Balancing the interests in the context of data retention (INVODAS)

Austria

Prof. Dr. Nikolaus Forgó/Dr. Hartwig Gerhartinger

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

The Directive has <u>not</u> been transposed into Austrian law yet.

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?

The reason for the delay of the transposition process in Austria lies mainly in a combination of severe constitutional law concerns and serious scepticism within significant parts of the Austrian public about the retention of data for the purpose of criminal prosecution without any specific reason. NGOs managed to guarantee significant media coverage about the issue so that any political move in the arena will be intensively discussed.[1]

Another cause for the delay is that the transposition of the Directive in Austria affects the competencies of three ministries. Whereas the regulation of the duty to retain telecommunication data falls under the competency of the Federal Ministry of Transport, Innovation and Technology (BMVIT), adaptions in the field of criminal law (changes of the penal code and the criminal procedure code) underlie the competency of the Federal Ministry of Justice (BMJ). Finally, changes in the field of the security police underlie the competency of the Federal Ministry for the Interior (BMI). The separation of competencies made it necessary to compromise in the issue from the very beginning. This task has turned out to be especially difficult because of the political situation in Austria so that finally, general political reasons have to be considered: Austria's current government unites politicians from the social-democratic (SPÖ) and the conservative (ÖVP) party: Whereas the minister for infrastructure and telecommunication is a social-democrat, the ministers for justice and for the interior are conservative.

Already in spring 2007 the BMVIT presented a (first) ministerial draft[2] for the amendment of the Austrian telecommunication act 2003 (TKG 2003)[3] in order to implement the requirements of the Directive. Within the subsequent consultation process severe concerns were brought forward not only by private data protection organisations but also by official bodies like the Austrian Data Protection

---

1 See e.g. Kommenda, *Telekom-Daten: Lizenz zum Speichern - Gesetzesentwurf*, Die Presse 2007/20/01; Aichinger, *Doch noch Hoffnung auf Privatsphäre*, Die Presse 2009/08/06; Aichinger, *Datenspeicherung: Ausstieg möglich*? Die Presse 2009/51/01.

2 Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird, 61/ME XXIII. GP, http://www.parlament.gv.at/PAKT/VHG/XXIII/ME/ME_00061/imfname_076383.pdf.

3 Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 - TKG 2003), published in BGBl. I Nr. 70/2003, lastly changed by BGBl. I Nr. 50/2010.

Commission.[4] These critics challenged not only the constitutionality of the draft proposal but also the lawfulness of the Directive itself:[5]

It was pointed out that the retention of telecommunication data for prosecution purposes without any (concrete/reasonable) suspicion constituted a massive intervention into the basic rights provided by the ECHR (art. 8) and the Austrian constitutional law. Such an intervention could – if at all – only be justified if it was appropriate and proportional. The comprehensive storage of communication data provided by the Directive, however, was in the critique seen as ineffective and therefore inappropriate in order to prevent organised crime, as criminal organisations could easily circumvent the storage of their communication data by choosing providers domiciled outside the EU or by using prepaid mobile telephony services.

In addition, the critics held that the scope of intervention according to this ministerial draft was too wide, since access to the retained data would have been granted even for the investigation, detection and prosecution of minor criminal infringements, like stalking or dangerous threat. Thus, the legal possibilities to access retained data according to the ministerial draft would have gone beyond those provided by the Directive. Apart from that, the legal requirements for the storage of and the access to retained data were criticised as vague and unclear. Furthermore, the critics pointed out that there were no provisions as to the security of the retained data.

Due to these mainly constitutional concerns the transposition process was at first deferred and finally came to a halt, when premature parliamentarian elections in summer/autumn 2008 took place. At the same time, in the light of the proceedings Ireland / Council and Commission before the ECJ, C-301/06, concerning a potential unlawfulness of the Directive for formal reasons, a public debate restarted in Austria about whether the Directive had to be transposed into Austrian national law at all.[6]

In April 2009, the Commission decided to bring an action against Austria because of the non-transposition of the Directive (treaty violations proceeding under art. 226 EC/art. 258 TFEU).[7] As a consequence the BMVIT invited the Ludwig Boltzmann Institute of Human Rights (BIM)[8] – which in February 2008 already had been assigned to elaborate a comparative study on the status of application of the

---

4 The law proposal of the BMVIT as well as the respective statements within the consultation process are published at http://www.parlament.gv.at/PAKT/VHG/XXIII/ME/ME_00061/index.shtml.

5 The main arguments of the various parties are summarised in the answers to questions 45 and 49 below.

6 See e.g. Aichinger, *Doch noch Hoffnung auf Privatsphäre*, Die Presse 2009/08/06; Aichinger, *Datenspeicherung: Ausstieg möglich?* Die Presse 2009/51/01.

