Extract: Decision G 47/2012 e.a. regarding data retention

I. Background

1. Basing itself on its decision of 27 March 2012, the government of the Province of Carinthia filed an application with the Constitutional Court on 6 April 2012 according to Art. 140 (1) of the Federal Constitutional Act (*'Bundesverfassungsgesetz', B-VG*) seeking the annulment of explicitly listed provisions of the Telecommunications Act ('*Telekommunikationsgesetz 2003', TKG 2003*) (G 47/12), inter alia, of S 102a, which was inserted by the amendment Federal Law Gazette BGBl. I 27/2011.

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

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

4. The application of 11,129 other individuals was rejected by the Constitutional Court in the decision of 10 June 2014 (G 62/2012-36, G 70/2012-30, G 71/2012-26).

5. With decision of the 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 review proceedings and referred the following questions to the Court of Justice of the European Union for a preliminary ruling according to Art. 267 TFEU:

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

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

2. 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 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 purposes 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 relation 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) 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting 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 that latter article?'

6. The Court of Justice of the European Union joined the preliminary ruling request of the Constitutional Court with a corresponding request of the Irish High Court. With the judgment of the Grand Chamber in the Joined Cases C-293/12 and C-594/12, Digital Rights Ireland und Seitlinger and others of 8 April 2014 the Court of Justice of the European Union found that the Data Retention Directive was invalid.

7. On 12 June 2014 the Constitutional Court held a public hearing where the applying provincial government, the second and third applicants or their representatives and the representatives of the Federal Government submitted their opinions particularly to questions concerning the technical implementation of the data retention obligation, the scope of the affected services and the range of offenses for which in practice requests for information are directed at the providers. At the hearing the question was discussed to what extent an inseparable link exists between the contested provisions of TKG 2003, on the one hand, and the provisions of StPO as well as SPG relating to data retention on the other hand.

II. National Law

1. S 102a Telecommunications Act 2003 (*'Telekommunikationsgesetz 2003', TKG 2003*) which obliges providers of public communication services to store explicitly listed data, reads as follows:

Data retention

Section 102a (1) Beyond the authorisation to store or process data pursuant to S 96, 97, 99, 101 and 102, providers of public communications services shall store data in accordance with paras. 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 S 135 para. 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 para. 1 applies only to those data pursuant to paras 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 para. 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 para. 1 does not apply to those providers whose undertakings are exempt from the financing contribution requirement pursuant to S 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 S 99 para. 2, once the retention period has ended, the data to be stored pursuant to para. 1 are to be deleted without delay, at the latest within one month after the end of the retention period. The provision of information after the end of the retention period shall not be permissible.

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

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

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

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

5. S 135 Code of Criminal Procedure (*"Strafprozessordnung")* Federal Law Gazette, BGBl. 631/1975 as amended by Federal Law Gazette BGBl. I 33/2011, reads as follows:

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

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

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

(2a) The provision of information on retained data (S 102a and S 102b TKG) shall be admissible in the cases enumerated in para. 2, sub-paras. 2 to 4.

(3) Surveillance of communications shall be admissible,
1. in the cases of para. 2 (1),
2. in the cases of para. 2 (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 (S 278 to S 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 S 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 (letter a) will use the technical device or establish a connection with such device;

4. in the cases of para 2 (4).

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

(Constitutional Provision)
Fundamental Right to Data Protection

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

(2) Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority the restriction shall only be permitted based on laws necessary for the reasons stated in Art. 8 para. 2 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

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

1. the right to obtain information as to who processes what data concerning him, where the data originated, for which purpose they are used, as well as to whom the data are transmitted;

2. the right to rectification of incorrect data and the right to erasure of illegally processed data.

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

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

III. Considerations

The Constitutional Court has considered the following (…):

1. Procedural Requirements

1.1. The Constitutional Court together with the Court of Justice of the European Union to which questions for the preliminary ruling were submitted (…) provisionally assumed in its decision of 28 November 2012, *VfSlg. 19.702/2012*, for the purposes of the proceedings of constitutional review of the act, that the application of the government of the Province of Carinthia G 47/2012 and the individual applications of G 59/2012 and G 62, 70, 71/2012 are admissible (see IV.1.1. of the decision of 28 November 2012 in *VfSlg. 19.702/2012*). In the continuing proceedings the admissibility of the applications needs to be determined individually.

1.2. The Court of Justice of the European Union has in its judgment in the Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland und Seitlinger and others*, of 8 April 2014 (…) which, inter alia, has been rendered based on a request for a preliminary hearing by the Constitutional Court (*VfSlg. 19.702/2012*) declared that the Data Retention Directive is invalid without restricting the temporal effect of the declaration of invalidity. Thus, the declaration of invalidity has a retroactive effect (*cf. CJEU 13.5.1981, Rs 66/80, International Chemical Corporation, Slg. 1981, 1191 [para. 13 ff.]*). In this way the Data Retention Directive has been removed from Union law with effect *ex tunc* (see, generally, the temporal effect of judgments of the Court of Justice of the European Union in preliminary ruling procedures with which Union law is declared invalid, (…))

1.3. A direct application of the provisions of the Data Retention Directive and other provisions of Union law, which would at most cause the Constitutional Court to perceive the primacy of application of Union law and which would in particular affect the admissibility of the individual applications of G 59/2012 and of G 62, 70, 71/2012 (*cf. e.g.*

VfSlg. 14.499/1996, 15.771/2000, 17.508/2005, 18.298/2007) are therefore not directly applicable.

1.4. The application G 47/2012:

1.4.1. In accordance with Art. 140 para. 1 (2) of the Federal Constitutional Act ('*Bundesverfassungsgesetz', B-VG*) the Constitutional Court determines the constitutionality of a federal law also at the request of a provincial government. The application of the government of the Province of Carinthia is such a request.

1.4.2. The boundaries of the annulment of a provision of law of which the constitutionality needs to be reviewed, as the Constitutional Court has repeatedly stated both on its own initiative as well as initiated by the application for proceedings to review a legislative act (*VfSlg. 13.965/1994 mwN, 16.542/2002, 16.911/2003*), necessarily have to be drawn up in such a way that on the one hand the remaining part of the legislation does not receive a completely modified content and that on the other hand the inextricable connected purpose of the repealed part of legislation is also covered.

1.4.3. When following this basic position, the scope of the contestation of the provision in review for other grounds of inadmissibility of the application may not be too narrow in the law review proceedings (*cf. e.g. VfSlg. 8155/1977, 12.235/1989, 13.915/1994, 14.131/1995, 14.498/1996, 14.890/1997, 16.212/2002*). The applicants have to challenge those provisions which form an inseparable unit for the legal assessment of the possible unconstitutionality of the legal position. It is a matter for the Constitutional Court to decide in which way such unconstitutionality can be removed, should the Constitutional Court share the view of the requesting court (*VfSlg. 16.756/2002, 19.496/2011*). The scope of a provision to be reviewed and possibly repealed needs to be limited in such a way, that on the one hand not more is removed from the current legislation than is necessary to set aside the admissible alleged illegality, and that on the other hand the remaining part does not undergo any change in its meaning. Since both objectives can never be achieved completely at the same time, it needs to be assessed in each individual case, whether and to what extent the one objective takes precedence over the other (*cf. VfSlg. 19.496/2011 mwN*).

