CJEU, *Digital Rights Ireland and Seitlinger and Others,* paragraph 69). The Court of Justice of the European Union answered the first question in the sense that the Data Retention Directive is invalid (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 71).

9.2. From the reasoning on the first question submitted for a preliminary ruling by the Constitutional Court it follows that "there is no need to answer its second question" (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 72).

10. In the following, the Constitutional Court left it to the parties in the proceedings before the Constitutional Court to comment on the impact of this judgment on the proceedings before the Constitutional Court. The applicant province government, the applicants under G 59/2012 and G 62,70,71/2012, and the Federal Government made use of this opportunity to submit comments.

[…]

11. On 12 June 2014, the Constitutional Court held a public oral hearing in which the applicant province government, the second and third applicants and their representatives, respectively, and the representatives of the Federal Government commented, in particular, on questions concerning the technical implementation of the obligation to retain data, on the scope of services affected, and on the range of offences for which requests for information are being addressed to operators in practice. In the oral hearing, it was also discussed in how far an inseparable link between the challenged provisions of the *TKG* 2003 on the one hand and the provisions of the Code of Criminal Procedure and the Security Police Act governing data retention on the other existed.

## II. The Law

1. Article 15 of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, 37, last amended by Directive 2009/136/EC, OJ 2009 L 337, 11, provides – in extracts – as follows:

"Article 15
Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.
[1a. inserted by Article 11 of the Data Retention Directive]
1b. […]

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.
3. […]"

2. Article 13 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, OJ 1995 L 281, 31, as amended by Regulation (EC) No 1882/2003, OJ 2003 L 284, 1, provides – in extracts – as follows:

"SECTION VI
EXEMPTIONS AND RESTRICTIONS
Article 13
Exemptions and restrictions
1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.
2. […]"

3. The applications submitted seek, inter alia, that provisions of the Federal act by which a Telecommunications Act was enacted (*Telekommunikationsgesetz 2003, TKG 2003*), Federal Law Gazette *BGBl*. I 70/2003, be repealed. The applications are partly directed at specified provisions of the *TKG* 2003 as amended by Federal Law Gazette *BGBl*. I 27/2011 (such as the application by the Government of the Province of Carinthia G 47/2012, see I.1 above), and partly against specified provisions of the *TKG* 2003 as amended by Federal Law Gazette *BGBl*. I 102/2011 (such as the applications G 59/2012, G 62,70,71/2012).

3.1. The relevant provisions of the *TKG* 2003, Federal Law Gazette *BGBl*. I 70/2003 as amended by *BGBl*. I 27/2011, provide – in extracts – as follows (the challenged provisions are highlighted):

"Section 1
General
Purpose

Section 1(1) The purpose of this Federal Act is to promote competition in the field of electronic communications so that the population and the economy can be provided with reliable, low-cost, high-quality and innovative communications services.
(2)-(3) […]
(4) The following Directives of the European Union have been transposed by this Federal Act:
1.-5. […]
6. Directive 2006/24/EC 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, OJ L 105, 13.04.2006, p. 54.

[…]

Duties to provide information

Section 90(1)-(5) […]
(6) Providers of communications services shall be obliged to provide information to administrative authorities, at their written and substantiated request, on master data, as defined in section 92 paragraph 2 subparagraph 3 points (a) to (e), of subscribers who are suspected of having committed an administrative offence by an act using a public telecommunications network, to the extent that this is possible without the processing of traffic data.
(7) At the written request of the competent courts, public prosecutor's offices or the police responsible for criminal investigations (section 76a paragraph 1 Code of Criminal Procedure), providers of communications services are obliged to provide those authorities with information on master data (section 92 paragraph 3 subparagraph 3) on subscribers for the investigation and prosecution of actual suspicions of a criminal offence. This shall apply accordingly to requests from law-enforcement authorities in accordance with section 53 paragraph 3a subparagraph 1 Security Police Act (*Sicherheitspolizeigesetz, SPG*). In urgent cases, such requests may be conveyed orally on a preliminary basis.
(8) Providers of mobile communications networks shall maintain records of the geographical location of the radio cells used to operate their services in order to ensure that a cell ID can be accurately matched to its actual geographical location with an indication of geo-coordinates for any point in time within the last six months.

[…]

Section 12

Confidentiality of the communications, Data protection general

Section 92(1) Unless otherwise provided by this Federal Act, the provisions of the Data Protection Act 2000, Federal Law Gazette *BGBl*. I No 165/1999, shall apply to the facts regulated in this Federal Act.

(2) The provisions of the Code of Criminal Procedure shall remain unaffected by the provisions of this section.

(3) Irrespective of section 3, in this section the term

1. "provider" means an operator of public communications services;
2. "user" means any natural person using a publicly available communications service, for private or business purposes, without necessarily having subscribed to this service;

2a. "subscriber identifier" means an identifier which enables communication to be attributed to a specific subscriber

2b. "e-mail address" means the unique identifier assigned to an electronic mailbox by an Internet e-mail provider;

3. "master data" means all personal data required for the establishment, processing, modification or termination of the legal relations between the user and the provider or for the production and publication of subscriber directories, including

a) name (surname and first name in the case of natural persons, name or designation in the case of legal entities),

b) academic degree in the case of natural persons,

c) address (residential address in the case of natural persons, registered office or billing address in the case of legal entities),

d) subscriber number and other contact information for the communication,

e) information on type and contents of the contractual relationship,

f) financial standing;

4. "traffic data" means any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof;

4a. "access data" means the traffic data created at the operator during access by a subscriber to a public communications network and required for assignment to the subscriber of the network addresses used for a communication at a specific point of time;

5. "content data" means the contents of conveyed communications (subparagraph 7);

6. "location data" means any data processed in a communications network or by a communications service, indicating the geographic position of the telecommunications terminal equipment of a user of a publicly available communications service; in the case of fixed-link telecommunications terminal equipment, location data refer to the address of the equipment;

6a. “cell ID” means the identity of the cell from which a mobile telephony call originated

6b. “retained data" means data which are stored solely in order to fulfil an obligation to retain data pursuant to section 102a;

7. "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available communications service.

This does not include any information conveyed as part of a broadcasting service to the public over a communications network except to the extent that the information can be related to the subscriber or user receiving the information;
8. "call" means a connection established by means of a public telephone service allowing two-way or multi-way communication in real time;
8a. "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;
9.-16. […]

Confidentiality of the communications

Section 93(1) The content data, traffic data and location data shall be subject to confidentiality of the communications. Confidentiality of the communications shall also refer to the data of unsuccessful connection attempts.
(2) Every operator and all persons who are involved in the operator's activities shall observe confidentiality of the communications. The obligation to maintain confidentiality shall continue to exist also after termination of the activities under which it was established.
(3) Persons other than a user shall not be permitted to listen, tap, record, intercept or otherwise monitor communications and the related traffic and location data as well as pass on related information without the consent of all users concerned. This shall not apply to the recording and tracing of telephone calls when answering emergency calls and to cases of malicious call tracing, surveillance of communications and information on communication data, including retained data, as well as to technical storage which is necessary for the conveyance of a communication.
(4) […]
(5) Editorial confidentiality (section 31 Media Act [*Mediengesetz*]) and other confidentiality obligations laid down in other Federal acts shall be complied with, subject to the protection of clerical and professional secrecy and the ban on their circumvention pursuant to section 144 and section 157 paragraph 2 Code of Criminal Procedure. The provider shall not be obliged to verify such compliance.

Technical facilities

Section 94(1) In accordance with the regulations issued under paragraphs 3 and 4, the provider shall be obliged to make available all facilities necessary for monitoring communications and for providing information on data in communications, including information on retained data in accordance with the provisions of the Code of Criminal Procedure (*Strafprozessordnung, StPO*). For the provision of information, the provider is to be reimbursed 80% of the costs (personnel and material costs) incurred in order to establish the functions necessary pursuant to the regulations issued under paragraphs 3 and 4 in the provider's systems. In agreement with the Federal Minister of the Interior, the Federal Minister of Justice and the Federal Minister of Finance, the Federal

Minister of Transport, Innovation and Technology shall issue an regulation defining the assessment base for this percentage and the procedures for asserting such claims to reimbursement. This regulation shall take into account, in particular, the economic reasonableness of the effort, any possible interest of the undertaking concerned in the services to be provided and any possible danger caused by the technical facilities provided which is to be averted by the participation requested, as well as the simplicity and economy of the procedure.

(2) The provider shall be obliged to cooperate to the required extent in the monitoring of communications and in the provision of information on communications data, including information on retained data, in accordance with the provisions of the Code of Criminal Procedure (*Strafprozessordnung, StPO*). In agreement with the Federal Minister of Transport, Innovation and Technology and the Federal Minister of Finance, the Federal Minister of Justice shall issue an regulation providing for adequate compensation of costs, taking into account, in particular, the economic reasonableness of the effort, any possible interest of the undertaking concerned in the services to be provided and any possible danger caused by the technical facilities provided which is to be averted by the participation requested, as well as the public duty of the administration of justice.

(3) By way of regulation, the Federal Minister of Transport, Innovation and Technology, in agreement with the Federal Ministers of the Interior and Justice, may specify, in line with the state of the art, detailed provisions for the design of the technical facilities to guarantee interception of communications according to the provisions of the Code of Criminal Procedure and for the protection of the data to be transmitted from unauthorised notice or use by third parties. A report shall be submitted to the executive committee of the National Council directly after the regulation has been issued.

(4) The transmission of traffic data, location data and master data which require the processing of traffic data, including the transmission of retained data, under the provisions of the Code of Criminal Procedure *(Strafprozessordnung, StPO)* as well as the Security Police Act (*Sicherheitspolizeigesetz, SPG*), must be carried out using a transmission technology which allows the identification of the sender and recipient as well as ensuring data integrity. The data are to be transmitted in comma-separated value (CSV) file format using an advanced encryption technology. This does not apply to the transmission of data in cases pursuant to section 98, of data in cases pursuant to section 99 paragraph 5 subparagraphs 3 and 4 in cases of imminent danger, of location data in cases requiring determination of current whereabouts pursuant to Article 134 et seq. Code of Criminal Procedure, or the transmission of accompanying call data in the course of communications monitoring. In agreement with the Federal Minister of the Interior and the Federal Minister of Justice, the Federal Minister of Transport, Innovation and Technology may issue an regulation stipulating a standardised

definition of the syntax, data fields and encryption for the storage and transmission of the data as well as further specifications regarding storage of the logs prepared pursuant to section 102c. A report shall be submitted to the executive committee of the National Council directly after the regulation has been issued.

[…]

Information to operators of emergency services

Section 98(1) Operators shall provide information to operators of emergency services, at their request, on master data as defined in section 92 paragraph 3 subparagraph 3 points (a) to (d) as well as on location data as defined in section 92 paragraph 3 subparagraph 6. Both cases shall require an emergency to permit the transmission, which can be only averted by providing this information. The need for transmission of the information shall be documented by the emergency service operator and shall be presented to the operator without delay, however, at the latest within 24 hours. The operator must not make the transmission dependent on previous presentation of the need. The emergency service operator shall be responsible for the legal permissibility of the request for information.