7 ECJ, 29 July 2010, C-189/09, European Commission / Republic of Austria.

8 The Ludwig Boltzmann Institute of Human Rights (BIM) is a non governmental and non profit research organisation established in 1992. It aims to contribute to the scientific human rights discourse at the national, European and global level. For further information see http://bim.lbg.ac.at.

Directive[9] – to prepare a draft act transposing the Directive to Austrian law.[10] The draft proposed by the BIM as well as its comments were transferred word by word into a new ministerial draft published in September 2009.[11]

Also the BIM itself stressed serious concerns about the lawfulness of the Directive public (especially in the light of the coming into force of the Charter of fundamental rights of the European Union, art. 7 and 8) and stated that it was not at all or at least very hardly possible to transpose the Directive into the national law in a way that would be in line with the ECHR and the Austrian constitution. Therefore the aim of the proposal was to find a solution to transpose the Directive in a way that provided as much safety elements as possible and interferes the least with fundamental rights of users. The concerns raised by the BIM and later within the consultation process of the second draft act[12] were also presented by the Austrian government within the treaty violations proceeding before the ECJ. Nevertheless Austria was convicted for the non-transposition of the Directive in June 2010.[13] The ECJ however did not take a position regarding the constitutionality of the Directive, since this question was not subject to the proceeding.[14]

In the following the media, in particular the print-media, reported on the ECJ proceedings about the potential unlawfulness of the Directive and, thus, increased the pressure on the Austrian government not to transpose the very unpopular Directive.[15] In this context the Austrian government decided to postpone the transposition of the Directive once again until the end of these proceedings.

3. Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?

In a recent response to a parliamentary request the federal minister of transport, innovation and technology declared that the present ministerial draft of 2009 (novel to the TKG 2003) had already been completed in due consideration of the responses received in the first consultation process.[16] This amended draft version was

---

9 http://bim.lbg.ac.at/de/projekte-datenschutz/rechtsvergleichende-analyse-hinblick-umsetzung-richtlinie-200624eg-ueber-vorrat.

10 http://bim.lbg.ac.at/de/informationsgesellschaft/bimentwurf-zur-vorratsdatenspeicherung-begutachtung.

11 http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00117/imfname_173172.pdf.

12 http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00117/index.shtml.

13 http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=de&newform=newform&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&radtypeord=on&typeord=ALL&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=C-189%2F09&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=&resmax=100&Submit=Suchen.

14 See Gerhartinger, *Anmerkung zu EuGH 29. 7. 2010, C-189/09*, jusIT 2010/80, 172.

15 See e.g. Aichinger, *Doch noch Hoffnung auf Privatsphäre*, Die Presse 2009/08/06; Aichinger, *Datenspeicherung: Ausstieg möglich?* Die Presse 2009/51/01.

16 http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00117/index.shtml.

published[17] and constitutes the basis for the following remarks. It only exists in a German version.

In her response[18] the minister announced, however, that the amended draft version would not be submitted to the Austrian parliament before the European Commission had published the report about the transposition of the Directive, which is currently drafted (publication due in autumn 2010, but delayed[19]). This announcement has to be seen in context of a the ongoing preliminary ruling procedure at the ECJ, brought by the Irish High Court, where the ECJ has to deal with constitutional law concerns as to the Directive for the first time.

For all this it seems that (a significant part[20] of) the Austrian government is still hoping for the chance that the Directive is declared unlawful on a European level so that a transposition of the Directive into Austrian national law becomes obsolete. At the same time the Austrian government communicates that it will be prepared to transpose the Directive, in order to avoid another conviction through the European Court of Justice (ECJ), which then would implicate a fine against Austria.

In this context it has to be pointed out that the present ministerial draft act covers only one part of the rules required for the full implementation of the Directive. In order to fully transpose the Directive into Austrian law further amendments to the Austrian code of criminal procedure (Strafprozessordnung, StPO),[21] the security police code (Sicherheitspolizeigesetz, SPG)[22] and the copyright act (Urheberrechtsgesetz, UrhG)[23] would be necessary. These issues, however, are under the competence of the Federal Ministry of Justice (BMJ) and the Federal Ministry for the Interior (BMI), which have not presented corresponding ministerial drafts yet. So, as for the moment, it is not foreseeable, when the transposition process will be finalised.

4. In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or

---

17 http://static2.orf.at/vietnam2/files/futurezone/201030/tkg__2010_data-retention_124398.pdf.

18 Response of the Federal Minister of Transport, Innovation and Technology, 5629/AB XXIV.GP, 27.07.2010, http://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_05629/imfname_193454.pdf.