1.4.4. Against this background, the application of the government of the Province of Carinthia proves as inadmissible as the scope of the contested legislation is too narrow. Due to the fact that the applying provincial government challenged a number of provisions of the Telecommunications Act ('*Telekommunikationsgesetz 2003', TKG 2003*) in particular S 102a TKG 2003, which in its opinion are inseparably linked to data retention but not the provisions of the Code of Criminal Procedure ('*Strafprozessordnung', StPO*) and Security Police Act ('*Sicherheitspolizeigesetz', SPG)* which governs the "*Beauskunftung*" (providing information) of retained data, it did not challenge all the provisions that form an inseparable unit for the

review of any possible unconstitutionality of the provisions regulating data retention (cf. 2.3 below).

1.4.5. Already, for this reason the application of the government of the Province of Carinthia needs to be rejected as inadmissible.

1.5. The application G 59/2012:

1.5.1. In accordance with Art. 140 para. 1 (1) (c) B-VG the Constitutional Court decides on the constitutionality of laws at the request of a person who alleges that this unconstitutionality directly infringed his rights and if he has been affected by this law without a court decision having been rendered or ruling having been issued. As the Constitutional Court has held previously in *VfSlg. 8009/1977* which starts to be settled case law the fundamental requirement for the right to file an application is that the law directly intervenes in the legal sphere of the person concerned and in the case of the law being unconstitutional it violates his rights. In this case the Constitutional Court has to accept the submissions of the applicant and only has to determine whether the argued effects are of such a nature as Art. 140 para. 1 (1) (c) B-VG requires for the eligibility to file an application (*cf. e.g VfSlg. 11.730/1988, 15.863/2000, 16.088/2001, 16.120/2001*).

1.5.2. Not every party who is addressed by the provision has *locus standi* to contest the law. It is also necessary that the law directly interferes in the legal sphere of the applicant. Such an interference should only then be accepted if it is by its very nature and extent clearly determined by the law itself and if it not merely potentially but actually impairs the (legally protected) interests of the applicant and if the applicant has no reasonable way of protecting his interests from the allegedly unlawful interference *VfSlg. 11.868/1988, 15.632/1999, 16.616/2002, 16.891/2003*).

1.5.3. Concerning the criteria of case law for the scope of the requested repeal of legal provisions in the present individual application, reference can be made to the application by the government of the Province of Carinthia in 1.4.2 and 1.4.3.

1.5.4. The individual application is directed against S 102a TKG 2003 as well as other in detail described provisions which are inseparably linked to S 102a TKG 2003. The second applicant possibly also challenges S 134 (2a) and S 135 para. 2a StPO as well as the more detailed phrases in S 53 para. 3 (3) and S 53 para. 3b SPG, because these are inseparable to S 102a TKG 2003 (…).

1.5.5. According to the Federal Government the addressee of S 102a TKG 2003 is not a “final customer” as the second applicant. Therefore, he was not legally affected by this provision. The counter-argument thereto is that the contested provision in S 102a TKG 2003 on the ground of its linguistic version – as the Federal Government emphasized in its submissions –

only addresses 'public communication service providers', 'Internet access service providers', 'providers of public telephone services including Internet telephone services' and 'e-mail service providers'. However, the provision has according to its content and purpose such an effect on the second applicant as 'user' (cf. S 92 para. 3 (2) TKG 2003) of public communication services, which not only intervenes in its actual situation, but also in the legal sphere particularly shaped by the constitutionally guaranteed rights in Art. 8 ECHR and S 1 Data Protection Act ('*Datenschutzgesetz', DSG 2000)* of the second applicant. Therefore, the second applicant is according to the purpose and content of the contested provision to be regarded as the addressee of the provision (*cf. VfSlg. 13.038/1992, 13.558/1993, 19.349/2011*).

1.5.6. On the question of a reasonable alternative way to submit concerns to the Constitutional Court, the following should be noted:

1.5.6.1. Due to the arrangement in S 102a TKG 2003, the therein mentioned providers are obliged to store certain data pertaining to the second applicant. The obligation and authorization for storage directly affects the second applicant's legal sphere, without the need for a specific legal act or for the intention of such. Unlike in cases where, for example, governmental institutions are authorized by legal order to take certain measures which lead to an impairment of the legal sphere of the person subject to the law under certain circumstances and only in the case of their implementation (*cf. e.g. VfSlg. 18.831/2009*), are in this case those circumstances present that interfere in the legal sphere merely due to the continuing obligation to store data and its adherence thereto.

1.5.6.2. Under the circumstances of the present case, the Constitutional Court cannot find that there is a reasonable alternative way available for the second applicant to defend himself against the alleged illegality of the contested provisions:

1.5.6.3. The alternatives essentially raised by the Federal Government in their submissions regarding the enforcement of the alleged unconstitutionalities, the declaratory decision or the decisions of the ordinary courts in accordance with DSG 2000are not a suitably reasonable alternative for the second applicant's individual application.

1.5.6.4. The Federal Government seems to assume on the one hand that the second applicant with regard to the data stored according to S 102a TKG 2003 could have requested information according to S 26 DSG 2000, following which he could have lodged a complaint with the former Data Protection Commission alleging that his right to information according to S 26 DSG 2000 has been infringed. Then the Data Protection Commission would have had to decide the complaint by providing a decision. According to Art. 144 B-VG an appeal could have been instituted against the decision. In this way, the concerns with regard to the constitutionality of the provisions on data retention could have been brought to the Constitutional Court. On the other hand, the Federal Government submits that the second

applicant could have requested the erasure of the retained data by way of a civil action (S 27 in conjunction with S 32 DSG 2000). As a result, the thereto appointed courts (cf. S 32 para. 4 DSG 2000) would have had to submit any unconstitutionality of the provisions to be applied by them to the Constitutional Court (cf. Art. 89 para. 2 second sentence B-VG, Art. 140 para. 1 (1) (a) B-VG).

1.5.6.5. It is true that the Constitutional Court, inter alia, has pronounced in connection with provisions of the SPG that individuals who have a firm suspicion that their data was obtained on the basis of the provisions of SPG have or had the following reasonable ways at their disposal: the obtaining of a declaratory decision regarding the right to information according to S 26 DSG 2000, the obtaining of decision on the erasure rights according to S 27 DSG 2000, the right of appeal according to S 31 DSG 2000 in conjunction with S 90 SPG, as well as the filing of the complaint with the former Data Protection Commission according to S 30 para. 1 DSG 2000, which can lead to a system inspection according to S 30 para. 2 DSG 2000 in the case of a reasonable suspicion (*VfSlg. 18.831/2009*). There are no reasons for the Constitutional Court to deviate from the case law in these proceedings.

1.5.6.6. However, the mentioned ways do not prove to be reasonable in this particular matter. It should be borne in mind that the second applicant is directly and currently affected by the contested provisions, as he must assume in any event that certain data concerning him – even if not necessarily determined by state institutions but by legal regulation, namely on the basis of the regulation in S 102a para. 1 TKG 2003 for the purpose of 'investigation, detection and prosecution of criminal offences, the seriousness of which is justified by a regulation in S 135 para. 2a StPO' – was and is being stored. In S 102a para. 1 TKG 2003 it is stated that this data concerning a specific and limited group of persons is not only to be stored in exceptional circumstances but that *all* providers of public communication services in accordance with para. 2 to 4 of this provision fall under the obligation to store data from the date of generation or processing until six months after the termination of the communication.