(2) In cases where it is not possible to determine a current location, the cell ID of the last communication registered for the communication equipment belonging to the endangered person may be processed, even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose. The provider shall inform the subscriber concerned about the provision of location data pursuant to this item at the earliest 48 hours and at the latest 30 days after such provision; in general, this information is to be provided by sending a short message (SMS) or in writing where it is not possible to send a short message. The information sent to the subscriber shall include the following:

a) the legal basis for the provision of information;
b) the data in question;
c) the date and time of the query;
d) an indication of the body which requested the location data as well as the contact information for that body.

Traffic data

Section 99(1) Except for cases regulated by this law, traffic data must not be stored or transmitted and shall be erased or made anonymous by the operator without delay after termination of the connection. The permissibility of further use of traffic data transmitted in accordance with paragraph 5 shall be based on the provisions of the Code of Criminal Procedure *(Strafprozessordnung, StPO)* as well as the Security Police Act *(Sicherheitspolizeigesetz, SPG*).

(2) If required for the purposes of subscriber billing, including interconnection payments, the operator shall store traffic data up to the end of the period during which the bill may be lawfully challenged or payment pursued. In case of a dispute, these data shall be made available in full to the decision-taking body as well as to the arbitration authority. If proceedings on the amount of the charges are instituted, the data must not be erased until the final decision on the amount of the charges is taken. The amount of stored traffic data must be restricted to what is absolutely necessary.
(3)-(4) […]
(5) Traffic data may be processed for information purposes with regard to the following:
1. data on communications pursuant to section 134 paragraph 2 Code of Criminal Procedure (*Strafprozessordnung, StPO*);
2. access data, even those stored as retained data pursuant to section 102a paragraph 2 subparagraph 1, paragraph 3 subparagraph 6 points (a) and (b) or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5 for a maximum of six months prior to the query, to courts and public prosecutor's offices in accordance with section 76a paragraph 2 *StPO*;
3. traffic data and master data in cases where it is necessary to process traffic data for this purpose and for the provision of information on location data to competent law-enforcement agencies pursuant to the Security Police Act (*Sicherheitspolizeigesetz, SPG*) in accordance with section 53 paragraph 3a and 3b *SPG*. In cases where it is not possible to determine a current location, the cell ID of the last communication registered for the communication equipment may be processed, even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose;
4. access data, even in cases where these data were retained in accordance with section 102a paragraph 2 subparagraph 1 or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5 no more than three months prior to the query, to competent law-enforcement agencies pursuant to the Security Police Act (*Sicherheitspolizeigesetz, SPG*) in accordance with section 53 paragraph 3a subparagraph 3 *SPG*.

[…]

Data retention

Section 102a (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 2a 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 is 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 102b, the claims to information on this use of data shall be based solely on the provisions of the Code of Criminal Procedure.

Information on retained data

Section 102b (1) 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 Article 135 paragraph 2a Code of Criminal Procedure.
(2) The data to be stored pursuant to section 102a 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 according to the provisions of the Code of Criminal Procedure and the procedure prescribed therein.
(3) The data is to be provided in an "appropriately protected form" according to section 94 paragraph 4.

Data security, logging and statistics

Section 102c (1) Retained data is to be stored in such a way that it is possible to differentiate the data stored in accordance with sections 96, 97, 99, 101 and 102. The data is to be protected by appropriate technical and organisational measures against unlawful destruction, accidental loss or unlawful storage, processing, access and disclosure. Likewise, 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. Log data are to be stored for a period of three years after the end of the data storage period for each retention date. The Austrian Data Protection Commission, which is responsible for data protection supervision under section 30 Data Protection Act (*Datenschutzgesetz, DSG* 2000), shall be responsible for monitoring compliance with these provisions. The Federal Minister of Transport, Innovation and Technology may issue an regulation detailing the standards of due care to be observed in order to ensure data security.
(2) Providers obliged to store data pursuant to section 102a shall ensure that any access to retained data as well as any queries and information provided on retained data pursuant to section 102b are logged in a non-alterable form.
These logs shall include the following:

1. the reference to the public prosecutor's order or court order pursuant to the provisions of the Code of Criminal Procedure *(Strafprozessordnung, StPO)* which was conveyed to the provider along with the request for information and which formed the basis for the provision of data;
2. in cases pursuant to section 99 paragraph 5 subparagraphs 3 and 4, the law-enforcement agency's reference number conveyed to the provider along with the request for information;
3. the date of the request as well as the date and exact time at which the information was provided;
4. the number of data records provided, broken down by date and category pursuant to section 102a paragraphs 2 to 4;
5. the storage duration of the conveyed data at the time when provision was ordered;
6. the name and address of the subscriber concerned in the information on retained data, to the extent that the provider is able to provide such data; and
7. a unique identifier which makes it possible to identify the persons who accessed the retained data within the provider's undertaking.

(3) Log data is to be stored in such a way that it is possible to differentiate them from retained data and from data stored in accordance with sections 96, 97, 99, 101 and 102.

(4) The providers obliged to store data pursuant to sections 102a shall
1. convey the log data pursuant to paragraph 2 to the Austrian Data Protection Commission and the Data Protection Council for the purpose of supervising data protection and ensuring data security; and
2. convey the log data pursuant to paragraph 2 subparagraphs 2 to 4 to the Federal Minister of Justice for the purpose of reporting to the European Commission and the Austrian National Council.

(5) Log data are to be conveyed at the written request of the Austrian Data Protection Commission or the Federal Minister of Justice; in addition, by 31 January each year, log data from the previous calendar year must be conveyed to the Federal Minister of Justice.

(6) Beyond the logging obligations pursuant to paragraph 2, storage of the data records conveyed shall not be permitted.

[…]

Administrative penal regulations

Section 109(1)-(2) […]
(3) Any person who
1.-21. […]
22. violates section 102a by failing to store data; this offence shall not be punishable in cases where the investment costs required for this purpose have

not yet been reimbursed on the basis of an regulation issued pursuant to section 94 paragraph 1;
23. violates section 102a paragraph 8 by failing to delete data;
24. violates section 102b by providing information on data in the absence of a court authorisation;
25. violates section 102b by transmitting data over a communications network in unencrypted form;
26. violates section 102c by failing to log data or to provide the necessary information
shall be guilty of an administrative offence and shall be punished by a fine of up to EUR 37,000.00.
(4)-(9) […]

[…]

Entry into effect

Section 137(1)-(3) […]
(4) Sections 94 paragraphs 1 and 102a paragraph 1 as amended by Federal Law Gazette I *BGBl*. No. 27/2011 shall enter into force as of 1 April 2012".

3.2. Section 1 paragraph 4 of the Telecommunications Act 2003 (*TKG* 2003), Federal Law Gazette *BGBl*. I 70/2003 as amended by *BGBl*. I 102/2011, provides – in extracts – as follows (the challenged provision is highlighted):

"(4) The following Directives of the European Union have been transposed by this Federal Act:
1.-6. […]
7. Directive 2006/24/EC 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, OJ L 105, 13 April 2006, p. 54."

3.3. The remaining provisions of the *TKG* 2003 challenged in the applications G 59/2012 and G 62,70,71/2012 had not been amended by the Federal act amending the Telecommunications Act 2003, the Federal act on the establishment of an Austrian Communications Authority and a Federal Communications Board **(***KommAustria-Gesetz*) and the Consumer Authorities Cooperation Act (*Verbraucherbehörden-Kooperationsgesetz*) (Federal Law Gazette *BGBl*. I 102/2011). After the entry into force of the latter Federal act, they were applicable as amended by the Federal act amending the Telecommunications Act 2003 (*TKG* 2003) (Federal Law Gazette *BGBl*. I 27/2011) (see II.3.1 above).

3.4. As of 1 January 2014, the term "Data Protection Commission" was replaced by the term "Data Protection Authority" in section 102c paragraphs 1, 4 and 5 *TKG* 2003 (Article 2 of the Federal act amending the Data Protection Act 2000 [*DSG-Novelle 2014*], Federal Law Gazette *BGBl*. I 83/2013).

4. The Federal Security Police Act (*Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei* [*Sicherheitspolizeigesetz, SPG*]), Federal Law Gazette *BGBl*. 566/1991 as amended by *BGBl*. I 13/2012, provides – in extracts – as follows (the challenged provisions are highlighted):

"Chapter 2

Investigation service, limitation to the exercise of official duties

Section 52. In accordance with this chapter, personal data may be used by the law-enforcement authorities only to the extent which is necessary to carry out their duties. Authorisations based on other Federal acts shall remain unaffected thereby.

Permissibility of processing

Section 53(1) The law-enforcement authorities may collect and further process personal data in order to

1. comply with the general duty of rendering first general assistance (section 19);
2. combat criminal organisations (section 16 paragraph 1 subparagraph 2 and section 21);
2a. conduct an extended potential danger identification (section 21 paragraph 3) subject to the conditions of section 91c paragraph 3;
3. avert dangerous attacks (section 16 paragraphs 2 and 3, and section 21 paragraph 2); including measures of crime prevention which are required for averting danger (section 16 paragraph 4 and section 28a);
4. prevent likely dangerous attacks against life, health, public morality, freedom, property or the environment (section 22 paragraphs 2 and 3) or to prevent dangerous attacks by means of a crime analysis, if, given the nature of such attack, it is likely that it will be committed repeatedly;
5. for the purposes of searches (section 24);
6. maintain public order in a given event;
7. analyse and assess the probability of a threat to constitutional institutions and their capacity to act by the commission of criminal acts pursuant to chapters fourteen and fifteen of the Criminal Code.

(2) The law-enforcement authorities may collect and further process data which they have processed in executing Federal or province laws for the purposes and under the conditions set out in paragraph 1; however, they shall not be allowed

to perform an automated matching of data within the meaning of section 141 Code of Criminal Procedure. Existing bans on transmission shall remain unaffected.

(3) The law-enforcement authorities may request information from the services of the territorial entities (*Gebietskörperschaften*), other public-sector entities and institutions operated by the latter which is needed to avert dangerous attacks, for an extended identification of dangers under the conditions set out in paragraph 1, or to combat criminal organisations. The provision of such information may be refused only if other public interests outweigh the interests of averting danger or if there is any other statutory duty of confidentiality beyond the duty of official secrecy (Article 20 paragraph 3 of the Federal Constitution).

(3a) The law-enforcement authorities may request information from operators of public telecommunications services (section 92 paragraph 3 subparagraph 1 *TKG* 2003 [*Telekommunikationsgesetz 2003*], Federal Law Gazette *BGBl*. I No 70) and from other service providers (section 3 subparagraph 2 E-Commerce Act [*E-Commerce-Gesetz, ECG*], Federal Law Gazette *BGBl*. I No 152/2001):

1. concerning the name, address and subscriber number of a specific line, if such is required to carry out their duties under this Federal act;
2. concerning the IP address for a given communication and time of transmission, if such data is required as an essential prerequisite to avert
a) a concrete danger to the life, health or freedom of a person within the framework of the general duty of rendering first general assistance (section 19),
b) a dangerous attack (section 16 paragraph 1 subparagraph 1) or
c) a criminal organisation (section 16 paragraph 1 subparagraph 2),
3. concerning the name and address of a user to whom an IP address was assigned at a given moment in time, if such data is required as an essential prerequisite to avert
a) a specific danger to the life, health or freedom of a person within the framework of the general duty of rendering first assistance (section 19),
b) a dangerous attack (section 16 paragraph 1 subparagraph 1) or
c) a criminal organisation (section 16 paragraph 1 subparagraph 2),
<u>even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 4 in conjunction with section 102a *TKG* 2003,</u>
4. concerning the name, address and subscriber number of a given line by referring to a call that was made from that line, indicating the time period as specifically as possible and the number called, if this is necessary to comply with the general duty of rendering first general assistance or to avert dangerous attacks.