19 See for example http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

20 As mentioned, there are different point of views at stake: The minister for Justice publicly supports the Directive and its implementation, see for example http://www.justiz.gv.at/internet/html/default/2c94848525f84a630126d60a672a0492.de.html;jsessionid=988456CEDFBEAFE47BEEFA3404877DA3.

21 Strafprozessordnung 1975 (StPO), published in BGBl. Nr. 631/1975, lastly changed by BGBl. I Nr. 64/2010.

22 Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), published in BGBl. Nr. 566/1991, lastly changed by BGBl. I Nr. 133/2009.

23 Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz, UrhG), published in BGBl. Nr. 111/1936, lastly changed by BGBl. I Nr. 58/2010.

for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.

(Q 7) Type of provisions transposing the Directive

According to sect. 2 of the Austrian data protection act (Datenschutzgesetz, DSG 2000)[24] the legislation and enforcement in the field of the protection of automation supported data processing are under the competency of the federal authorities.[25] The proposed draft rules are simple acts of the Austrian parliament. Certain primarily technical or organisational aspects may be regulated by a detailed regulation issued by the competent minister (Verordnungsermächtigung, power to issue statutory instruments).

(Q 8) Terms defined in art. 2. sub. 2 of the Directive also defined within the national law transposing the Directive

The Austrian TKG contains a set of general definitions in its sect. 3 and a set of specific definitions relevant for its chapter 12 concerning the secrecy of communication and data protection in its sect. 92 sub. 3.

Sect. 92 sub. 3 already contains several definitions literally corresponding to definitions given by art. 2 of the Directive 2002/58/EC. This is true for the terms "user" (para. 2), "traffic data" (para. 4), "location data" (para. 6), "communication" (para. 7), "call" (para. 8), and "value added service" (para. 9).

Further, sect. 92 sub. 3 TKG contains a definition of the term "*Anbieter*" (provider/operator of public communication services, para. 1) as well as it defines different data categories:

- the term "*Stammdaten*" (master data, para. 3) comprehends any personal data necessary to establish, process, change, and terminate the contractual relationship between the provider and the subscriber or to create and edit the subscriber lists;

- the term "*Zugangsdaten*" (access data, para. 4a) describes the traffic data, that are created at the provider, when the subscriber accesses the communication network, and which are necessary to assign the network address used for a communication at a certain point in time to a subscriber;

- the term "*Inhaltsdaten*" (content data, para. 5) comprehends the content of any transferred communication.

The new definitions given by art. 2 para. 2 of the Directive, according to the proposed draft, shall systematically be implemented in the already existing catalogue of definitions in sect. 92 para. 3 TKG. However, only two of these

---

[24] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), published in BGBl. I Nr. 165/1999 lastly changed by BGBl. I Nr. 133/2009.

[25] For further information see *Jahnel*, Datenschutzrecht (2010), nn. 3/2 ss.

definitions shall be transposed literally. This is the case for the terms "cell ID" (sect. 92 sub. 3 para. 6a TKG-draft) and "unsuccessful call attempt" (sect. 92 sub. 3 para. 8a TKG-draft).

We would like to point out that the draft proposes to introduce a distinction between the terms "*Benutzer*" ("user") and "*Teilnehmer*" ("subscriber") by including a new para. 2a to sect. 92 sub. 3 TKG-draft. By „user" the draft rules mean the originator of a conversation, whereas the term „subscriber" denotes the person who concluded the contract with the service provider. Since only natural persons can conduct a communication, the draft rules did not include legal persons into the existing definition of the term "user".[26] The legal definition of "user", thus, differs from the concept of the Directive according to which this term also comprehends legal persons (art. 2 sub. 2 lit. b).

Within the explanatory notes it is argued that in the majority of the cases the provider will only be able to reliably identify the subscriber, but not the originator of a specific communication. Therefore it is held sufficient that the communication is relatable to a "subscriber identification" (*Teilnehmerkennung*). The providers do not necessarily have to identify their customers.[27]

In contrast to the Directive the ministerial draft does not contain a definition of the term „data" corresponding to art. 2 para. 2 lit. a of the Directive, since sect. 93 sub. 3 TKG already contains a whole set of definitions of different data categories.[28] In sect. 92 sub. 3 para. 6b, however, the TKG-draft provides a definition of the term „*Vorratsdaten*": This term describes all data retained exclusively on the basis of the retention obligation provided by sect. 102a TKG-draft.