1.5.6.7. It is correct that the second applicant who has filed an information request according to S 26 DSG 2000 or an erasure request according to S 27 DSG 2000 could have approached those providers of communication services, where he is aware that they store data concerning him. Subsequently, he could have challenged the reactions of the providers with an appeal. Although the second applicant can in theory submit his concerns about the constitutionality of the provisions in question directly (Art. 144 B-VG) or indirectly (Art. 89 para. 2 second sentence B-VG, Art. 140 para. 1 (1) (a) B-VG) to the Constitutional Court, the exceptional and special circumstances in this matter prevent the second applicant from choosing this way:

1.5.6.8. As the Constitutional Court has repeatedly stated in the connection with individual applications submitted in accordance with Art. 139 und 140 B-VG, the individual who is

affected by general legal provisions only has the right to file the applications to review the regulation and legislation in exceptional and special circumstances. Namely, if it is generally possible that legal or administrative proceedings are introduced which ultimately provides these individuals with the opportunity to promote the initiation of the official review procedure of legislation through the Constitutional Court. Otherwise, one would arrive at the duplication of legal protection which is not in line with the principle that an individual application is merely a subsidiary legal remedy (*cf. e.g. VfSlg. 8312/1978, 11.344/1987, 15.786/2000, 18.182/2007, 19.126/2010*).

1.5.6.9. The special and exceptional circumstances are as follows:
Due to the obligation to store according to S 102a TKG 2003 and the providing of information according to S 135 para. 2a StPO as well as S 53 SPG there is a wide scope of data which is either stored with the providers of public communication services or (at the providing of information) with the police and prosecution authorities. The storage obligation is not only applicable to those providers with whom the second applicant entered into a contract but also the providers of the 'communication partner' of the second applicant, i.e. those individuals with whom the second applicant, for example, telephoned or sent e-mails (cf. S 102a para. 3 (1) and (3) TKG 2003; for mobile networks S 102a Para. 3 (6) TKG; for email services S 102a Para. 4 (3) and (4) TKG 2003). The second applicant is faced with a barely manageable number of providers which could have stored his data on the basis of S 102a TKG 2003. It is practically impossible to determine which provider has stored or stores which data in what periods of time on the basis of S 102a TKG 2003.

1.5.6.10. Moreover, it should be noted that if the second applicant would proceed with a judicial erasure procedure concerning the stored data about him against one provider, further data will continuously be stored by other providers on the basis of S 102a TKG 2003. The erasure of data for which the second applicant would seek legal action, would have already occurred at the time the Constitutional Court would have had to decide the request by a court according to Art. 89 para. 2 B-VG, thus the admissibility of the application would be in question.

1.5.6.11. These circumstances correspond according to the weight of the impending disadvantages to those circumstances for which the Constitutional Court already considered the available alternatives to be unreasonable (*cf. VfSlg. 11.853/1988, 12.379/1990, 15.786/2000*).

1.5.7. In view of the specific features of the data retention the second applicant did not have another reasonable way than to submit the individual application.

1.5.8. However, the application proves to be inadmissible in so far as the repeal of S 1 para. 4 (7) TKG 2003 is sought, because this provision was announced together with BGBl. I 27/2011 and is contested 'in its applicable version (BGBl. I 102/2011)'. Furthermore,

it is inseparably linked with S 102a TKG 2003 and includes the ‘note on the implementation of Directive 2006/24/EG‘.

1.5.8.1. As stated above (see 1.5.1) the Constitutional Court has to rely on the facts of the application when considering the admissibility of the application.

1.5.8.2. Against this background, the second applicant is not able to demonstrate to what extent the contested legal provision has to be in conflict with a constitutional provision and where the alleged ‘inseparable connection’ is in the unconstitutionalities seen in S 102a TKG 2003 and the contested provision. Therefore, the application to repeal S 1 para. 4 (7) TKG 2003 has to be rejected.

1.5.9. S 102c para. 1, 4 and 5 TKG 2003 in the contested version was amended with a new version in accordance with Art. 2 der DSG-Novelle 2014, BGBl. I 83/2013 with effect from 1 January 2014. In so far where the application is directed against provisions which already have been declared invalid the application in this regard has to be rejected.

1.5.10. The application is admissible where it does not contest S 1 para. 4 (7) TKG 2003 and S 102c para. 1, 4 and 5 TKG 2003.

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

1.6.1. With regard to the third applicant nothing emerged which would lead to a different evaluation than that of application G 59/2012 (see above 1.5).

1.6.2. This application is also admissible.

2. On the merits

2.1. The Constitutional Court has to limits itself to the discussion of the raised issues in a proceeding to review the constitutionality of a law according to Art. 140 B-VG, which was initiated by an application (*cf. VfSlg. 12.691/1991, 13.471/1993, 14.895/1997, 16.824/2003*). Thus, the court solely has to assess from the reasons set out in the application whether the contested provision is unconstitutional (*VfSlg. 15.193/1998, 16.374/2001, 16.538/2002, 16.929/2003*).

2.2. The relevant constitutional law provisions:

2.2.1. In the present applications it is submitted that the contested provisions violate the rights set out in S 1 DSG 2000, Art. 8 ECHR as well as Art. 7 and 8 of the Charter of Fundamental Rights of the European Union (‘Charter of Fundamental Rights').

2.2.2. As the Constitutional Court already held in its decision in *VfSlg. 19.702/2012* with which it requested a preliminary ruling from the Court of Justice of the European Union that the Federal Constitutional Law contains an independent fundamental right to data protection besides Art. 8 ECHR. The constitutional provision of S 1 DSG 2000 provides that every natural or legal person is entitled to the confidentiality of personal data concerning him in so far as there is an interest worthy of the protection (S 1 para. 1 DSG 2000, (…)). S 1 para. 2 DSG 2000 contains a substantive legal reservation according to which, apart from the use of personal data which is of vital interest of the affected person or with his consent, limitations of the right of confidentiality are only permissible for the protection of prevailing legitimate interests of another, namely, for the interferences of an authority only based on laws, which are necessary for the grounds mentioned in Art. 8 para. 2 ECHR.

2.2.3. For the legal basis S 1 para. 2 DSG 2000 requires, going beyond Art. 8 para. 2 ECHR, that the use of data which is particularly worthy of protection due to its nature is only intended for the safeguarding of important public interests and that at the same time adequate safeguards to protect the confidentiality interests of the affected persons are set out in law.

2.2.4. The Constitutional Court considered in *VfSlg. 19.702/2012* that the Data Retention Directive – this was the reason for the preliminary ruling procedure – could be implemented only by infringing the fundamental right of S 1 DSG 2000 and that as a result thereof the Constitutional Court could be precluded from reviewing the legal regulations on data retention (*cf. VfSlg. 15.427/1999*). Since there would be no room for an implementation which is constitutionally conform, the Constitutional Court is precluded from a review of the legal regulations measured against the standard of S 1 DSG 2000. The Court of Justice of the European Union declared the regulation to be invalid and, therefore, this consideration is also no longer valid so that S 1 DSG 2000 and Art. 8 ECHR are in any event again the relevant measure in the legal review procedure.