(3b) If, based on given facts, it is suspected that there is currently a danger to the life, health or freedom of a person, the law-enforcement authorities may request information from operators of public telecommunication services concerning location data and the international mobile subscriber identity (IMSI) of the terminal equipment carried by the person at risk or the person accompanying them, in order to render assistance or avert such a danger, <u>even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5</u>

subparagraph 3 in conjunction with section 102a *TKG* 2003, and apply technical means for localizing the terminal equipment.

(3c) In the cases of paragraphs 3a and 3b, the law-enforcement authority shall be responsible for the legal admissibility of the request for information. The requested authority shall provide the requested information immediately and, in the case of paragraph 3b, against reimbursement of costs pursuant to the Regulation on Surveillance Costs (*Überwachungskostenverordnung, ÜKVO*, Federal Law Gazette *BGBl*. II No 322/2004). In the case of paragraph 3b, the law-enforcement authority shall thereafter submit to the operator without delay, no later than within 24 hours, a written documentation. In the cases listed in paragraph 3a subparagraph 3 and paragraph 3b, the law-enforcement authority shall inform the data subject that information was requested to assign their name or address to a given IP address (section 53 paragraph 3a subparagraph 3) or to identify their location (section 53 paragraph 3b), if the use of retained data pursuant to section 99 paragraph 5 subparagraphs 3 or 4 in conjunction with section 102a *TKG* 2003 was necessary for that purpose. In such a case, the data subject shall, verifiably and as soon as possible, be informed of the legal basis and the date and time of the request for information. Informing data subjects may be deferred for as long as this would thwart the purpose of the investigation and may be dispensed with altogether if the data subject is verifiably in possession of such information already, or if it is impossible to inform the data subject.

(3d) In order to prevent or avert dangerous attacks against the environment, the law-enforcement authorities may request information from Federal, province and local authorities about facilities and installations they have approved, where, owing to the use of machinery or equipment, the storage, use or production of substances, their mode of operation and equipment, or for other reasons, there is a heightened fear of danger to the life and health of several persons or a severe hazard to property or the environment should the facility or installation diverge from the state that is compliant with the law. The requested authority is under an obligation to provide such information.

(4) Aside from the cases of paragraphs 2 to 3b and 3d, the law-enforcement authorities may collect and further process personal data for the purposes of paragraph 1 from all other accessible sources, using appropriate means, in particular by accessing generally available data.

(5) In individual cases, and under the terms of section 54 paragraph 3, the law-enforcement authorities may, in order to fend off dangerous attacks and combat criminal organisations, use personal image data which have been lawfully recorded by means of image and audio recording devices by public or private legal entities and transmitted to the law-enforcement authorities, if certain facts suggest a serious danger for public safety, as well as for an extended identification of dangers (section 21 paragraph 3) as well as for the purpose of searches (section 24). In such a case, special attention shall be given to assuring the proportionality (section 29) of the interference with the data subject's private sphere and the given occasion. The use of data on non-public behaviour shall not be permissible."

5. The Code of Criminal Procedure 1975 (*StPO*), Federal Law Gazette *BGBl*. 631 as amended by *BGBl*. I 35/2012, provides – in extracts – as follows (the challenged provisions are highlighted):

"Part 5
Seizure of letters, information on communications data, Information on retained data, and Surveillance of communications and of persons,

Definitions
Section 134. Within the meaning of this Federal act
1. […]
2. "information on communications data" means the provision of information on traffic data (section 92 paragraph 3 subparagraph 4 *TKG*), access data (section 92 paragraph 3 subparagraph 4a *TKG*), which are not subject to an order pursuant to section 76a paragraph 2, and location data (section 92 paragraph 3 subparagraph 6 *TKG*) of a telecommunications service or an information society service (section 1 paragraph 1 subparagraph 2 Notification Act [*Notifikations-gesetz]*),
2a. "information on retained data" means providing information on data which providers of public communications services must store pursuant to section 102a paragraphs 2 to 4 *TKG* and which, pursuant to subparagraph 2, are not subject to the provision of information pursuant to section 99 paragraph 2
3.-5. […]

Seizure of letters, information on communications 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 communications 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 collect data about the accused;

4. if, based on given facts, it is to be expected that the whereabouts of a fugitive or absent perpetrator 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 102a and 102b *TKG*) shall be permissible 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 278b 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 278b Code of Criminal Procedure, or
b. if it can be assumed, based on given facts, that the person strongly suspected of having committed a criminal act (point a) will use the technical device or establish a connection with such device;
4. in the cases of paragraph 2 subparagraph 4."

5.1. The provisions of the Code of Criminal Procedure as amended by Federal Law Gazette *BGBl*. I 53/2012 challenged by the third applicant do not deviate from the provisions stated.

6. The relevant provisions of the Federal Act on the Protection of Personal Data (Data Protection Act 2000 [*Datenschutzgesetz 2000, DSG 2000*]), Federal Law Gazette *BGBl*. I 165/1999 as amended by *BGBl*. I 83/2013, provide – in extracts – as follows:

"Article 1
(Constitutional Provision)
Fundamental Right to Data Protection
Section 1(1) Anyone shall have the right to secrecy of their personal data, 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) Unless personal data are used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are permitted only to safeguard the overriding legitimate interests of another person. In the event of interferences by a public authority, such 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 *BGBl*. No 210/1958). Such laws may provide for the use of data that deserve special protection only in order to safeguard important public interests and shall provide for suitable safeguards for the protection of the data subjects' interest in secrecy. Even with permitted restrictions, the interference with the exercise of a fundamental right shall be conducted using only the least intrusive of all effective means.
(3) Insofar as their personal data are destined for automated processing or manual processing, i.e. in filing systems without automated processing, as provided for by law, anyone shall have the right to
1. obtain information as to who processes which data concerning them, where the data originated, for which purpose they are used, as well as to whom the data are transmitted;
2. have incorrect data rectified and illegally processed data deleted.
(4) Restrictions of the rights pursuant to paragraph 3 shall only permitted under the conditions laid out in paragraph 2.

[…]

## Part 6
## Legal Remedies
## Control Rights of the Data Protection Authority

Section 30(1) Pursuant to this Federal Act, anyone shall have the right to lodge an application with the Data Protection Authority for an alleged infringement of their rights or breach of a controller's or processor's obligations concerning them.
(2) The Data Protection Authority shall have the right to examine data applications if there is a reasonable suspicion that the rights and obligations stated in paragraph 1 have been infringed. The Data Protection Authority may in particular order the controller or processor of the examined data application to provide all necessary clarifications and to grant access to data applications and relevant documents.
(2a) If an application which is admissible under paragraph 1 or a reasonable suspicion under paragraph 2 relates to a data application (filing system) which is subject to the obligation of notification, the Data Protection Authority may review whether the notification obligation has been met and take appropriate action pursuant to sections 22 and 22a as required.
(3) Data applications subject to prior control pursuant to section 18 paragraph 2 may be examined even if there is no suspicion of an unlawful use of data. The same applies to those fields of government where a public sector controller invokes the general applicability of section 26 paragraph 5 and section 27 paragraph 5.

(4) For the purposes of inspection, the Data Protection Authority shall have the right, after having informed the owner of the premises and the controller (processor), to enter premises where data applications are carried out, to operate data processing equipment, run the processing to be examined and make copies of storage media to the extent which is indispensable to be able to exercise its control rights. The controller (processor) shall render the assistance necessary for such inspection. The controls are to be exercised in a way which least interferes with the rights of the controller (processor) and of third parties.
(5) Information obtained by the Data Protection Authority or its agents during any examination shall be used only for controls conducted in the implementation of data protection regulations. This includes the use of information for litigation in court by an intervening party or the Data Protection Authority pursuant to section 32. Moreover, the obligation of confidentiality also exists vis-à-vis courts and administrative authorities, in particular fiscal authorities, with the reservation that, if a suspicion of a criminal act pursuant to sections 51 and 52 of this Federal Act or a criminal act pursuant to sections 111a, 119, 119a, 126a to 126c, 148a or section 278a of the Criminal Code, Federal Law Gazette *BGBl*. No 60/1974, or of any crime punishable by more than five years of imprisonment arises from such inspection, charges shall be filed and requests for assistance pursuant to section 76 Code of Criminal Procedure, Federal Law Gazette *BGBl*. No 631/1975 regarding such crimes and offences shall be complied with.
(6) To establish the rightful state, the Data Protection Authority may, unless measures pursuant to sections 22 and 22a or paragraph 6a have to be taken, issue recommendations and set an appropriate deadline for compliance as required. If a recommendation is not complied with within the set period, the Data Protection Authority may, depending on the kind of violation, *ex officio*,
1. bring a criminal charge pursuant to sections 51 or 52, or
2. in the case of severe violations by a private sector controller, file a lawsuit before the competent court of law pursuant to section 32 paragraph 5, or
3. in the case of a violation by controllers who are bodies of a territorial entity, involve the highest competent authority. This authority shall take measures within an appropriate period of time, not exceeding twelve weeks, to ensure that the recommendation made by the Data Protection Authority is complied with or inform the Data Protection Authority why the recommendation was not complied with. This reason may be publicly disclosed by the Data Protection Commission in an appropriate manner unless this is contrary to official secrecy.
(6a) If the operation of a data application puts the interests of secrecy of the data subject deserving protection seriously and directly at risk (imminent danger), the Data Protection Authority may prohibit the continuation of the data application by way of administrative ruling (*Bescheid*) in accordance with section 57 paragraph 1 of the General Administrative Procedures Act (*Allgemeines Verwaltungsverfahrensgesetz, AVG*), Federal Law Gazette *BGBl*. No 51/1991. It is also possible to prohibit such continuation partially, if this is technically feasible, gives a meaningful result with regard to the purpose of the data application, and is sufficient to eliminate the risk. If the interdiction is not complied with immediately, criminal charges shall be brought pursuant to section 52 paragraph 1 subparagraph 3. If an interdiction under this paragraph has become final, any

pending procedure for correction pursuant to section 22a paragraph 2 has to be discontinued without any further formalities. The data application is to be deleted from the register in line with the extent of the interdiction.
(7) The intervening party shall be informed as to how his application was dealt with.