The term "retained data" does not constitute a new category of data within the (aforementioned) existing range of data categories; it rather refers to the purpose of storage of the data. As a consequence sect. 102b TKG-draft regarding the disclosure duty with regard to retained data and sect. 102c TKG-draft regarding the security and logging of retained data are only applicable if "operational" purposes (such as billing) for storing communication related data have ceased to exist. This leads to the still unsolved question when this is the case and if the storage of traffic and location data is at all necessary for operational purposes like billing, e.g. if the subscriber disposes of a flat-rate access to communication services. The national data protection authority answered negatively on this question.[29] The same is true for the cell-ID, which generally is not necessary for billing purposes. Hence, some data of a communication that have to be stored by a service provider are to be qualified as "Vorratsdaten" from the moment of their creation.

---

26 The definition of "master data" (para. 3) though, is amended insofar as also the data of legal entities is included.

27 See p. 35 of the BIM-draft.

28 These are the terms: master data (para. 3), traffic data (para. 4), access data (para. 4a), content data (para. 5) location data (para. 6).

29 See Datenschutzkommission, Recommendation K213.000/0005-DSK/2006, http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20060929_K213000_0005_DSK_2006_00/DSKTE_20060929_K213000_0005_DSK_2006_00.html.

Dimension 1 (State – citizen)

(Q 9) Data to be retained

Under Austrian law public telecommunication service providers are already entitled to store telecommunication data (traffic data and location data) for operational purposes, e.g. the conveyance of a communication or the billing thereof. Providers generally store this information for the period of (at least) 3 months.[30]

According to the draft act providers will have to retain specific data (especially IP-addresses and location data) for the period of six months from the time of their creation (sect. 102a TKG-draft).

What sort of data providers have to retain varies according to the services provided (see sect. 102a sub. 2 to 4 TKG).

Providers of internet access services have to retain the following data (sect. 102a sub. 2 TKG-draft):

1. name, address and ID of the subscriber to whom a public IP-address has been allocated at a certain point in time under specification of the time zone;

2. date and time of the assignment and the withdrawal of a public IP-address of an internet access service under specification of the time zone;

3. number of the calling telephone extension used for the access to the internet;

4. distinct ID of the extension used for the access to the internet.

Providers of public telephone services, including internet telephony services, have to retain the following data (sect. 102a sub. 3 TKG-draft):

1. subscriber ID or any other ID of the calling and the called extension;

2. in case involving supplementary services such as forwarding or call transfer, the subscriber number to which the call is routed;

3. name and address of the dialling and the called subscriber;

4. date, time of beginning, and duration of the communication process under specification of the time zone;

5. type of the service used (calls, supplementary services and messaging or multimedia services).

6. Concerning mobile telephony, further:

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

[30] See p. 31 of the BIM-draft.

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

c. date and time of the initial activation of the service and in case of a prepaid mobile service the location label (Cell-ID) from which the service was activated;

d. location label (Cell-ID) at the beginning of the communication process.

Providers of email services have to retain the following data (sub. 4)

1. ID of the subscriber;

2. name and address of the subscriber to whom an email-address has been allocated at a certain point in time;

3. for sending an email, the email-address and the public IP-address of the sender of an email as well as the email-addresses of all recipients of the email;

4. for receiving an email and the delivery to an electronic mailbox, the email-address of the sender and that of the recipient of the message as well as the public IP-address of the ultimate communication device;

5. for the logging in and out at email-services, date, time, subscriber ID and public IP-address of the subscriber under specification of the time zone.

Regarding unsuccessful call attempts[31] according to sect. 102a sub. 5 TKG-draft – in conformity with art. 3 para. 2 of the Directive – the retention obligation only exists where those data are generated, processed, and stored or logged by providers in the process of supplying the communication services. There is however no obligation for the providers to generate, process, store or log these data under Austrian law.

In addition, sect. 90 sub. 8 TKG-draft states that the providers of mobile communication networks have to keep records as to the location of the mobile devices (Cell-ID) which allows for the traceability of these devices at any time within the last 6 months.

In correspondence to the Directive, sect. 102a sub. 7 TKG-draft clarifies that the content of a communication, in particular the content of accessed websites, must not be stored under this provision.

(Q 10) Retention of electronic data beyond the data retained in accordance with the Directive

The Austrian government is trying to implement the Directive in such a way as to ensure the highest level of data protection. Therefore it seems unlikely that the retention obligation under Austrian law will go beyond the data retained in accordance with the Directive.

---

[31] This term is defined by sect. 92 para. 8a TKG-draft in conformity to art. 2 para. 2 lit. f of the Directive.

(Q 11) Purposes of the data retention

According to the draft rules[32] the data retained in accordance with sect. 102a TKG may only be used for the investigation, detection and prosecution of serious criminal offenses. Although this enumeration seems to be exhaustive, which means that the retained data must not be used for other purposes, as e.g. the prevention of crime, the TKG-draft allows access to retained data also in cases of emergency or where it necessary to prevent a danger for the life, health and freedom of a person (see also answer to question 15).