2.2.5. The result is consistent with the fact that the Court of Justice of the European Union, given the invalidity of the Data Retention Directive, did not find it necessary to answer the questions (…) concerning the interpretation of Art. 7, 8, 52 und 53 Charter of Fundamental Rights (CJEU, *Digital Rights Ireland und Seitlinger and others*, para. 72).

2.2.6. Even Art. 15 para. 1 second sentence RL 2002/58/EG does not change the result. The regulation merely determines that Member States can provide through legal provisions that data can be stored for a limited period of time for the reasons listed in this paragraph. Such measures must 'comply with the general principles of community law including the principles set out Article 6 paragraphs 1 and 2 of the Treaty on the European Union' (Art. 15 para. 1 last sentence RL 2002/58/EG). According to Art. 15 para. 2 RL 2002/58/EG the provisions of Chapter III of the Directive 95/46/EG apply to judicial remedies, liability and sanctions with regard to national rules which are adopted according to RL 2002/58/EG, and

to the individual rights resulting from this directive. However, the directive does not provide for more detailed provisions for the implementation of the limitations stated in Art. 15 para. 1 second sentence RL 2002/58/EG, thus it needs to be assumed that the legislator has a wide discretion concerning the implementation. Therefore, precedence over national constitutional law and the two mentioned constitutionally guaranteed rights does not come into consideration.

2.2.7. Art. 7 and 8 Charter of Fundamental Rights may also be considered as a standard in these proceedings to review the legislation. As the Constitutional Court has set out in the preliminary ruling request *VfSlg. 19.702/2012* following its previous ruling (*VfSlg. 19.632/2012*), the guaranteed rights of the Charter of Fundamental Rights form within the area of the application of the Charter of Fundamental Rights (Art. 51 para. 1 Charter of Fundamental Rights) a standard of review for the proceedings of judicial review, particularly for the proceedings that are according to Art. 139 und 140 B-VG. This is the case when the relevant guarantee of the Charter of Fundamental Rights is similar to the constitutionally guaranteed rights of the Austrian Federal Constitution in its formulation and determination. Legal regulations which were issued on the basis of the implementation of the directive form at least one case of implementation of Union law (*cf. only VfSlg. 19.632/2012*). Even though the Data Retention Directive has been declared invalid (with effect *ex tunc*) the contested provisions – especially those that were announced by BGBl. I 27/2011 – were only issued following the implementation of Union law because they were adopted within the scope of RL 2002/58/EG and in particular Art. 15 Para. 1 thereof.

2.2.8. If the legislator makes use of his discretion when implementing Union law and creates regulations which affect besides a fundamental right of the Charter of Fundamental Rights another constitutionally guaranteed right, then the Constitutional Court decides on the basis of this right whether it has the same scope of application as the right in the Charter of Fundamental Rights (*VfSlg. 19.632/2012*) and if the limits for permissible legislative interference with the constitutionally guaranteed rights are narrower or at least not wider than the corresponding rights of the Charter of Fundamental Rights. This can be assumed for both Art. 8 ECHR as well as S 1 DSG 2000:

2.2.8.1. Art. 8 ECHR determines the interpretation of Art. 7 Charter of Fundamental Rights in such a way as is evident by the comments on Art 7 Charter of Fundamental Rights that this Art 7 ‘corresponds’ to it and therefore ‘has the same meaning and scope’. (Art. 52 para. 3 Charter of Fundamental Rights, the references to the jurisprudence of the European Court of Human Rights in the judgment of the Court of Justice of the European Union in *Digital Rights Ireland und Seitlinger and others*, para. 35, 47, 54 f. are also in this sense).

2.2.8.2. S 1 DSG 2000 contains a substantive legal reservation which defines the limits for interference with the fundamental rights in a much narrower sense than what

Art. 8 para. 2 ECHR does. Apart from the use of personal data in the vital interest of the affected person, or with his consent limitations of the right of confidentiality are only permissible for the protection of prevailing legitimate interests of another, namely, for the interferences of a governmental authority purely based on laws, which are necessary for the grounds mentioned in Art. 8 para. 2 ECHR.

For the legal basis S 1 para. 2 DSG 2000 requires beyond the scope of Art. 8 para. 2 ECHR that data which by its very nature are particularly worthy of protection may only be made use of to safeguard important public interests and that simultaneously adequate safeguards protecting the confidentiality interests of the individual are legally set down. Finally, these provisions explicitly prescribe that in the case of permissible limitations the interference with the fundamental right must be in a 'least intrusive and goal orientated manner'.

2.2.9. According to previous court decisions of the Constitutional Court it follows from this regulation that a stricter standard must be applied to the proportionality of the interference with the fundamental right according to S 1 DSG 2000 than the one already provided for in Art. 8 ECHR (*VfSlg. 16.369/2001, 18.643/2008*). This level of protection is also unaffected by the Charter of Fundamental Rights in those matters where the legislator has a discretion in implementing Union law (cf. Art. 53 Charter of Fundamental Rights; see above 2.2.6). Against this background the contested provisions need to be measured against the standard of the Federal Constitutional law, namely against S 1 DSG 2000 and Art. 8 ECHR.

2.3. Regarding the concerns expressed against S 134 (2a) and S 135 para. 2a StPO as well as S 53 para. 3a (3) and S 53 para. 3b SPG and against S 102a TKG 2003 the following is stated:

2.3.1. The applicants seek the annulment of S 102a TKG 2003, inter alia, on the grounds that it violates the constitutionally guaranteed right provided for in S 1 DSG 2000. S 134 (2a) and S 135 para. 2a StPO as well as S 53 para. 3a (3) and S 53 para. 3b SPG were (as submitted by the third applicant) 'to be seen as one unit with the provisions of the storage obligation (S 102a TKG) and the use of retained data (S 102b TKG, S 99 para. 5 (2) to (4) TKG)', these provisions would also violate the mentioned fundamental right, particularly, because the 'possibilities of access' provided for in the mentioned provisions of the StPO and SPG were over reaching (according to the second applicant).

2.3.2. Providers of public communication services (cf. S 92 para. 2 (1) TKG 2003) are required by S 102a para. 1 TKG 2003 to store certain categories of data which are generated or processed in the course of the provision of public communication services (cf. S 102a para. 5 first sentence TKG 2003) 'going beyond the permission for storage or processing according to S 96, 97, 99, 101 und 102'. These categories of data need to be stored from the time of production or processing until six months after the completion of the communication. The data is stored according to S 102a para. 1 last sentence TKG 2003

exclusively for the investigation, detection and prosecution of criminal offences and the seriousness of these criminal offences justifies an order according to S 135 para. 2a StPO.