Complaint before the Data Protection Authority

Section 31(1) The Data Protection Authority shall decide on complaints by persons or groups of persons whose right to information pursuant to section 26 or section 50 paragraph 1 third sentence or whose right to disclosure of an automatically processed individual decision pursuant to section 49 paragraph 3 has allegedly been infringed insofar as the request for information (the application for information or disclosure) does not relate to the use of data for acts serving the legislature or judicature.
(2) Furthermore, the Data Protection Authority shall decide on complaints by persons or groups of persons whose right to secrecy (section 1 paragraph 1) or whose right to correction or deletion (sections 27 and 28) has allegedly been infringed, unless such claim has to be asserted before a court pursuant to section 32 paragraph 1 or is directed against a body serving the legislature or judicature.
(3) The complaint shall contain:
1. a description of the right considered to be infringed,
2. to the extent reasonable, a description of the legal entity or the body which is deemed responsible for the alleged infringement (respondent),
3. the facts from which the infringement is derived,
4. the reasons on which the alleged unlawfulness is based,
5. a request to establish the existence of the alleged infringement, and
6. any details which are necessary to decide whether the complaint has been filed in due time.
(4) A complaint pursuant to paragraph 1 shall be accompanied by the relevant request for information (the application for information or disclosure) and a reply by the respondent, as appropriate. A complaint pursuant to paragraph 2 shall be accompanied by the relevant request for correction or deletion and a reply by the respondent, as appropriate.
(5) The control rights granted to the Data Protection Authority by section 30 paragraphs 2 to 4 also apply in the complaint procedure pursuant to paragraph 1 and 2 vis-à-vis the respondent. The duty of confidentiality pursuant to section 30 paragraph 5 shall equally apply to this procedure.
(6) If the complaint filed pursuant to paragraphs 1 or 2 is admissible, any control procedure instituted based on an application under section 30 paragraph 1 on the same issue has to be discontinued by providing pertinent information (section 30 paragraph 7). Nevertheless, the Data Protection Authority may, even when the complaint procedure is pending, proceed *ex officio* pursuant to section 30 paragraph 2, if there is a reasonable suspicion that obligations under data protection provisions have been infringed beyond the scope of the individual complaint. Section 30 paragraph 3 shall remain unaffected thereby.

(7) Inasmuch as a complaint pursuant to paragraphs 1 or 2 is found to be justified, it shall be granted and the existence of an infringement established. If an established infringement of the right to information (paragraph 1) falls under the responsibility of a controller in the private sector, the latter shall moreover be ordered, upon request, to – again – respond to the request for information pursuant to section 26 paragraphs 4, 5 or 10, to the extent required to eliminate the infringement having been established. Inasmuch as the complaint is found to be unjustified, it shall be rejected.
(8) A respondent against whom a complaint for infringement of rights pursuant to sections 26 to 28 has been filed may, by responding to the claimant pursuant to section 26 paragraph 4 or section 27 paragraph 5, eliminate the alleged infringement retroactively, for as long as the proceedings before the Data Protection Authority have not been terminated. If the Data Protection Authority deems the complaint to be settled by such response by the respondent, it shall hear the claimant thereon. At the same time, the latter shall be informed that the Data Protection Authority will end the proceedings without further formalities if he does not give, within a reasonable period of time, a reason why he considers the originally alleged infringement as still not having been at least partially eliminated. If such answer by the claimant modifies the merits of the case (section 13 paragraph 8, General Administrative Procedures Act) the initial complaint shall be deemed withdrawn and a new complaint deemed as having been filed simultaneously. In such a case, the initial complaint procedure shall also be terminated without further formalities, and the claimant be informed thereof. Late replies shall be disregarded.
[…]

Court Action

Section 32(1) Claims for infringement of the rights of a person or a group of persons to secrecy, rectification or deletion of data against natural persons, groups of persons, or legal entities established under private law, shall, as long as such legal entities were not acting in the execution of their duties under the law during the alleged infringement, be brought before the civil courts.
(2) If data have been used contrary to the provisions of this Federal Act, the data subject shall is entitled to the discontinuance and redress of such unlawful condition.
(3) In order to safeguard the claims for discontinuance based on this Federal Act, injunctions may be issued even if the requirements set out in section 381 Enforcement Act (*Exekutionsordnung*) are not met. This also applies to orders concerning the obligation to make a notation.
(4) Actions and applications for injunctions pursuant to this Federal Act shall in the first instance be lodged with the regional civil court (*Landesgericht*) in whose district the claimant (applicant) has his habitual residence or registered office. Actions (applications) may, however, also be brought before the regional civil court in whose district the respondent has his habitual residence, registered office or a branch office.
(5) Whenever there is a justified suspicion that a serious data protection violation has been committed by a private sector controller, the Data Protection

Authority shall file an action for a declaratory judgment (section 228 Code of Civil Procedure) with the court having jurisdiction pursuant to paragraph 4 second sentence.
(6) On request of an intervening party (section 30 paragraph 1) the Data Protection Authority shall, if such action appears necessary to safeguard the interests of a large number of natural persons protected under this Federal Act, join the proceedings in support of the intervening party as third-party intervener (sections 17 et seq. Code of Civil Procedure).
(7) In the case of an admissible claim pursuant to paragraph 1 which according to the view of the court relates to a data application subject to the obligation of notification, the court may request the Data Protection Authority to conduct a review pursuant to sections 22 and 22a. The Data Protection Authority shall inform the court of the outcome of this review. The court shall then also notify the parties of the outcome, unless the proceedings have been decided with final effect.

## III. Considerations

The Constitutional Court has considered the applications which were joined, applying sections 187 and 404 Code of Civil Procedure (*ZPO*) in conjunction with section 35 paragraph 1 Constitutional Court Act (*VfGG*) *mutatis mutandis*, for joint hearing, deliberation and decision:

### 1. As to the admissability

1.1. In its decision of 28 November 2012, *VfSlg. 19.702/2012*, by means of which questions were referred to the Court of Justice of the European Union for a preliminary ruling, the Constitutional Court provisionally assumed for the purpose of judicial review proceedings that the application by the Government of the Province of Carinthia G 47/2012 and the individual applications G 59/2012 and G 62,70,71/2012 are admissible (see IV.1.1. of the decision of 28 November 2012, *VfSlg. 19.702/2012*). In the judicial review proceedings, which are now resumed, the admissibility of the applications will be examined in detail.

1.2. In its judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* of 8 April 2014, which was, inter alia, rendered after referral for a preliminary ruling by the Constitutional Court (*VfSlg. 19.702/2012*),

the Court of Justice of the European Union declared the Data Retention Directive as invalid, without limiting the temporal effect of the declaration of invalidity. The declaration of invalidity therefore has retroactive effect (cf. CJEU 13 May 1981, C-66/80, *International Chemical Corporation*, [1981] ECR 1191 [paragraph 13 et seqq.]). The Data Retention Directive has such been removed with *ex-tunc* effect from Union law (cf. generally, concerning the temporal effect of judgments of the Court of Justice of the European Union in preliminary ruling procedures by which Union law is declared invalid, e.g. *Kadelbach, Die Wirkungen von im Vorabentscheidungsverfahren ergangenen Urteilen, in: Holoubek/Lang [Hrsg.], Das EuGH-Verfahren in Steuersachen, 2000, 119 [126 et seqq.]; B. Schima, Das Vorabentscheidungsverfahren vor dem EuGH², 2004, 106 et seqq.; Öhlinger/Potacs, EU-Recht und staatliches Recht[5], 2014, 76 et seq.).*

1.3. A direct application of provisions of the Data Retention Directive or other provisions of Union law, which would at most lead the Constitutional Court to observe the primacy of application of Union law and which would affect in particular the admissibility of the individual applications G 59/2012 and G 62,70,71/2012 (cf. e.g. *VfSlg. 15.771/2000, 17.508/2005, 18.298/2007*), can therefore be ruled out.

1.4. Application G 47/2012:

1.4.1. Pursuant to Article 140 paragraph 1 subparagraph 2 of the Constitution *(B-VG*), the Constitutional Court decides on the unconstitutionality of a Federal act also on application by a province government. The application filed by the Government of the Province of Carinthia constitutes such an application.

1.4.2. The Constitutional Court has repeatedly held in judicial review proceedings instituted ex-officio as well as by application *(VfSlg. 13.965/1994* and further references*, 16.542/2002, 16.911/2003*) that the limits for repealing a provision of law to be reviewed for its constitutionality must, by necessity, be drawn so that, on the one hand, the content of the remaining part of the law is not completely altered and, on the other, all provisions which are inseparably linked to the passage to be repealed are equally covered.

[…]

1.4.4. Against this backdrop, the application by the Government of the Province of Carinthia is inadmissible, as the scope of the challenged legislation is too narrow. Given the fact that the applicant province government has challenged numerous provisions of the Telecommunications Act 2003 (*TKG* 2003) which it believes to be inseparably linked to data retention and in particular to section 102a *TKG* 2003, but not the provisions of the Code of Criminal Procedure (*StPO*) and of the Security Police Act (*SPG*) which govern the provision of information on retained data, it did not challenge all provisions which form an inseparable unit for assessing whether the provisions on data retention may be unconstitutional (cf. 0 below).

1.4.5. For this reason alone, the application by the Government of the Province of Carinthia is to be rejected on substantive grounds.

1.5. Application G 59/2012:

1.5.1. Pursuant to Article 140 paragraph 1 subparagraph 1 point (c) of the Constitution (*B-VG*), the Constitutional Court decides on the unconstitutionality of laws on application by a person maintaining that their rights have been directly infringed by such unconstitutionality, if the law became effective for that person without a court decision having been rendered or without an administrative ruling (*Bescheid*) having been issued. As the Constitutional Court has held in its established case law starting with *VfSlg. 8009/1977*, the eligibility to file an application rests on the precondition that the law directly interferes with the legal sphere of the person concerned and – if unconstitutional – infringes their rights. In such a case, the Constitutional Court is held to rely on the submissions made by the applicant and can merely examine whether the effects invoked by the applicant are such in nature as required by Article 140 paragraph 1 subparagraph 1 point (c) of the Constitution (*B-VG*) to give rise to the right to file an application (cf. e.g. *VfSlg. 11.730/1988, 15.863/2000, 16.088/2001, 16.120/2001).*

1.5.2. However, not every party addressed by a provision has *locus standi* to challenge the law. As an additional criterion, the law must directly interfere with the applicant's legal sphere. Such interference can be assumed only if its nature and extent are clearly determined by the law itself, if it actually and not just

potentially impairs the (legally protected) interests of the applicant, and if there is no other reasonable route available to avert the – allegedly – unlawful interference (*VfSlg. 11.868/1988, 15.632/1999, 16.616/2002, 16.891/2003).*

[…]

1.5.6.2. In the circumstances of the present case, the Constitutional Court cannot perceive any reasonable alternative which would be open to the second applicant to effectively counter the infringement of rights caused by the alleged unlawfulness of the challenged provisions:

[…]

1.5.6.8. The Constitutional Court has repeatedly held when ruling on individual applications filed under Articles 139 and 140 of the Constitution that individuals affected by a general legal norm are entitled to file an application for judicial review of an regulation or law in special, exceptional circumstances only, if it is generally possible to institute court or administrative proceedings which would ultimately allow them to induce the Constitutional Court to institute judicial review proceedings ex-officio; or else one would be faced with duplication in the system of legal protection, which would be incompatible with the principle of an individual application being a legal remedy on a merely subsidiary basis (cf. e.g. *VfSlg. 8312/1978, 11.344/1987, 15.786/2000, 18.182/2007, 19.126/2010).*

1.5.6.9. These special and exceptional circumstances are the following: The obligation to retain data pursuant to section 102a *TKG* 2003 and to provide information pursuant to section 135 paragraph 2a *StPO* and section 53 *SPG* generates a huge volume of data which are stored either with the providers of public communications services or (after such information has been provided) with the law-enforcement or criminal prosecution authorities. Besides, not only those providers with whom the second applicant had or has entered into a contract are under an obligation to retain data, but also the providers of the second applicant's "communication partners", i.e. those persons whom the second applicant would e.g. call or send e-mails (cf. section 102a paragraph 3 subparagraphs 1 and 3 *TKG* 2003; for mobile networks section 102a paragraph 3 subparagraph 6 *TKG* 2003; for e-mail services section 102a paragraph 4

subparagraphs 3 and 4 *TKG* 2003). The second applicant is confronted with a sheer unmanageable number of providers which may have stored his data pursuant to section 102a *TKG* 2003. For all practical purposes, it is impossible to determine which provider has stored or is storing which data in which periods on the basis of section 102a *TKG* 2003.