Which criminal offenses are to be considered as "*serious*" under this provision is was unclear for a long time, as this question concerns criminal law matters, which underlie the competency of the BMJ. The draft act (sect. 102b sub. 1 last sentence TKG-draft) presented by the BMVIT only referred to a – still not existing – catalogue of criminal offences within the StPO, which shall define which criminal offenses allow for access to the retained data. The BMJ, however, has not yet presented any proposal in this respect.[33]

The present "solution" is the outcome of an intensive debate about the scope of access to retained data in Austria. The first ministerial draft referred to sect. 17 SPG, which comprehends all criminal actions punishable with a prison term for over one year. This would have opened a wide access to the retained data, even for the investigation, detection and prosecution of crimes which are commonly perceived as minor offences. This proposal has therefore been heavily criticised as to wide, although it has to be acknowledged that Austrian criminal law (sect. 134 and 135 sub. 2 StPO) allows for access to the data of a communication (even its content) under similar circumstances.

Another possible solution would have been to refer to the term "Verbrechen" (felony) provided by sect. 17 StGB. This term describes an intentional act, which is punishable with a prison term for more than three years. This concept, however, seemed to be to narrow in some cases. Therefore, the BMVIT proposed in its draft to create a specific catalogue of criminal acts which should allow for the access to retained data.

In contrast to the Directive, the retention obligation according to the proposed draft act shall only apply to the providers of public telecommunications services, but not to providers of public communications networks. Within the comments to the draft

---

32 Sect. 102a sub. 1 last sentence TKG and sect. 102b sub. 1 last sentence TKG-draft.

33 The present text of the law refers to the general requirements to access data of a communication provided by sect. 135 para. 2 StPO. Accordingly access to retained data underlies the same conditions that apply to the access to other data of a telecommunication. Thus, on the one hand, a certain level of uniformity regarding access to communication data on the basis of the StPO is achieved. On the other hand, it has to be pointed out that the Austrian legislator has opted for very low access requirements. Upon explicit consent of the subscriber, access to retained telecommunication data already has to be granted in case of criminal offences with a maximum prison term of more than six months. According tot he explanatory notes this shall enable to access retained data in order to prosecute crimes like "cyber-stalking" (sect. 107 para. 2 StG) and child pornography (sect. 207a para. 3 StGB).

it is stated that there were no cases conceivable where the data to be retained under sect. 102a sub. 2 to 4 TKG is exclusively stored at the network providers, so that the standards set by the Directive were met. By excluding network providers from the retention obligation a redundant storage of the date should be avoided.[34]

(Q 12) Retention and/or transmission of sensitive data

The initial version of the second draft act contained no special rules regarding the retention and/or transmission of "sensitive data". Due to severe criticism put forward within the consultation process by, in particular, the Austrian bar association[35] as well as journalist organisations[36] a new sub. 5 shall be inserted to sect. 93 TKG, according to which it is not allowed to circumvent the journalist's privilege (sect. 31 Mediengesetz)[37] and other statutory confidentiality obligations (protected by the right to refusal to give evidence according to sect. 157 StPO) by transmitting data on the basis of the TKG.

In order to guarantee this, a new independent agency shall be installed by order of the competent ministries (BMVIT and BMI), so that the retained data shall not be transferred directly to the demanding authority. This (clearing-)agency will have to make the transmitted data anonymous, if the subscriber belongs to a protected group listed on a blacklist.[38] The transmission of retained data to the demanding authority is only licit in accordance with sect. 144 sub. 3 StPO. Thus, retained data of e.g. a lawyer or a journalist can only be accessed if these persons themselves are under suspicion.

As the creation of this agency as well as a detailed regulation about the transmission procedure will have to be made up by the competent ministries, no further information can be provided for the time being.[39]

---

34 See p. 51 of the comments to the BIM-draft.

35 Österreichischer Rechtsanwaltskammertag, 65/SN-117/ME XXIV. GP, pp. 4 s.

36 Österreichischer Journalisten Club, 2/SN-117/ME XXIV. GP, p. 2.

37 Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz - MedienG), published in BGBl. Nr. 314/1981, lastly changed by BGBl. I Nr. 8/2009.

38 Potential members of the protected groups, however, will not be automatically inserted into this list, but rather have to register in advance.