2.3.3. S 135 para. 2a StPO in conjunction with S 135 para. 2 (2) to (4) StPO determines that the providing information on retained data (S 134 (2a) StPO) is permissible if it is expected that thereby the investigation of an intentional crime which is punishable by a prison sentence of more than six months is furthered and the holder of the technical equipment which was or will be the origin or destination of a transmission of a message expressly consents to the provision thereof (S 135 para. 2 (2) StPO); if it is expected that thereby the investigation of an intentional crime which is punishable by imprisonment of more than one year is furthered and that on the basis of certain facts it can be assumed that thereby data of the accused can be determined (S 135 para. 2 (3) StPO); or if it is to be expected on the basis of certain facts that thereby the whereabouts of a fugitive or absent accused who is strongly suspected to have intentionally committed a crime which is punishable with a prison sentence of more than one year can be determined (S 135 para. 2 (4) StPO). According to S 135 para. 2a StPO the providing information on the retained data is to be ordered by the state prosecutor on the basis of judicial approval (S 137 para. 1 StPO). An appeal according to S 87 StPO can be submitted against such a judicial approval after it has been delivered to the affected individual (S 138 para. 5 StPO). According to S 147 para. 1 (2a) StPO the legal protection commissioner (*Rechtsschutzbeauftragter*) is responsible for assessing and controlling the order, authorization, approval and execution of the provision of information on retained data according to S 135 para. 2a StPO. The legal protection commissioner has the right to appeal (S 147 para. 3 StPO) against the approval of an investigative measure according to S 147 para. 1 (2a) StPO. After completion of the investigative measures the legal protection commissioner must be given the opportunity to view the entire results before they are filed in the matter. Furthermore, he is entitled to request the erasure of the results or parts thereof and to convince himself of the proper erasure of these results (S 147 para. 4 StPO).

2.3.4. According to S 53 para. 3a (3) SPG security authorities are entitled to request information concerning the name and address of a user who was assigned an IP address at a particular time from providers of public communication services if the security authorities need this data as an essential prerequisite to counter a concrete danger to the life, health or freedom of an individual in the context of the first general obligation to render assistance (S 19 SPG), a dangerous attack (S 16 para. 1 (1) SPG) or a criminal association (S 16 para. 1 (2)), 'even if the use of retained data according to S 99 para. 5 (4) in conjunction with S 102a TKG 2003 is required for this'. On the basis of S 53 para. 3b SPG security authorities are further entitled to require from providers of public telecommunication services information about location data and the international mobile subscriber identity (IMSI) of the carried equipment of a person in danger or a person accompanying the person in danger, 'even if the use of retained data in terms S 99 para. 5 (3) in conjunction with S 102a TKG 2003 is required for this.'

The requirement for the providing information according to S 53 para. 3b SPG is that there is an actual threat to the life, health or freedom of an individual which can be assumed due to the set of circumstances and that the security authorities take the necessary steps within the scope of their duty to provide assistance or to avert danger (S 53 para. 3b SPG). The actions of the security authorities in accordance with the mentioned provisions of the SPG require no judicial approval. According to S 91c para. 1 SPG the legal protection commissioner needs to 'be notified as soon as possible' about this request for information. He is responsible for the review of such a notification (S 91c para. 1 last sentence SPG).

2.3.5. According to S 1 para. 1 DSG 2000 everyone is entitled to the confidentiality of personal data concerning him, in so far as he has a legitimate interest worthy of protection, in particular with regard to the respect of the private and family life. Limitations of this fundamental right are according to the reservation of S 1 para. 2 DSG 2000 (apart from the affected individual's vital interests in the use of personal data or his consent thereto) only permissible for interferences of a public authority only based on legislation, if they are necessary for the reasons mentioned in Art. 8 para. 2 ECHR and if they are sufficiently precise so that they provide in a foreseeable manner for everyone under which conditions the determination or the use of personal data is allowed 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 limitations of the fundamental right to data protection must be proportional when balancing the seriousness of the interference and the weight of the objectives pursued (cf. Art. 8 in conjunction with Art. 52 para. 1 Charter of Fundamental Rights and CJEU, *Digital Rights Ireland und Seitlinger and others*, para. 38, 47, 69 as well as ECtHR, 4.12.2008 [GK], case *S. and Marper*, Appl. 30562/04, EuGRZ 2009, 299 [para. 101]). Such laws may only provide for the use of data which by its very nature is worthy of protection for the safeguarding of important public interests and must simultaneously set adequate safeguards for the protection of the confidentiality interests of the affected individual (S 1 para. 2 second sentence DSG 2000).

Also in the case of permissible limitations according to Art 8 para. 2 ECHR, the interference with the fundamental rights may only be carried out in the least intrusive and goal orientated manner according to the last sentence of S 1 para. 2 DSG 2000. Therefore, the respective legislator must provide for these requirements a sufficient matter-specific regulation so that the cases of permissible interferences with the fundamental right of data protection are defined and limited (*cf. e.g. VfSlg. 18.643/2008, 19.657/2012, 19.659/2012, 19.738/2013*).

2.3.6. The fundamental right of data protection which is enshrined in S 1 DSG 2000 provides for constitutional protection against the identification of personal data (*VfSlg. 12.228/1989, 12.880/1991, 16.369/2001*). The data which needs to be stored according to S 102a

TKG 2003 and which needs to be provided according to S 135 para. 2a StPO and S 53 para. 3a (3) as well as S 53 para. 3b SPG is personal data as defined in S 1 para. 1 DSG 2000. In particular, all the categories of data listed in para. 2 to 4 of S 102a TKG 2003 are of such a nature that the identity of the person concerned is determined or is at least determinable. Particularly, with regard to the possibilities of linking with other information (e.g. the conclusions which can be drawn from accumulated calls of a particular subscriber number) listed by the applicants, a legitimate interest of confidentiality worthy of protection exists within the affected data as defined by S 1 para. 1 DSG 2000.

2.3.7. The providers of public communication services are obliged by S 102a para. 1 TKG 2003 to store data in accordance with para. 2 to 4 of this provision. This obligation interferes with the fundamental right of data protection enshrined in S 1 DSG 2000 as well as with the right to respect for private and family life enshrined in Art. 8 ECHR of the users of public communication services (*VfSlg. 19.738/2013*; (…) ECtHR 26.3.1987, case *Leander*, Appl. 9248/81, para. 48; ECtHR 16.2.2000 [GC], case *Amann*, Appl. 27.798/95, [para. 65 ff.]; ECtHR 4.5.2000 [GC], case *Rotaru*, Appl. 28.341/95, [para. 43]; ECtHR 3.7.2007, case *Copland*, Appl. 62.617/00, , 415 [para. 43 f.]; ECtHR, case *S. and Marper*, para. 67; (…)).

2.3.7.1. The fact that the storage is done by providers of public communication services – i.e. by private companies – who are obliged to store data according to S 102a TKG 2003 does not change the existence of an interference with the rights in S 1 DSG 2000 and Art. 8 ECHR by the legislator. A 'communication service provider' includes everyone who offers a communication service (S 92 para. 3 first half of the sentence in conjunction with S 3 (9) TKG 2003) but who – in contrast to the 'operator of a communication service' (S 3 (1) TKG 2003) –does not necessarily control all the functions of this service (…). The TKG 2003 assumes that 'providers' as well as 'operators' of a communication service are (private) companies (see only S 1 para. 1, S 34 ff. TKG 2003).

2.3.7.2. These companies have no margin due to the imposed obligation to store data according to S 102a TKG 2003. According to S 109 para. 3 (22) TKG 2003 they would commit an administrative offence if they would act contrary to the storage obligation in S 102a TKG 2003.