1.5.6.10. Moreover, if the second applicant were to institute legal proceedings for the deletion of the retained data concerning his person against a provider, providers would still continue to store data on the basis of section 102a *TKG* 2003. At the time the Constitutional Court would have to decide on an application pursuant to Article 89 paragraph 2 of the Constitution (*B-VG*), the data whose deletion the second applicant is seeking by way of court proceedings would have already been deleted, which would put in question the admissibility of the application.

1.5.6.11. By the seriousness of the impending disadvantage, these circumstances are equivalent to those in respect of which the Constitutional Court has held earlier that it would be unreasonable to resort to the – theoretically existing – alternative recourse (cf. *VfSlg. 11.853/1988, 12.379/1990, 15.786/2000*).

1.5.7. Given these inherent specifics of data retention, no other reasonable recourse was open to the second applicant than filing an individual application.

[…]

1.6. Application G 62,70,71/2012:

1.6.1. As regards the third applicant, nothing has emerged which would lead the Court to an assessment that would differ from that of the application G 59/2012 (see 1.5 above).

1.6.2. This application is equally admissible.

2. **On the merits**

In proceedings to review the constitutionality of a law pursuant to Article 140 of the Constitution (*B-VG*) which are initiated by application, the Constitutional Court must limit itself to addressing issues which have been raised (cf. *VfSlg. 12.691/1991, 13.471/1993, 14.895/1997, 16.824/2003*). Therefore, it must only assess whether the challenged provision is unconstitutional for the reasons set out in the justification of the application (*VfSlg. 15.193/1998, 16.374/2001, 16.538/2002, 16.929/2003*).

2.2. The standard of review:

2.2.1. In the applications filed, it is submitted that the challenged provisions violate section 1 *DSG* 2000, Article 8 ECHR, and Articles 7 and 8 of the Charter of Fundamental Rights.

2.2.2. As has been argued by the Constitutional Court earlier in its decision *VfSlg. 19.702/2012*, by which it submitted a reference for a preliminary ruling to the Court of Justice of the European Union, Federal constitutional law contains a fundamental right to data protection in its own right, in addition to Article 8 ECHR. The constitutional provision of section 1 *DSG* 2000 grants every natural and legal person the right to secrecy of their personal data, inasmuch as an interest deserving protection exists (section 1 paragraph 1 *DSG* 2000, see II.6 above). Section 1 paragraph 2 *DSG* 2000 contains a substantive legal reservation according to which, apart from the use of personal data in the vital interest of the data subject or with their consent, the right to secrecy may be limited only to protect the overriding legitimate interests of a third party, namely in case of an intervention by a public authority the restriction shall only be permitted based on the laws necessary for the reasons stated in Article 8(2) ECHR.

2.2.3. In terms of the legal base, section 1 paragraph 2 *DSG* 2000 stipulates, beyond Article 8(2) ECHR, that data which deserve special protection may only be used to safeguard important public interests provided that suitable safeguards for the protection of the data subject's interest in secrecy are laid down in law at the same time.

2.2.4. In its decision *VfSlg. 19.702/2012*, the Constitutional Court considered that the Data Retention Directive – this being the reason for the preliminary ruling procedure – could only be implemented in a manner which infringes the fundamental right set out in section 1 *DSG* 2000 and that, in consequence, the Constitutional Court could be barred from reviewing legal provisions governing data retention (cf. *VfSlg. 15.427/1999*). Since no latitude for implementation in conformity with the Constitution exists, the Constitutional Court argued that it would be barred from assessing the legal provision using section 1 *DSG* 2000 as a standard of review. With the Court of Justice of the European Union having declared the Directive invalid, this argument now has become void, so that section 1 *DSG* 2000 and Article 8 ECHR again form an absolute standard of review in judicial review proceedings.

2.2.5. This result concurs with the fact that the Court of Justice of the European Union felt it unnecessary to answer the questions on the interpretation of Articles 7, 8, 52 and 53 of the Charter submitted to it, given the invalidity of the Data Retention Directive (CJEU, *Digital Rights Ireland and Seitlinger and Others,* paragraph 72).

2.2.6. Not even Article 15(1) second sentence of Directive 2002/58/EC alters this result. It merely stipulates that Member States may adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. Such measures must "be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union" (Article 15(1) final sentence Directive 2002/58/EC). Article 15(2) of Directive 2002/58/EC stipulates that the provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to Directive 2002/58/EC and with regard to the individual rights derived from this Directive. This Directive does not, however, provide for more detailed provisions on how the restrictions set out in Article 15(1) second sentence of Directive 2002/58/EC are to be implemented, so that it must be assumed that the legislator enjoys wide discretion in implementation; precedence over national constitutional law and, in particular, the two specifically mentioned constitutionally guaranteed rights, is therefore to be ruled out.

2.2.7. Articles 7 and 8 of the Charter of Fundamental Rights may also be considered as a standard of review in these judicial review proceedings. As has been argued by the Constitutional Court in the referral for a preliminary ruling *VfSlg. 19.702/2012* and tying in with its earlier case law (*VfSlg. 19.632/2012*), the rights guaranteed by the Charter in its scope of application (Article 51(1) of the Charter) constitute a standard of review in judicial review proceedings, in particular in proceedings under Articles 139 and 140 of the Constitution (*B-VG*). This holds true at any rate if the guarantee accorded by the Charter corresponds, in its wording and degree of determination, to the constitutionally guaranteed rights laid down in the Austrian Federal Constitution. Legislative provisions which were adopted in order to transpose a directive constitute at any rate a case of implementation of Union law (*VfSlg. 19.632 /2012*). Even if the Data Retention Directive has now been declared invalid (with *ex-tunc* effect), the challenged provisions – specifically those promulgated in Federal Law Gazette *BGBl*. I 27/2011 – were enacted in implementing Union law, if only because they were adopted in the scope of application of Directive 2002/58/EC, precisely Article 15(1) of that Directive.

2.2.8. If, in using its discretionary scope in the implementation of Union law, the legislator creates provisions which also affect (another) constitutionally guaranteed right beside a fundamental right of the Charter, the Constitutional Court decides on the basis of this right, provided it has the same scope of application as the right under the Charter (*VfSlg. 19.632/2012*) and the limits for permissible interference by the legislator with the constitutionally guaranteed rights are drawn narrower, or at least not wider, than in the corresponding rights of the Charter. This can be assumed for Article 8 ECHR as well as for section 1 *DSG* 2000:

2.2.8.1. Article 8 ECHR qualifies the interpretation of Article 7 of the Charter in the sense that, pursuant to the explanations on Article 7 of the Charter , Article 7 "corresponds" to this Article and therefore "shall be the same" in "meaning and scope" (Article 52(3) of the Charter, to this effect also the references to the case law of the European Court of Human Rights in the judgment of the CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraphs 35, 47, 54 et seq.).

2.2.8.2. Section 1 *DSG* 2000 contains a substantive legal reservation, which draws the limits for interference with the fundamental right narrower than Article 8(2) ECHR. Besides the use of personal data in the vital interest of the data subject or with their consent, restrictions to the right to secrecy are permitted only to safeguard the overriding legitimate interests of another person; in the event of interferences by a public authority, such restriction shall only be permitted based on the laws necessary for the reasons stated in Article 8(2) ECHR.

As regards the legal base, section 1 paragraph 2 *DSG* 2000 stipulates beyond the scope of Article 8(2) ECHR that the use of data that deserve special protection may be provided for only in order to safeguard substantial public interests and that, at the same time, suitable safeguards for the protection of the data subject's interest in secrecy shall be provided for by law. Finally, this provision explicitly stipulates that even with permissible restrictions, interference with the fundamental right must use "only the least intrusive of all effective methods".

2.2.9. Consistent with the case law of the Constitutional Court, it follows from this provision that a stricter standard must be applied to the proportionality of an interference with the fundamental right to data protection pursuant to section 1 *DSG* 2000 than that which is derived from Article 8 ECHR (*VfSlg. 16.369/2001, 18.643/2008)*. This level of protection remains unaffected by the Charter also in those cases in which the legislator has discretion in the implementation of Union law (cf. Article 53 of the Charter; see 2.2.6 above). Against this backdrop, the challenged provisions must be assessed using Federal constitutional law, i.e. section 1 *DSG* 2000 and Article 8 ECHR, as a standard of review.

2.3. As regards the concerns raised against section 134 subparagraph 2a and section 135 paragraph 2a Code of Criminal Procedure (*StPO*), against section 53 paragraph 3a subparagraph 3 and section 53 paragraph 3b Security Police Act (*SPG*), and against section 102a Telecommunications Act 2003 (*TKG 2003*):

2.3.1. The applicants are seeking that section 102a *TKG* 2003 and others be repealed for infringing a right that is constitutionally guaranteed by section 1 *DSG* 2000. Section 134 subparagraph 2a and section 135 paragraph 2a *StPO* as well as section 53 paragraph 3a subparagraph 3 and section 53 paragraph 3b

*SPG*, they argue, must be "seen as forming a unit with the provisions governing the obligation to retain data (section 102a *TKG*) and the use of retained data (section 102b *TKG*, section 99 paragraph 5 subparagraphs 2 to 4 *TKG*)" (as submitted by the third applicant); these provisions would equally infringe the fundamental right at stake, in particular because the "possibilities of access" granted by the relevant provisions in the Code of Criminal Procedure and in the Security Police Act are excessive (submitted in particular by the second applicant).

2.2.3. Section 102a paragraph 1 *TKG* 2003 obliges providers of public communications services (cf. section 92 paragraph 3 subparagraph 1 *TKG* 2003) to store certain categories of data which were generated or processed in the course of providing public communications services (cf. section 102a paragraph 5 first sentence *TKG* 2003) "beyond the authorisation to store or process data pursuant to sections 96, 97, 99, 101 and 102" from the time of their generation or processing until six months after the communication is terminated. Pursuant to section 102a paragraph 1 final sentence *TKG* 2003, they are stored solely for the purpose of investigating, identifying and prosecuting criminal acts whose severity justifies an order pursuant section 135 paragraph 2a Code of Criminal Procedure (*StPO*).

2.3.3. Referring to section 135 paragraph 2 subparagraphs 2 to 4 *StPO*, section 135 paragraph 2a *StPO* states that information on retained data (section 134 subparagraph 2a *StPO*) may be provided if this is likely to help investigate a wilfully committed criminal act carrying a sentence of more than six months and if the owner of the technical device which was or will be the origin or target of communication explicitly consents to such information being provided (section 135 paragraph 2 subparagraph 2 *StPO*); if it is likely that the provision of information will 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 collect data about the accused (section 135 paragraph 2 subparagraph 3 *StPO*); or if, based on given facts, it can be expected that this will help identify the whereabouts of a fugitive or absent perpetrator who is strongly suspected of having wilfully committed a criminal act which carries a sentence of more than one year (section 135 paragraph 2 subparagraph 4 *StPO*). The provision of information on retained data

pursuant to section 135 paragraph 2a *StPO* requires an order from the public prosecutor's office based on a court authorisation (section 137 paragraph 1 *StPO*). Pursuant to section 87 *StPO*, a complaint may be lodged against such authorisation after it has been served on the person concerned (section 138 paragraph 5 *StPO*). Pursuant to section 147 paragraph 1 subparagraph 2a *StPO*, the commissioner for legal protection *(Rechtsschutzbeauftragter*) must examine and review the order, approval, authorisation and implementation of the provision of information on retained data pursuant to section 135 paragraph 2a *StPO*. The commissioner for legal protection has the right to lodge a complaint against the authorisation of an investigative measure pursuant to section 147 paragraph 1 subparagraph 2a *StPO* (section 147 paragraph 3 *StPO*). Once the investigative measure has been terminated, the commissioner for legal protection must be granted an opportunity to view the results in their entirety before they are filed. Moreover, he or she is entitled to apply for the full or partial erasure of results and to verify that these results were properly erased (section 147 paragraph 4 *StPO*).