39 In the meanwhile this agency has been established by Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO). The text is available under: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2011_II_402/BGBLA_2011_II_402.pdf. This agency shall provide an electronic mailbox system for the safe handling of requests, that shall be located at the Bundesrechenzentrum GmbH (Federal Computing Centre). For each request a unique, clearly identifiable transaction number (unique ID) shall be used to verify the authenticity and to track the request. Thus, solely the unique ID and not the name of the requesting party will be used. The agency shall maintain appropriate log files in which the requests and the respecitve answers shall be recorded. According to sect. 23 TKG-DSVO these protocol files shall also be accessible to the Data Protection Commission, and the law enforcement officer at the Federal Ministry of Justice (BMJ), and the Federal Ministry of the Interior (BMI). Furthermore, these log files shall be used for statistical purpses. For further information please see Gerhartinger, *Österreich: Durchführungsverordnungen zur Vorratsdatenspeicherung erlassen*, ZD-Aktuell 2012, 02729.

(Q 13) Retention period

All data retained in accordance with sect. 102a sub. 2 to 4 TKG-draft have to be stored from the moment of their creation or processing until 6 months after the communication ended.

(Q 14) Authorities allowed to access the retained data

The conditions to access retained data are governed by sect. 102b TKG-draft. Sub. 1 of this provision states that access to data retained on the basis of sect. 102a TKG-draft must only be granted by virtue of a court order and only in accordance with statutory provision referring explicitly to sect. 102a TKG-draft. In addition, retained data must only be accessed by public authorities which according to the provisions of the StPO are competent to access data of a communication.

(Q 15) Use of the retained data

As explained in answer to question 11, retained data can be used for the investigation, detection and prosecution of serious criminal offenses defined by a (yet not existing) catalogue within the StPO (sect. 102b sub. 1 TKG-draft).

The draft, however, provides four exceptions from this in cases of emergency and for the prevention of danger.

1. The first exception concerns access of providers of emergency services to retained data. Already under the current sect. 98 TKG providers are obliged (upon request) to disclose master data as well as location data to providers of emergency services, if this is necessary to prevent an emergency. This rule shall be extended by a sub. 2, according to which – in case the current location cannot be determined – the cell ID at the time of the last communication of the person in danger may be processed even if this retained data is required (sect. 98 sub. 2 TKG-draft).
2. The second exception concerns the use of retained data for the investigation, detection and prosecution, even if the investigation does not concern a serious crime. In this case retained data may be processed upon court order, if it has not been stored longer than 3 months before the request (sect. 99 sub. 5 para. 2 TKG-draft).
3. The third exception concerns the processing of traffic data to security authorities in case of a concrete danger for the life, health or freedom of a person. The processing of retained data (cell ID of the last communication with the device of the person in danger) shall be permitted if the current location of the person in danger cannot be determined (sect. 99 sub. 5 para. 3 TKG-draft).
4. Exception four concerns the processing of traffic data in order to provide information about access data or email-data that have been stored on the basis of sect. 102a TKG-draft. These data may be accessed within three months after their storage. A prerequisite is, however, that these data are necessary to prevent a concrete danger for the life, health or freedom of a person (sect. 99 sub. 5 para 4. TKG-draft).

(Q 16 and 17) Requirements

The requirements are defined by sect. 102b sub. 1 TKG-draft. According to this provision, in general a court order is required. Exceptions are proposed for the cases of an emergency where the danger could not be prevented if a court order would have to be obtained. This might be true for cases where a person gets lost in the mountains (which in the debate is often mentioned as a positive "side-effect") or got kidnapped.

(Q 18) Information about the access to retention data

There are no provisions granting the aggrieved party the right to be heard or to be notified prior to the data access. Sect. 102a sub. 9 TKG-draft states that the information rights of the aggrieved party as to a data transfer effected in accordance with sect. 102b TKG-draft are those provided by the StPO. The relevant rules regarding the surveillance of and access to a communication are stated in sect. 134 ss. StPO.

Sect. 138 sub. 5 StPO only states that the prosecution department has to transmit its ordinance as well as the respective court order to the suspect immediately after the data has been accessed. This notification can however be postponed if an immediate transfer would jeopardize the purpose of these proceedings or any other proceedings against the suspect. As the postponement constitutes a further infringement of the aggrieved person's fundamental right to data protection, the court has to respect the principle of proportionality.[40] In any case, the suspect has to be notified about the access to his communication data with the notification about the indictment.[41]

As there is no prior notification of the aggrieved party, Austrian law provides for the information of a third party. This third party is the "legal protection officer" (*Rechtsschutzbeauftragter*), who has to control the ordinances of the prosecution department as well as the court orders and their execution (sect. 147 StPO).[42] Therefore the legal protection officer has to be informed about all steps within this procedure.[43]

(Q 19) Information about the data accessed

The aggrieved party's right to be informed about access to data of a communication is regulated by sect. 139 StPO. According to sub. 1 of this provision the suspect is granted to right to inspect all results of the surveillance measures effected against him/her. [44] As far as justified interests of third parties are concerned, the respective results can be restrained from this right. Sect. 139 sub. 2 StPO states that all persons