2.3.8. The storage of data on the ground of the obligation according to S 102a TKG 2003 and access to the data (providing information) by police and prosecution authorities – in particular on the basis of S 135 para. 2a StPO and S 53 Para. 3a (3) as well as S 53 para. 3b SPG – constitute an interference with the fundamental right of data protection (S 1 DSG 2000) and the right to respect for private and family life under Art. 8 ECHR (*cf. e.g. VfGH 1.10.2103, G 2/2013* with further reference to the case law of the Constitutional Court; for the interference with Art. 8 ECHR further ECtHR 26.3.1987, case *Leander*, Appl. 9248/81,

para. 48; ECtHR 4.5.2000 [GK], case *Rotaru*, Appl. 28.341/95, ÖJZ 2001, 74 [para. 46]; ECtHR 29.6.2006 [admissibility decision], case *Weber and Saravia*, Appl. 54.934/00, para. 79).

2.3.9. Regulations which constitute a serious violation of fundamental rights such as the contested provisions may be admissible for combating serious crimes, provided they comply with the strict requirements of S 1 DSG 2000 and Art. 8 ECHR. Whether such an interference with regard to S 1 para. 2 DSG 2000 and Art. 8 para. 2 ECHR is permissible depends on the requirements of the conditions of the storage of data for retention and on the requirements of their erasure as well as on the legal safeguards when determining the possibilities of official and private access to this data. The contested provisions of TKG 2003, StPO and SPG do not fulfil these requirements:

2.3.10. The provisions concerning the retention of data including the provisions on information on retained data in the StPO and SPG serve to achieve the objectives mentioned in Art. 8 para. 2 ECHR, namely, in particular, the maintenance of public peace and order and the protection of rights and freedoms of others. The legislator could within his scope of discretion reasonable expect that the regulations on data retention are abstractly suitable to achieve these objectives (*cf. CJEU, Digital Rights Ireland und Seitlinger and others*, para. 44 and 49 for Art. 7 und 8 Charter of Fundamental Rights).

2.3.11. A further requirement for the proportionality and thereby the permissibility of the interference is that the severity of the specific interference does not exceed the weight and importance of the objectives which are to be achieved through data retention.

2.3.11.1. The point of departure of the assessment of the proportionality of data retention is the idea that the fundamental right of data protection in a democratic society – in the area of protection relevant here – is directed towards the facilitating and safeguarding of confidential communication between individuals. The individual and his free personal development do not only depend on the public communication but also on the confidential communication in the community; freedom as the right of an individual and as a condition of a society are determined by the quality of the information relations (…).

2.3.11.2. The importance and weight of the aims pursued through data retention are significant as is expressed by legislator with the purpose in S 102a para. 1 last sentence TKG 2003. Even assuming that the regulation according to the wording of para. 1 serves an important public interest (see above 2.3.10) it is necessary that due to the 'dispersion range' of the interference, the scope and nature of the affected data (see below 2.3.14.3) and the resulting severity of the interference with the right of informational self-determination (data can be accessed which not only enables the creation of a movement profile but also that conclusions can be drawn concerning private preferences and the acquaintances of an individual in the case where data can be linked; see below 2.3.14.5), the legislator ensures with appropriate regulations that the data is only made available to police and prosecution

authorities in the presence of a important public interest with comparative weight in an individual case and if it is subject to judicial control. It should be noted that state action was and is faced in many ways – not least also in the fight against crime for which data retention is intended – with special challenges by the rapid distribution of the use of 'new' communication technologies (e.g. mobile telephony, e-mail, exchange of information in the context of the World Wide Web) in the last two decades. The case law of the Constitutional Court has always considered this changed environment of police investigations (*cf. e.g. VfSlg. 16.149/2001, 16.150/2001, 18.830/2009, 18.831/2009, 19.657/2012*). It should be noted that the expansion of technical possibilities also leads thereto, that the dangers which these expansions holds for the freedom of individuals have to be countered in an adequate way.

2.3.11.3. The Court of Justice of the European Union has emphasized in its judgment in *Digital Rights Ireland und Seitlinger and others* that the Data Retention Directive provides for no objective criteria which makes it possible to limit the access of the competent national authorities to data and their subsequent use for the purpose of prevention, detection or prosecution of criminal offences which with regard to the extent and severity of the interference with the fundamental rights enshrined in Art. 7 and Art. 8 of the Charter of Fundamental Rights can be considered as sufficiently serious to justify such interference (para. 60). On the contrary, the Data Retention Directive in Art. 1 para. 1 only generally makes reference to the serious criminal offences determined by the national law of the member states.

2.3.11.4. The Federal Government emphasizes in its observations on the judgment of the Court of Justice of the European Union in *Digital Rights Ireland und Seitlinger and others* that the providing information on the retained data against the will of the 'monitored user' is only admissible if it is expected that thereby an investigation of an intentionally committed offence which is punishable by imprisonment of more than one year is solved. The providing information on retained data with regard to the elements of S 135 para. 2 (2) StPO aims at providing victims of persistent stalking (S 107a StGB) a possibility for the effective prosecution of offenders.

2.3.11.5. The Federal Government is legally incorrect with its submissions that the regulation in S 135 Para. 2a in conjunction with S 135 Para. 2 (2) to (4) StPO is sufficiently differentiated and thereby proportional. The Court of Justice of the European Union has emphasized that the Data Retention Directive should contribute to the fight against serious crime (*CJEU, Digital Rights Ireland und Seitlinger and others*, para. 60). The same applies for the directive implemented by the provisions in TKG 2003, StPO and SPG. It is possible for the legislator to stipulate that only the investigation of crimes with a certain sentence should rely on the providing information on retained data. However, in addition the legislature would have to ensure that the seriousness of the offence – which is expressed by the respective penalty – justifies in the individual case the interference with the constitutionally guaranteed rights of

the individuals who are affected by the providing of 'their' retained data. In this respect the offences included in S 135 para. 2a in conjunction with S 135 para. 2 (2) to (4) StPO are too undifferentiated and therefore too wide. It does not make provision for whether the requests for providing information are only permitted for offences which either have heavy penalties (e.g. S 207a StGB) or the solving of which necessarily requires the use of retained data due to the nature of the offence (e.g. S 107a para. 1 in conjunction with para. 2 (2) StGB).

2.3.11.6. The proportionality of the storage of data for retention is – regardless of the reservation of the judicial approval of the providing information on retained data (S 135 para. 2a in conjunction with S 137 para. 1 StPO), the referral of the legal protection commissioner and his right of appeal according to S 147 para. 1 (2a) und para. 3 second sentence StPO – already, therefore, not assured because due to S 135 para. 2a StPO in conjunction with S 102a, S 102b para. 1 TKG 2003 it is not guaranteed that retained data is only then provided if it serves the criminal prosecution and solving of the investigation which in the individual case is a serious threat to the objectives stated in Art. 8 para. 2 ECHR and which justifies such interference. Therefore, S 135 para. 2a StPO is conflict with S 1 para. 2 DSG 2000.

2.3.12. S 134 (2a) StPO which defines the term 'information on retained data' for the scope of application of StPO may not be separated from S 135 para. 2a StPO and, therefore, needs to be repealed.

2.3.13. The second and third applicants request the phrase 'even if the use of retained data according to S 99 para. 5 (4) in conjunction with S 102a TKG 2003 is required for this' and in S 53 para. 3a (3) SPG and in S 53 para. 3b the phrase 'even if the use of retained data according to S 99 para. 5 (3) in conjunction with S 102a is required for this' to be declared unconstitutional and therefore repealed.