2.3.4. Pursuant to section 53 paragraph 3a subparagraph 3 *SPG*, the law-enforcement authorities may request operators of public communications services to furnish information about the name and address of a user to whom an IP address was assigned at a given time, if such data is essential to prevent a specific hazard for the life, health or freedom of an individual in compliance with the general duty of rendering first assistance (section 19 *SPG*), to fend off a dangerous attack (section 16 paragraph 1 subsection 1 *SPG*), or to combat a criminal association (section 16 paragraph 1 subparagraph 2 *SPG*), "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 4 in conjunction with section 102a *TKG* 2003". Section 53 paragraph 3b *SPG* moreover entitles the law-enforcement authorities to request information from operators of public communications services concerning location data and the international mobile subscriber identity (IMSI) of the terminal equipment carried by a person at risk or the person accompanying them, "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 3 in conjunction with section 102a *TKG* 2003".

As a precondition for information to be provided pursuant to section 53 paragraph 3b *SPG*, there must be a suspicion, based on given facts, of a current danger to the life, health or freedom of a person, and the law-enforcement authorities must intervene in complying with their duty of rendering first general assistance or avert dangers (section 53 paragraph 3b *SPG*). Judicial authorisation is not required whenever the law-enforcement authorities intervene based on the above provisions. Section 91c paragraph 1 *SPG* stipulates that the commissioner for legal protection must be "notified as soon as possible" of requests for information. He or she has responsibility for reviewing such notifications (section 91c paragraph 1 final sentence *SPG*).

2.3.5. Section 1 paragraph 1 *DSG* 2000 provides that every person has a right to secrecy of their personal data if they have an interest deserving protection, in particular as regards the right to respect for private and family life. By virtue of the statutory reservation of section 1 paragraph 2 *DSG* 2000, this fundamental right may be restricted (unless the data subject has a vital interest in, or consents to, the use of their personal data), in the case of an interference of a public authority based on the laws which are necessary for the reasons stated in Article 8(2) ECHR and which determine in a sufficiently precise (i.e. generally predictable) manner under which conditions the collection and use of personal data is permitted for the performance of specific administrative tasks (cf. *VfSlg. 16.369/2001, 18.146/2007, 18.963/2009, 18.975/2009, 19.657/2012, 19.738/2013*).

Legal restrictions of the fundamental right to data protection must be proportionate on weighing the seriousness of the interference and the importance of the objectives pursued (cf. also Article 8 in conjunction with Article 52(1) Charter and CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraphs 38, 47, 69 and ECtHR 4 12 2008 [GC], case *S. and Marper*, appl. 30.562/04, EuGRZ 2009, 299 [paragraph 101]). Such laws may provide for the use of data that deserve special protection only in order to safeguard substantial public interests and shall at the same time provide suitable safeguards for the protection of the data subjects' interest in secrecy (section 1 paragraph 2 second sentence *DSG* 2000).

The final sentence of section 1 paragraph 2 *DSG* 2000 states that, also with restrictions which are permissible pursuant to Article 8(2) ECHR, the fundamental right may only be interfered with if the least intrusive of all effective methods is used. The legislator must therefore adopt substantive legislative provisions which meet these requirements in terms of specifically defining and limiting cases of permissible interferences with the fundamental right to data protection (cf. e.g. *VfSlg. 18.643/2008, 19.657/2012, 19.659/2012, 19.738/2013*).

2.3.6. The fundamental right to data protection guaranteed in section 1 *DSG* 2000 provides for a constitutional safeguard against collecting personal data (*VfSlg. 12.228/1989, 12.880/1991, 16.369/2001).* The data to be retained pursuant to section 102a *TKG* 2003 and to be provided pursuant to section 135 paragraph 2a *StPO* and section 53 paragraph 3a subparagraph 3 and section 53 paragraph 3b *SPG* are personal data within the meaning of section 1 paragraph 1 *DSG* 2000. Specifically, all the data categories listed in paragraphs 2 to 4 of section 102a *TKG* 2003 are ones by which the identity of the data subject is determined or is at least determinable. Given the possibility of interlinking data with other information, which was also brought up by the applicants (e.g. the conclusions which may be inferred from frequent calls of a given subscriber number) there is at any rate an interest in secrecy of the data concerned within the meaning of section 1 paragraph 1 *DSG* 2000.

2.4.7. The obligation imposed on providers of public communications services by section 102a paragraph 1 *TKG* 2003 to retain data pursuant to paragraphs 2 to 4 of this provision interferes with the fundamental right to data protection of the users of public communications services under section 1 *DSG* 2000 and the right to respect for private and family life laid down in Article 8 ECHR (*VfSlg. 19.738/2013*; cf. Explanatory notes to the government bill of the *TKG* Amendment, Federal Law Gazette *BGBl*. I 27/2011, 1074 *BlgNR 24. GP*, 21; cf. also *Feiel, Datenspeicherung auf Vorrat und Grundrechtskonformität, jusIT 2008, 97 [99];* on interference with Article 8 ECHR also *VfSlg. 12.689/1991;* ECtHR 26.3.1987, case *Leander,* appl. 9248/81 [paragraph 48]; ECtHR 16 February 2000 [GC], case *Amann,* appl. 27.798/95, *ÖJZ* 2001, 71 [paragraph 65 et seqq.]; ECtHR 4 May 2000 [GC], case *Rotaru,* appl. 28.341/95, *ÖJZ* 2001, 74 [paragraph 43]; ECtHR 3 April 2007, case *Copland*, appl. 62.617/00, *EuGRZ* 2007, 415

[paragraph 43 et seq.]; ECtHR, case *S. and Marper*, paragraph 67; *Kolb, Vorratsdatenspeicherung, 2011, 113).*

2.3.7.1. Even though the data are stored by providers of public communications services – i.e. by privates – who are obliged to retain data under section 102a *TKG* 2003, the legislator is still infringing the rights guaranteed by section 1 *DSG* 2000 and Article 8 ECHR. A "provider of a communications service" includes anyone who offers a communications service (section 92 paragraph 3 first half sentence in conjunction with section 3 subparagraph 9 *TKG* 2003), but who – unlike the "operator of a communications service" (section 3 subparagraph 3 *TKG* 2003) – does not necessarily control all functions of that service (*Steinmaurer*, *in: Stratil [Hrsg.], TKG[4], 2013, section 92 note 6*). The *TKG* 2003 assumes that both "providers" and "operators" of communications services are (private) companies (see section 1 paragraph 1, section 34 et seqq. *TKG* 2003).

2.3.7.2. These companies do not enjoy any discretion as regards the obligation to retain data imposed by section 102a *TKG* 2003. Pursuant to section 109 paragraph 3 subparagraph 22 *TKG* 2003, they would commit an administrative offence if they failed to store data in contravention of section 102a *TKG* 2003.

2.3.8. The storage of data based on the obligation stipulated by section 102a *TKG* 2003 and access to these data ("provision of information") by law-enforcement and criminal prosecution authorities – in particular on the basis of section 135 paragraph 2a *StPO* and of section 53 paragraph 3a subparagraph 3 and of section 53 paragraph 3b *SPG* – constitutes an interference with the fundamental right to data protection (section 1 *DSG* 2000) and with the right to respect for private and family life enshrined in Article 8 ECHR (cf. e.g. *VfGH* 01/10/2013, G 2/2013 with further references; as regards interference with Article 8 ECHR, furthermore ECtHR, case *Leander*, paragraph 48; ECtHR, case *Rotaru*, paragraph 46; ECtHR 29 June 2006 [admissibility decision], case *Weber and Saravia*, appl. 54.934/00 [paragraph 79]).

2.3.9. Provisions like those challenged which severely interfere with a fundamental right may be allowed to combat serious crime, if they comply with the strict requirements of section 1 *DSG* 2000 and of Article 8 ECHR. Whether such interference is admissible in terms of section 1 paragraph 2 *DSG* 2000 and

Article 8(2) ECHR depends on the specific conditions governing the retention of data and the requirements as to their erasure, as well as on the legal safeguards determining the possibilities of access to such data by government authorities and privates. The challenged provisions of the *TKG* 2003, the *StPO* and the *SPG* do not satisfy these requirements:

2.3.10. The provisions on data retention in the *StPO* and in the *SPG*, including those on the provision of information on retained data, serve to attain the goals set out in Article 8(2) ECHR, in particular the maintenance of public order and peace and the protection of rights and freedoms of others. Within its scope of discretion, the legislator could, moreover, justifiably assume that the rules governing data retention are suitable in abstract terms to reach these goals (cf. also CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraphs 44 and 49 as regards Articles 7 and 8 of the Charter of Fundamental Rights).

2.3.11. As a further prerequisite for the proportionality and thus the admissibility of the interference, the severity of the specific interference must not exceed the weight and importance of the goals to be achieved through data retention.

2.3.11.1. The understanding that the fundamental right to data protection in a democratic society – in the sphere of protection that is relevant here – is aimed at facilitating and safeguarding confidential communication between individuals underlies any assessment of the proportionality of data retention. Individuals and their unhindered personal development rely not only on public but also on confidential communication within society; perceived as a right of the individual and a condition of a society, freedom is determined by the quality of informational relations (cf. *Berka, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT, 2012, volume I/1, 22*).

2.3.11.2. The weight and importance of the goals to be achieved by data retention, as also expressed by the legislator by a limitation of purpose set out in section 102a paragraph 1 final sentence *TKG* 2003, are considerable. But even if these provisions, as evidenced by the wording of paragraph 1, serve an important public interest (see 2.3.10 above), the legislator must, considering the "spread" of an interference (see 2.3.14.3 below), the scope and nature of the data concerned (see 2.3.14.5 below) and the resultant severity of the

interference with the right to informational self-determination (it is possible to access data which, if interlinked, not only allow to draw up movement profiles, but also to infer personal preferences and acquaintances of an individual; see 2.3.14.5 below), adopt appropriate rules to ensure that these data are being made accessible in individual cases to criminal prosecution authorities only if an equally important public interest exists, and only subject to judicial control. In this context, one should bear in mind that, over the past two decades, the rapidly spreading use of "new" communication technologies (e.g. mobile telephony, e-mail, sharing of information via the World Wide Web, etc.) has brought on considerable challenges for state action in many respects – not least in fighting crime, which data retention is to serve. The case law of the Constitutional Court has always taken account of this changed environment governing police investigations (cf. e.g. *VfSlg. 16.149/2001, 16.150/2001, 18.830/2009, 18.831/2009, 19.657/2012*). At the same time, one must not forget that expanded technical possibilities necessitate adequate action to counter the risks for the freedom of the individual which this expansion brings in its wake.