40 Reindl-Krauskopf, *WK-StPO*, §§ 137, 138 [48.].

41 From this time on he has full access to the official files (sect 51 sub. 2 StPO).

42 For further information see Reindl-Krauskopf, *WK-StPO*, §§ 146, 147 [1 ss.]

43 For further information see Reindl-Krauskopf, *WK-StPO*, §§ 146, 147 [6 ss.].

44 For further information see e.g. Reindl-Krauskopf, *WK-StPO* § 139 [1-5].

affected by inquiry measures (including access to retained data), have the right to inspect the files as far as the data contained are related to them.[45]

(Q 20) Recourse

The legal remedy against court orders is regulated by sect. 87 StPO (Beschwerde), This rule serves as a basis for an aggrieved party to seek recourse to the courts.

In addition, the aggrieved party can demand the deletion of the respective data in case the data was unlawfully accessed on the basis of sect. 139 sub. 4 StPO, if the data accessed cannot or must not be used in a trial against the aggrieved party.

(Q 21) Legal provisions protecting the data retained against unauthorised access in a particular way (not technical or organisational)

The security of retained data is regulated by the proposed sect. 102c TKG-draft. Retained data (data exclusively stored on the basis of sect. 102a sub. 2 to 4 TKG-draft) shall be marked since they underlie strict access and security standards. Therefore it is important, that retained data are distinguishable from data stored in accordance with the sect. 96, 97, 99, 101 and 102 TKG (proposed sect. 102c sentence 1 TKG). These data are to be protected against unlawful destruction, incidental loss or unlawful storage, processing, transfer or dissemination. Furthermore it has to be guaranteed that retained data can only be accessed by authorised persons.

The draft act however, does not regulate in detail, by which technical and organisational measures these requirements are to be achieved by the providers. It rather takes a technology-neutral approach by stating that the providers have to foresee capable technical and organisational measures in order to fulfil these requirements, although it provides that these requirements can be regulated in a more detailed way by the competent BMVIT.[46]

Furthermore the present draft act states that providers have to keep protocols about every access to the retained data as well as every request and every transfer of retained data (sect. 102c sub. 2 TKG-draft). These protocols have to contain specific data concerning to the authority requesting access to the retained data and the specific purpose of the request, the date of the request as well as the date and time of the transfer, the retained data accessed, the person to whom the data pertains, and the unique ID of the person accessing the data within the sphere of the provider (sect. 102c sub. 2 para 1 to 6 TKG). These protocol data have to be transferred to the data protection commission as well as to the BMJ upon request, and accordingly to

---

45 For further information see e.g. Reindl-Krauskopf, *WK-StPO* § 139 [6-9].

46 In the meanwhile the respective regulation has been issued by the BMVIT: Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO). The text is available under: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2011_II_402/BGBLA_2011_II_402.pdf. For further information please see Gerhartinger, *Österreich: Durchführungsverordnungen zur Vorratsdatenspeicherung erlassen*, ZD-Aktuell 2012, 02729.

the latter annually on the 31st of January. According to the revised draft act these data have to be stored for three years form the end of the retention period of a specific data (sect. 102c sub. 1 TKG). The compliance to these rules is controlled by the data protection commission (sect. 30 DSG 2000).

(Q 22) deletion of transmitted data

Data have to be deleted (ex officio) if they cannot be used anymore for proceedings against the aggrieved party (sect. 139 sub. 4 StPO).

Dimension 2: State – economy

(Q 23) Private bodies/enterprises obligated to retain data

The present draft act provides a conclusive list of telecommunication providers underlying the retention obligation (sect. 102a TKG-draft). These are providers of internet access services (sub. 2), providers of public telephony services including internet-telephony (sub. 3), and providers of email-services (sub. 4). Thus, in contrast to the Directive, the retention obligation applies only to providers of telecommunication services, whereas there is no such obligation for providers of public telecommunication networks. Within the comments to the draft it is stated that it was dispensable to provide a retention obligation for network providers, as the data that has to be retained was always stored in the sphere of the service providers as well. By excluding the network providers from the retention obligations a doubled storage of the communication data should be prevented.[47]

(Q 24) Exceptions

An exception for small telecommunications providers from the general obligation to retain data had already been provided by the initial draft act (proposed sect. 102a sub. 6 TKG-draft). According to this first version the retention obligation was not valid for enterprises which (upon prior decision) were classified as small or micro-enterprises in the sense of the Commission Recommendation of 6 May 2003, 2003/361/EG. The new sub. 6 to sect. 102a TKG refers to enterprises which are exempt from the payment of the financing fees provided by sect. 10 KommAustria-Gesetz.[48] This means that providers with an annual turnover of (at the moment) less than 315.000 Euro are not covered by the retention obligation.