2.3.13.1. According to the SPG the providing information on retained data needs – unlike as required by StPO –no judicial approval. The referral of the legal protection commissioner according to S 91c para. 1 SPG, who is responsible for the 'review of notifications made according to this paragraph', i.e. a review *ex post* (S 91c para. 1 last sentence SPG), is certainly not sufficient.

2.3.13.2. Furthermore, the above expressed concerns regarding S 135 para. 2a StPO also apply to the contested phrases of the mentioned provisions of SPG. The security duties of the police to access retained data lack any limitation related to the weight of an impending offence. Only negligence offences are not covered by them.

2.3.13.3. This does not satisfy the requirements of the proportionality of the interference with the fundamental right of data protection with the data being accessed according to

S 53 para. 3a (3) SPG or S 53 para. 3b SPG. Therefore, the contested phrases in these provisions should be declared unconstitutional und repealed.

2.3.13.4. The fact that according to S 53 para. 3a (3) SPG the security authorities can 'only' provide the name and the address of a user to whom an IP address was assigned to at a certain time and according to S 53 para. 3b SPG 'only' provide the location data which were stored in compliance with S 102a TKG 2003 does not change the result in light of the above mentioned remarks to II.2.3.13.1 (…).

2.3.14. In connection with the requirements to provide information ('providing information') S 102a TKG 2003 also proves to be unconstitutional. The provisions relating to providing information on retained data together with the provisions of TKG 2003 which require the storage of data constitute a serious violation of the constitutionally guaranteed data protection right in S 1 DSG 2000 of the 'user' (S 92 para. 3 (2) TKG 2003) of public communication services or individuals otherwise affected by the storage and thus also the second and third applicant (see above 2.3.7).

2.3.14.1. The applicants never alleged nor was it submitted in the hearing that the storage and processing of the data of the type mentioned in S 102a TKG 2003 are completely unsuitable to contribute to solving the investigation of a serious crime. The suitability of the interference with the fundamental rights needs to be examined in an abstract way, as it neither requires a specific percentage of the frequency of the application of the provisions in practice, nor a specific 'success rate' in the solving of the investigation of crimes. It is sufficient if the legislature was allowed to assume the suitability of the measure that has to serve the envisaged purpose (see in this context the seventh reason of consideration of the invalidated Data Retention Directive; *CJEU, Digital Rights Ireland und Seitlinger and others*, para. 43). The Constitutional Court does not consider in these proceedings whether each individual date to be retained according to S 102a TKG 2003 displays this suitability. It is by no means established from the outset that the storage of all the data to be stored for retention and processing according to S 102a TKG 2003 in the implementation of the invalid Data Retention Directive is proportional. The mere possibility to make use of new technologies for further monitoring measures does not in advance justify an interference with the freedoms protected by S 1 DSG 2000 and Art. 8 ECHR.

2.3.14.2. The Constitutional Court has already emphasized in its decision in *VfSlg. 19.702/2012* that the 'distribution range' of the unfounded storage exceeds those interferences in the legal sphere which it ever had to decide and which is protected by S 1 DSG 2000 (cf. BVerfGE 125, 260 [318 ff.]). This applies to the affected category of individuals, the scope and nature of the data as well as the purposes for which it is required and also the modalities of the use of data.

2.3.14.3. It needs to be considered that the storage affects primarily the users of fixed networks, mobile communication, Internet access services and e-mail services (S 92 para. 3 (14) und 15 TKG 2003) and thus the population of Austria is affected to a large extend. At the end of 2013 every business had an average of two fixed networks and more than half of every household had such a connection. On average 1.5 SIM cards for mobile telephony can be attributed to every inhabitant. Around 60% of households and businesses had Internet access via mobile or fixed broadband and the market penetration of broadband in the framework of smartphone tariffs amounted to 87% for household and businesses (…). Hence, almost the entire population is affected by the obligation to store data according to S 102a TKG 2003 (see *CJEU*, *Digital Rights Ireland und Seitlinger and others*, para. 56).

2.3.14.4. The Constitutional Court has already found in its decision in *VfSlg. 19.702/2012* that the data retention includes almost exclusively those individuals who have provided no cause – in the sense that they behaved in such a manner that would require state interference – for the storage of their data (*cf. CJEU, Digital Rights Ireland und Seitlinger and others*, para. 58). Rather, the vast majority of the population uses public communication services for the exercise of fundamental rights, in particular the freedom of expression, information and communication.

The second applicant submits that he is without previous criminal conviction. This applies to almost all individuals affected by the data retention. With regard to this majority, the limitation of the right to confidentiality of personal data in the sense of S 1 para. 1 DSG 2000 and the right of erasure under S 1 para. 3 DSG 2000 weighs particularly heavy.

2.3.14.5. According to the scope and nature of the data it applies that certain 'traffic data' and 'location data' are included in the storage obligation of S 102a TKG 2003, which are generated or processed in the course of the providing of public communication services. Traffic data means 'any data which is processed for the purpose of forwarding a message to a communication network or for the billing thereof' (S 92 para. 3 (4) TKG 2003). Location data is 'data processed in a communication network or by communication services and which indicate the geographical location of the telecommunication terminal equipment of a user of a public communication service and in the case of fixed telecommunication terminal equipment, the address of the institution are the location data' (S 92 para. 3 (6) TKG 2003). The storage of the content of communication, in particular, of data concerning the addresses accessed through the internet is expressly prohibited by S 102a para. 7 TKG 2003.

Irrespective of this, in the case of 'providing information' on retained data within the frame of S 135 para. 2a StPO and of S 53 SPG, it cannot be excluded that from the retained data conclusions can be drawn which are contrary to the right of confidentiality of personal data as it is guaranteed in S 1 para. 1 DSG 2000. In this respect, all the possibilities of the linking of data obtained in different contexts needs to be taken into consideration (...). Accordingly,

the interference with regard to the scope and nature of the stored data needs to be weighed heavily.

2.3.14.6. Moreover, it should be borne in mind that given the vast number of providers of public communication services and, therefore, the high number people obliged to store data, which is not transparent anymore, potentially have access to the stored data according to S 102a TKG 2003. This existing potential of abuse needs to be estimated in the assessment of the weight of the interference (cf. Decisions of the German Federal Constitutional Court BVerfGE 125, 260 [320]). It needs to be considered that the legislature took precautions against this risk, which exceed the requirements of the Data Retention Directive which the Court of Justice of the European Union declared to be inadequate (c.f. in particular the express obligation of encryption in S 94 para. 4 TKG 2003 and the technical and organizational measures of the Datensicherheitsverordnung [DSVO] adopted due to S 94 para. 4 TKG 2003 and the provision of Art. 7 of the invalid Data Retention Directive which in this regard is less extensive). In addition S 109 TKG 2003 contains penalty clauses which serve the protection against abuse. However, it needs to be stated that particular provisions are missing which criminalise the improper use of retained data by the provider under the obligation to store the data (see, however, S 301 Para. 3 StGB concerning the notifications relating to the content of results of providing information on the retained data):

2.3.14.7. In the Constitutional Court's decision for reference in (…) it has explicitly referred the Court of Justice of the European Union to the increased risk of abuse which is linked to data retention, because given the large number of providers of telecommunication services and, thereby, the vast number of individuals obliged to store data, which is not transparent anymore, have access to the stored traffic data which have to be retained for at least six months. The Court of Justice of the European Union came to the conclusion (*CJEU, Digital Rights Ireland und Seitlinger and others*, para. 66) that Art. 8 Charter of Fundamental Rights has the result that safeguards have to be created in order for retained data to be effectively protected against abuse risks and from unauthorized access and use. The same requirements exist under Art. 8 ECHR and S 1 DSG 2000.