2.3.11.3. In its judgment in the case *Digital Rights Ireland and Seitlinger and Others,* the Court of Justice of the European Union has emphasised that the Data Retention Directive fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecution concerning criminal offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference (paragraph 60). The CJEU argued that, on the contrary, the Data Retention Directive simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

2.3.11.4. Commenting on the judgment of the Court of Justice of the European Union in the case *Digital Rights Ireland and Seitlinger and Others*, the Federal Government has emphasised that the provision of information on retained data against the will of the "surveilled user" is admissible only if this is expected to help investigate a wilfully committed criminal act carrying a sentence of more than one year. Providing information on retained data in respect of the facts listed in section 135 paragraph 2 subparagraph 2 *StPO* would "ultimately" aim at

offering stalking victims (section 107a StGB [Criminal Code]) a possibility to effectively prosecute offenders.

2.3.11.5. The submission by the Federal Government that the provisions of section 135 paragraph 2a in conjunction with section 135 paragraph 2 subparagraphs 2 to 4 *StPO* are sufficiently differentiated and therefore proportionate is mistaken. As the Court of Justice of the European Union has underlined, the Data Retention Directive is to help fight serious crime (CJEU, *Digital Rights Ireland und Seitlinger and Others*, paragraph 60). The very same holds for the legal provisions by which the Directive is transposed in the *TKG* 2003, the *StPO* and in the *SPG*. The legislator is at liberty to target the investigation of crimes which are punishable by a given sentence when allowing the provision of information on retained data. In addition, however, it would have to ensure that the severity of the criminal offence – as expressed by the threatened punishment – justifies, in a given case, the interference with the constitutionally guaranteed rights of those who are affected by the provision of information on "their" retained data. In this respect, the list of offences covered by section 135 paragraph 2a in conjunction with section 135 paragraph 2 subparagraphs 2 to 4 *StPO* is too undifferentiated and therefore too broad in scope. It does not ensure that requests for information are admissible only for offences which carry a severe punishment (e.g. section 207a StGB) or for the investigation of which the use of retained data is essential in view of the way in which they are committed (e.g. section 107a paragraph 1 in conjunction with paragraph 2 subparagraph 2 StGB).

2.3.11.6. Regardless of the reservation that the provision of information on retained data is subject to court approval (section 135 paragraph 2a in conjunction with section 137 paragraph 1 *StPO*), to the involvement of the commissioner for legal protection and the latter's right to file a complaint pursuant to section 147 paragraph 1 subparagraph 2a and paragraph 3 second sentence *StPO*, the proportionality of the retention of data is not ensured – if alone for the fact that section 135 paragraph 2a *StPO* in conjunction with sections 102a, 102b paragraph 1 *TKG* 2003 does not ensure that information on retained data is provided only if such data help prosecuting and investigating criminal offences which, in a given case, severely jeopardise the objectives set

out in Article 8(2) ECHR and which would justify such interference. Section 135 paragraph 2a *StPO* therefore is in violation of section 1 paragraph 2 *DSG* 2000.

2.3.12. Section 134 subparagraph 2a *StPO*, which defines the term "information on retained data" for the scope of application of the *StPO*, is inseparably linked to section 135 paragraph 2a *StPO* and hence to be repealed for that reason.

2.3.13. The second and third applicants have applied that the phrase "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 4 in conjunction with section 102a *TKG* 2003," in section 53 paragraph 3a subparagraph 3 *SPG* and, in section 53 paragraph 2b *SPG*, the phrase "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 3 in conjunction with section 102a *TKG* 2003," be repealed as unconstitutional.

2.3.13.1. Pursuant to the *SPG* – and unlike the *StPO* – the provision of information on retained data does not require judicial approval. The involvement of the commissioner for legal protection pursuant to section 91c paragraph 1 *SPG*, who is responsible for "reviewing such notifications made according to this paragraph" – in other words for an *ex-post* review – (section 91c paragraph 1 final sentence *SPG*), is at any rate insufficient.

2.3.13.2. Further, the concerns raised above in respect of section 135 paragraph 2a *StPO* also apply to the challenged phrases in the listed provisions of the *SPG*. The powers of the law-enforcement authorities to access retained data are in no way limited to the seriousness of an impending criminal offence. Only negligence offences are not covered by these powers.

2.3.13.3. This does not satisfy the requirements as to the proportionality of an interference with the fundamental right to data protection by access pursuant to section 53 paragraph 3a subparagraph 3 or section 53 paragraph 3b *SPG*. The challenged phrases in these provisions are therefore to be repealed as unconstitutional.

2.3.13.4. Under section 53 paragraph 3a subparagraph 3 *SPG*, the law-enforcement authorities may "only" provide the name and address of a user to

whom an IP address was assigned at a given moment in time and "only" location data under section 53 paragraph 3b *SPG* which were retained as imposed by section 102a *TKG* 2003. This does not alter the result in the light of the above elaborations under III.2.3.13 (cf. *Berka*, ibid, 141, referring to the decision of the German Federal Constitutional Court *BVerfGE* 125, 260).

2.3.14. As regards the requirements of the provision of information, section 102a *TKG* 2003 also proves to be unconstitutional. The provisions relating to the provision of information on retained data, together with the provisions of the *TKG* 2003 which require the storage of retained data, constitute a severe interference with the fundamental, constitutionally guaranteed right to data protection laid down in section 1 *DSG* 2000 of the "users" (section 92 paragraph 3 subparagraph 2 *TKG* 2003) of public communications services or data subjects otherwise affected by data retention, and therefore also of the second and third applicants (see above 2.3.7).

2.3.14.1. Neither did the applicants maintain that storing and processing data pursuant to section 102a *TKG* 2003 would be totally unsuitable for helping to investigate serious criminal offences, nor did this emerge in the oral hearing. Whether an interference with a fundamental right is suitable must be therefore assessed in abstract terms, since it does not presuppose any given, concrete percentage rate as to the frequency of this legal provision being applied in practice, nor a defined "success rate" in the investigation of criminal offences. It suffices that the legislator could rightly assume that the measure is suitable to effectively serve the intended "purpose" (cf. in this context recital 7 of the Data Retention Directive, which has been declared invalid; CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 43). The Constitutional Court is not held to examine in these proceedings whether each individual datum to be retained pursuant to section 102a *TKG* 2003 is suitable for reaching that purpose. *Ab initio*, it is by no means established that the storage of all data for retention and processing under section 102a *TKG* 2003 in implementing the Data Retention Directive now declared invalid, is proportionate. The mere possibility of using new technology in addition to existing surveillance measures does not *a priori* justify an interference with the sphere of freedom protected by section 1 *DSG* 2000 and Article 8 ECHR.

2.3.14.2. In its decision *VfSlg. 19.702/2012*, the Constitutional Court has emphasised earlier that the "spread" of data being retained without a given occasion exceeds that of the interferences with the legal sphere protected by section 1 *DSG* 2000 it had to assess in its case law to date (cf. decision of the German Federal Constitutional Court *BVerfGE* 125, 260 [318 et seqq.]) in regard of the circle of persons affected, the scope and nature of the data, the tasks for which the storage of data was ordered, as well as the modalities of data use.

2.3.14.3. As to the targeted individuals, it is essentially users of fixed lines, mobile communication, Internet access and e-mail services (section 92 paragraph 3 subparagraphs 14 and 15 *TKG* 2003) and hence large parts of the Austrian population who are affected. In late 2013, for instance, every company had two fixed-line subscriptions on average and more than one in two households had one such subscription. On average, each inhabitant had 1.5 SIM cards for mobile telephony. Some 60 % of all households and companies had Internet access via mobile or fixed broadband, the broadband market penetration rate for smart phone tariffs was 87 % for households and companies (see RTR Telekom Monitor Annual Report 2013 on the use of fixed telephony and mobile telephony and the Internet in Austria https://www.rtr.at/en/komp/TKMonitor_2013/32128_TM_Annual_Review_2013.pdf).
The obligation to retain data pursuant to section 102a *TKG* 2003 such affects virtually the entire population (along these lines also CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 56).

2.3.14.4. In its decision *VfSlg. 19.702/2012*, the Constitutional Court held earlier that data retention affects almost exclusively persons who do not give rise to a cause for data retention – meaning that nothing in their conduct would require state intervention (cf. also CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 58). On the contrary, the overwhelming majority of the population uses public communications services to exercise their fundamental rights, i.e. in particular the freedom of expression, information and communication.

The second applicant maintained that he has never been criminally convicted before. This holds true for practically everyone affected by data retention. Considering this majority, the limitation of the right to secrecy of their personal

data within the meaning of section 1 paragraph 1 *DSG* 2000 and their right to data erasure in section 1 paragraph 3 *DSG* 2000 carries overwhelming weight.

2.3.14.5. As to the scope and nature of data, the obligation to retain data in section 102a *TKG* 2003 governs defined "traffic" and "location data" which are generated or processed in the course of the provision of public communications services. Traffic data are "any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof" (cf. section 92 paragraph 3 subparagraph 4 *TKG* 2003). Location data are "any data processed in a communications network or by a communications service, indicating the geographic position of the telecommunications terminal equipment of a user of a publicly available communications service; in the case of fixed-link telecommunications terminal equipment, location data refer to the address of the equipment" (cf. section 92 paragraph 3 subparagraph 6 *TKG* 2003). Section 102a paragraph 7 *TKG* 2003 explicitly forbids storing the contents of a communication, in particular data on addresses retrieved on the Internet.

Nevertheless, one cannot preclude that, contrary to the right to secrecy of personal data guaranteed by section 1 paragraph 1 *DSG* 2000, conclusions may be inferred from the retained data whenever information on retained data is provided pursuant to section 135 paragraph 2a *StPO* and section 53 *SPG*. In this respect, the possibility of interlinking data which were collected in different contexts must be taken into account (*Berka,* ibid, 76 and 111 et seq.). Considering the scope and nature of the retained data, the interference qualifies as particularly serious.

2.3.14.6. Moreover one must not forget that, given the vast number of providers of public communications services and therefore the vast number of parties obliged to store data, an extremely wide circle of persons potentially has access to data retained pursuant to section 102a *TKG* 2003. When weighing the seriousness of the interference, the potential for abuse which exists in this respect must be taken into account (cf. decision of the German Federal Constitutional Court *BVerfGE* 125, 260 [320]). On the one hand, the legislator has made provisions for that risk which exceed the requirements of the Data Retention Directive now found defective by the Court of Justice of the European

Union (cf. in particular the explicit obligation of data encryption set out in section 94 paragraph 4 *TKG* 2003 and the technical and organisational measures provided for in the Data Safety Regulation [*Datensicherheitsverordnung, DSVO*], which was issued on the basis of section 94 paragraph 4 *TKG* 2003, and the less far-reaching provision of Article 7 of the Data Retention Directive now declared invalid). Furthermore, section 109 *TKG* 2003 contains penal provisions designed to prevent abuse. On the other hand, however, specific provisions that would penalise the abuse of retained data by the providers who are under an obligation to store these data are lacking (cf. in contrast section 301 paragraph 3 StGB concerning notifications on the content of query results):

2.3.14.7. In its decision *VfSlg. 19.702/2012* on a referral for a preliminary ruling to the Court of Justice of the European Union, the Constitutional Court explicitly pointed to the heightened risk of abuse inherent in data retention. Given the vast number of providers of telecommunications services and thus the vast number of parties who are obliged to store data, an extremely wide circle of persons has access to these traffic data which must be retained for at least six months. The Court of Justice of the European Union reached the conclusion (CJEU, *Digital Rights Ireland and Seitlinger and Others*, paragraph 66) that Article 8 of the Charter results in a need to establish safeguards for retained data to be effectively protected against the risks of abuse as well as against unauthorised access and unlawful use. The same requirement exists under Article 8 ECHR and section 1 *DSG* 2000.