S 102c TKG 2003 now provides for individual requirements concerning the security of the retained data and the recording of their access. S 109 para. 3 TKG 2003 contains further administrative penal provision (with the penalty of a fine up to €37 000.00) in cases where contrary to S 102a para. 8 TKG 2003 the data is not erased, where contrary to S 102b TKG 2003 data is provided without a judicial approval and where contrary to S 102b TKG 2003 data is not transmitted in an encrypted form over a communication network.

Firstly, it should be noted that (in the absence of criminal conduct) the 'mere' unauthorized use of data that is included in the storage of retained data, is not punishable by an administrative penalty, therefore, the abuse of this data is not governed by (administrative) criminal law. In addition, the hearing revealed that the Data Protection Commission or Data

Protection Authority has not acted since the enactment of the provisions on data retention for the verification of the compliance with these provisions.

2.3.15. Regardless of the fact that the legislator allows (S 102a para. 1 last sentence TKG 2003) the storage of data on the basis of S 102a TKG 2003, even though expressly and exclusively for the investigation, detection and prosecution of crimes the seriousness of which justifies an order according to S 135 para. 2a StPO, and thus creates a legally defined purpose, the storage already is an interference of particular weight.

2.3.15.1. It should be taken into account that the data of those affected who have given no reason for the storage and, therefore, do not stand in any relation to the stipulated purpose in S 102a para. 1 last sentence TKG 2003, are not provided with the right of erasure in S 1 para. 3 DSG 2000 (*cf. e.g. VfSlg. 16.150/2001*) which forms part of the fundamental right of data protection for the period of six or seven months (S 102a para. 8 TKG 2003) stipulated by S 102a TKG. In addition, the erasure request can only be made by those providers obliged to store data, where the affected person knows that the provider stored data relating to him. With regard to all providers who stored data concerning an individual who is not aware of this fact cannot exercise the right of erasure.

2.3.15.2. According to S 1 para. 4 DSG 2000 a limitation of the right of erasure – such as the limitations of the right in S 1 para. 1 DSG 2000 – is only permissible under the conditions mentioned in S 1 para. 2 DSG 2000. According to case law of the Constitutional Court (c*.f. e.g. VfSlg. 12.768/1991* for S 1 DSG 1978) the right of erasure according to S 1 para. 3 DSG 2000 (only) requires legal provisions which make provision for a specific right of erasure. However, the case law is contrary to any interpretation of such provisions, which fails to take S 1 para. 3 DSG 2000 into account or limits the right of erasure not sufficiently in accordance with the requirements of S 1 para. 2 DSG 2000.

2.3.15.3. In addition and with regard to S 135 para. 2a StPO, the obligation to store data according to S 102a TKG 2003 entirely loses its purpose which is expressly stated in S 102a para. 1 last sentence TKG 2003 due to the unconstitutionality and repeal of S 135 para. 2a StPO and the contested phrases of the mentioned provisions of the SPG (see above 2.3.11.6 and 2.3.13.3). Storage for retention without a specific purpose – even if it is only for a short period of time – would in any event be unconstitutional (…). Thus S 102a TKG 2003 – as well as the Data Retention Directive – does not fulfil the requirement of a connection between the retained data and the threat to public safety (*CJEU*, *Digital Rights Ireland und Seitlinger and others*, para. 59).

2.3.16. Furthermore, the regulations regarding the erasure of data are not specified in such a manner which would comply with the requirement of a statutory regulation within the meaning of S 1 para. 2 DSG 2000. In particular, it is unclear if the data which has to be stored due to the obligation S 102a para. 1 TKG 2003 is to be permanently erased (c.f. in this

context Art. 7 (d) of the unconstitutionally declared Data Retention Directive: 'the data, except those that have accessed and preserved, shall be destroyed at the end of the period of retention.').

2.3.16.1. Considering the severity of the interference in itself, the rules regarding the data retention – (…) – lack provisions which clarify for the individuals who are under the obligation to store and who are affected by the storage that with the term 'erasure' of the retained data the recoverability of the data has to be excluded (…). Nothing can change the practice of providers who probably already out of economic considerations 'overwrite' retained data and so ultimately prevent the data's recoverability, as well as the practice of courts and authorities who 'physically' erase provided data according to the relevant submissions in the hearing before the Constitutional Court. An 'erasure' in the sense that only the access to data which continues to exist (and which can be reconstructed) is prevented does not meet the strict constitutional requirements (see above 2.2.8.2). Since this is not expressly clarified by S 102a para. 8 TKG 2003 and other provisions, the requirement of a sufficiently precise legal basis (S 1 para. 2 DSG 2000) is not fulfilled with regard to the interference exercised according to S 102a para. 1 TKG 2003.

2.3.16.2. A deficiency in the legal basis is also present with regard to the obligations of the operators and authorities in connection with 'always-on service' (…). If an Internet access service is operated and used as an 'always-on service' the question arises at what time the 'communication' within the meaning of S 102a para. 1 TKG 2003 is deemed as terminated. The Federal Government argued at the hearing before the Constitutional Court that S 102a para. 1 and S 102a para. 2 TKG 2003 have to be interpreted in such a way that they are in conformity with the constitution, so that for Internet access services the communication should be seen as terminated within the meaning of S 102a para. 1 TKG 2003, with the withdrawal of the public IP address of the provider. Therefore, according to S 102a para. 2 TKG 2003 the data should be stored for six months from the time of the withdrawal of the public IP address by the provider.

2.3.16.3. Even if it is correct that the described interpretation can lead to a practical result, the mere possibility of such an interpretation is not able to sufficiently replace the legal determination of the interference with the fundamental right so that also in this case the strict requirements for the legal basis for the interference with the fundamental right of data protection (see above 2.2.8.2) are not fulfilled.

2.3.17. As a result, the applicants are, therefore, correct to the extent where they argued that the regulations are not proportional in their context. The limitations of the fundamental right of data protection according to the legal reservation in S 1 para. 2 DSG 2000 are only permissible based on laws, which are necessary for the reasons mentioned on Art. 8 para. 2 ECHR and which regulate in a sufficiently precise manner that is clear to everyone, the conditions under which the investigation or use of personal data for the performance of

specific administrative tasks is allowed. Legal limitations on the fundamental right of data protection have to be the least invasive method to achieve the objectives and have to be proportionally in the balance between the seriousness of the interference and the weight of the pursued objectives.

2.3.18. The regulations (S 135 para. 2a StPO in conjunction with S102a TKG 2003, S 53 para. 3a (3) SPG in conjunction with S 102a TKG 2003, S 53 para. 3b SPG in conjunction with S 102a TKG 2003) concerning data retention do not fulfil these requirements for the above reasons.

2.4. (…)

2.5. (…)