Section 102c *TKG* 2003 contains only isolated provisions on the safety of retained data and on access logging. Section 109 paragraph 3 *TKG* 2003 moreover contains administrative penal provisions (penalty of a fine of up to EUR 37,000) for cases where data is not deleted in violation of section 102a paragraph 8 *TKG* 2003 (subparagraph 23), where information on data is provided in the absence of a court authorisation in violation of section 102b *TKG* 2003 (subparagraph 24), and where data are transmitted over a communications network in unencrypted form in violation of section 102b *TKG* 2003 (subparagraph 25).

First it is important to note that (if there is no criminally punishable offence) the "mere" unauthorised use of data which are stored for retention is not punishable

by an administrative fine so that, in this respect, the abuse of these data is not sanctioned by the means of (administrative) criminal law. Moreover, the oral hearing has revealed that the Data Protection Commission and the Data Protection Authority have not acted to review compliance with these provisions since the enactment of the provisions on data retention.

2.3.15. Disregarding the fact that the legislator allows the storage of data pursuant to 102a *TKG* 2003, even though explicitly and exclusively for the purpose of investigating, identifying and prosecuting criminal acts whose severity justifies an order pursuant to section 135 paragraph 2a *StPO* (section 102a paragraph 1 final sentence *TKG* 2003), and thereby creates a legally defined purpose, the storage as such constitutes an interference which carries specific weight.

2.3.15.1. It must be factored into account that the right of erasure which is part of the fundamental right to data protection pursuant to section 1 paragraph 3 *DSG* 2000 (cf. e.g. *VfSlg. 16.150/2001*) does not exist for the period of six or seven months required by section 102a *TKG* 2003 (section 102a paragraph 8 *TKG* 2003) for the data of those persons who do not give a cause for storage and are therefore in no way related to the purpose of storage stipulated in section 102a paragraph 1 final sentence *TKG* 2003. What is more, requests for erasure can only be addressed to such providers obliged to retain data of which the person concerned knows that they have retained their data. The right to erasure can equally not be exercised vis-à-vis providers who have retained data concerning a person, but of which that person is not aware.

2.3.15.2. The right to erasure pursuant to section 1 paragraph 4 *DSG* 2000 can be restricted only under the conditions of section 1 paragraph 2 *DSG* 2000, similar to the restriction of the right pursuant to section 1 paragraph 1 *DSG* 2000. Following the case law of the Constitutional Court (cf. e.g. *VfSlg. 12.768/1991* as regards section 1 *DSG* 1978), the right to erasure pursuant to section 1 paragraph 3 *DSG* 2000 (only) requires legal provisions which grant a concrete right to erasure. It is, however, contrary to any interpretation of such provisions which do not account for section 1 paragraph 3 *DSG* 2000 or which restrict the right to erasure in a way that does not meet the requirements of section 1 paragraph 2 *DSG* 2000.

2.3.15.3. Further, the obligation to store data pursuant to section 102a *TKG* 2003 becomes totally void of purpose – defined specifically in section 102a paragraph 1 final sentence *TKG* 2003 in respect of section 135 paragraph 2a *StPO* – due to the unconstitutionality and repeal of section 135 paragraph 2a *StPO* and the challenged phrases in the stated provisions of the *SPG* (see 2.3.11.6 and 2.3.13.3 above). Retaining data without a specific purpose, even if for a short period of time only, would at any rate be unconstitutional (cf. in a different context *Pernthaler, Die Verfassungsmäßigkeit des Bundesgesetzes über das land- und forstwirtschaftliche Betriebsinformationssystem [LFBIS-Gesetz] unter dem Gesichtswinkel der bundesstaatlichen Kompetenzverteilung und Verwaltungsorganisation, in: Funk/Pernthaler, Verfassungsfragen des land- und forstwirtschaftlichen Informationswesens, 1982, 51 [66]).* Therefore, section 102a *TKG* 2003 – like the Data Retention Directive – does not satisfy the requirement of a relationship which must exist between data whose retention is being provided for and a threat to public security (CJEU, *Digital Rights Ireland and Seitlinger and Others,* paragraph 59).

2.3.16. Ultimately, the provisions governing data erasure are not determined in a way that would satisfy the requirement of a legal base within the meaning of section 1 paragraph 2 *DSG* 2000. Specifically, it is unclear whether the data retained pursuant to section 102a paragraph 1 *TKG* 2003 are to be erased irreversibly (cf. in this context Article 7(d) of the Data Retention Directive declared invalid: "the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.").

2.3.16.1. Given the seriousness of the interference, the provisions on data retention – in particular section 94 paragraph 4, section 102a paragraph 8, section 102c *TKG* 2003 and the Data Security Regulation (*Datensicherheits-verordnung, DSVO*) issued on the basis of section 94 paragraph 4 and section 102c *TKG* 2003 – all lack provisions which would clarify for those affected by data retention and those obliged to store data that the "erasure" of retained data must preclude their recoverability (see along these lines on section 4 subparagraph 9 *DSG* 2000, Supreme Court OGH, 15 April 2010, *6 Ob 41/10p)*. For that matter, it makes no difference that, in practice, providers "overwrite" retained data at regular intervals, presumably for economic reasons, and thereby ultimately prevent their recoverability, and that courts and authorities

"physically" delete data in respect of which information has been provided, as evidenced by the submissions in the oral hearing before the Constitutional Court. "Erasure" in terms of merely preventing access to data which continue to exist (and are still recoverable) does not suffice to meet the strict constitutional requirements as elaborated (see 2.2.8.2 above). This being not precisely clarified by section 102a paragraph 8 *TKG* 2003 and by other provisions, any intervention pursuant to section 102a paragraph 1 *TKG* 2003 does not meet the requirement of a sufficiently precise legal base (section 1 paragraph 2 *DSG* 2000).

2.3.16.2. The legal base is equally inadequate regarding the duties of operators and authorities in the context of so-called "always-on services" (cf. Explanations on the government bill for the *TKG* amendment, Federal Law Gazette *BGBl*. I 27/2011, 1074 *BlgNR 24. GP*, 23). If an Internet access service is operated and used as an "always-on service", the question arises when a "communication" is considered terminated within the meaning of section 102a paragraph 1 *TKG* 2003. In the oral hearing before the Constitutional Court, the Federal Government has argued that section 102a paragraph 1 and section 102a paragraph 2 *TKG* 2003 are to be interpreted in a "constitutionally conforming" manner in that communication with Internet access services is to be considered terminated within the meaning of section 102a paragraph 1 *TKG* 2003 on withdrawal of the public IP address by the provider. Therefore, the data pursuant to section 102a paragraph 2 *TKG* 2003 would have to be stored for six months after the withdrawal of a public IP address by the provider.

2.3.16.3. Even if the interpretation as described may lead to a practicable result, the mere possibility of such an interpretation cannot replace the degree of determinateness of the interference with a fundamental right, so that, also in this case, the strict requirements as to a legal base for interferences with the fundamental right to data protection are not satisfied (see 2.2.8.2 above).

2.3.17. In the final analysis, the applicants are right in claiming that the provisions are not proportionate in their overall context: the limitations of this fundamental right to data protection pursuant to the statutory reservation of section 1 paragraph 2 *DSG* 2000 would be permissible only on the basis of laws which are required on the grounds set out in Article 8(2) ECHR and which are sufficiently precise, in other words lay down, in a manner that is predictable for

everyone, under which conditions personal data may be collected or used for performing specific administrative tasks. Statutory limitations of the fundamental right to data protection must be the least intrusive means to attain given objectives and must be proportionate when weighing the seriousness of the interference against the importance of the objectives to be reached.

For the above reasons, the provisions governing data retention (section 135 paragraph 2a *StPO* in conjunction with section 102a *TKG* 2003, section 53 paragraph 3a subparagraph 3 *SPG* in conjunction with section 102a *TKG* 2003, section 53 paragraph 3b *SPG* in conjunction with section 102a *TKG* 2003) do not satisfy these requirements when assessed in an overall context.

2.4. Concerning the submission relating to other provisions of the *TKG* 2003:

The second and third applicants are seeking that further provisions of the *TKG* 2003 be repealed for being inseparably linked to section 102a *TKG* 2003, and have filed the corresponding applications to repeal specified provisions fully or*, in eventu*, phrases of the provisions which they have specified in detail.

2.4.1. Section 102b ("Information on retained data") and section 102c paragraphs 2, 3 and 6 *TKG* 2003 are to be repealed since they are inseparably linked to section 102a *TKG* 2003. This equally applies to section 92 paragraph 3 subparagraph 6b (legal definition of the term "retained data") and to subparagraphs 22, 23, 24, 25 and 26 in section 109 paragraph 3 *TKG* 2003 (administrative penal regulations), which are to be repealed.

2.4.2. Moreover, the following phrases are to be repealed because they are inseparably linked to section 102a *TKG* 2003:

In section 93 paragraph 3 *TKG* 2003, the phrase "including retained data"; in section 94 paragraph 1 *TKG* 2003, the phrase "including information on retained data"; in section 94 paragraph 2 *TKG* 2003, the phrase "including information on retained data"; in section 94 paragraph 4 *TKG* 2003, the phrases "including the transmission of retained data," and "as well as further specifications regarding storage of the logs prepared pursuant to section 102c"; in section 98 paragraph 2 *TKG* 2003, the phrase ", even in cases where access to data retained in

accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose"; in section 99 paragraph 5 subparagraph 2 *TKG* 2003, the phrase ", even those stored as retained data pursuant to section 102a paragraph 2 subparagraph 1, paragraph 3 subparagraph 6 points (a) and (b) or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5 for a maximum of six months prior to the query"; in section 99 paragraph 5 subparagraph 3 *TKG* 2003, the phrase ", even in cases where access to data retained in accordance with section 102a paragraph 3 subparagraph 6 point (d) is necessary for this purpose"; in section 99 paragraph 5 subparagraph 4 *TKG* 2003, the phrases "even" and "in accordance with section 102a paragraph 2 subparagraph 1 or section 102a paragraph 4 subparagraphs 1, 2, 3 and 5".

2.5. In the light of this outcome, the applicants' submission that the challenged provisions also violate other constitutionally guaranteed rights need not be dealt with.

## VI. Result

3. Section 135 paragraph 2a *StPO*, the phrases "even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 4 in conjunction with section 102a *TKG* 2003," in section 53 paragraph 3a subparagraph 3 *SPG* and ", even if the use of retained data is necessary for such purpose pursuant to section 99 paragraph 5 subparagraph 3 in conjunction with section 102a *TKG* 2003," in section 53 paragraph 3b *SPG*, and section 102a *TKG* 2003, and the provisions of the *StPO* and the *TKG* 2003 or parts thereof set out in detail in the dictum, which are inseparably linked to the stated provisions, are therefore repealed as unconstitutional.

[…]

Vienna, 27 June 2014
The President:
HOLZINGER

Recording clerk:
SIMON