(Q 25) Data categories that had to be retained before the Directive?

For a better understanding it has to be pointed out that the notion „retained data“ (*Vorratsdaten*) of the present draft comprehends only data which is not stored for any other reasons than for the retention obligation provided by sect. 102a TKG-draft.

---

47 See explanations to the proposed sect. 102a sub. 1 TKG.

48 Bundesgesetz über die Einrichtung einer Kommunikationsbehörde Austria ("KommAustria") und eines Bundeskommunikationssenates (KommAustria-Gesetz - KOG), published in BGBl. I Nr. 32/2001, lastly changed by BGBl. I Nr. 50/2010.

The prevailing norms of the TKG already provide the legal basis for the storage of several data necessary in order to comply with the contractual obligations of the providers of telecommunication services. According to sect. 97 sub. 1 TKG the providers are entitled to store and process master data for the conclusion, accomplishment, change and termination of the contract with the subscriber, as well as for billing purposes, the creation of subscriber directories or the providing of information to providers of emergency services. These data generally have to be deleted at the termination of the contract at the latest.

Furthermore, the providers have to store traffic data for billing purposes (sect. 99 sub. 2 TKG), until the period within which customers may object to the billing of the providers has expired.

(26) Data security (other than in Q 21)

Under Austrian law the general data security measures are regulated in sect. 14 and 15 data protection law ("Datenschutzgesetz", DSG 2000). According to sect. 14 DSG 2000 controllers or processors using data have to ensure that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons. Measures to be taken depend on the kind of data used as well as the extent and purpose of the use and have to consider the state of technical possibilities and economic justifiability. These measures must safeguard a level of data protection appropriate with regard to the risks arising from the use and the type of data to be protected. Sect. 15 DSG 2000 regulates the confidentiality of the data used.

(Q 27) Additional costs of the implementation

As the Directive has not been transposed yet, there is no data available on this issue.

(Q 28) Reimbursement for obligated parties

According to sect. 94 sub. 1 TKG the providers are obliged to provide the infrastructure necessary for the observation of the telecommunication including the access to retained data under the StPO. Sect. 94 sub. 2 TKG states that providers have to contribute to the observation of communications as well as to the access to data of a communication transfer and the access to retained data. For each of these obligations an adequate reimbursement of costs is provided in the respective provisions, i.e. the providers receive a reimbursement of their investments effected (sect. 94 sub. 1 TKG) as well as a reimbursement of the continuous costs generated by the transfer of information to the authorised bodies (sect. 94 sub. 2 TKG). The conditions and terms of these reimbursements are to be specified by regulations of the competent ministries.

(Q 29) Rules governing the cooperation

The general conditions of the providers to cooperate with the public authorities are provided by the aforementioned sub. 1 and 2 of sect. 94 TKG. Sub. 4 of this provision specifies the standards (encrypted transfer of an e-mail containing a

"comma-separated value"-file) for the transfer of traffic data, location data and master data, including the transfer of retained data according to the rules provided by the StPO and the SPG. The specification of a uniform standard of the syntax, data fields and encryption for the storage and transfer of the data is subject to an administrative regulation. This is also true for the standards regarding the storage and transfer of the access protocols in the sense of sect. 102c TKG.

(30) Sanction or obligations in case of an infringement

The proposed draft act provides primarily administrative sanctions in case of an infringement of the data retention provisions. These sanctions shall be inserted into the general catalogue of sanctions for infringements of the TKG provided in sect. 109 TKG.

In addition to these new provisions the general provisions of the DSG 2000 have to be taken into account. According to sect. 33 para. 1 DSG 2000 a controller or processor who has culpably used data contrary to the provisions of the DSG 2000 shall indemnify the data subject pursuant to the general provisions of civil law. The claim for appropriate compensation for the defamation suffered shall be brought against the controller of the data used.

Dimension 3: State – state

(Q 31) Public body responsible for establishing the contact with the party retaining

According to the revised draft act the data retained by the providers will not be transferred directly to the entitled public authorities, but via an agency, which has to be independent from the courts. This agency shall be installed by order of the competent ministries (BMVIT and BMI), so that for now further information (as e.g. to how the contact between the different actors shall be established) cannot be provided.

(Q 32) Regional entities granted their own rights to of access

There are no regional entities that have been granted their own rights of access to retained data.

(Q 33) Rules governing the co-operation among the different bodies

The present draft act does not contain any provisions governing the co-operation among the different bodies. Within the proposed sect. 102b TKG it is only stated that the data has to be stored in a manner that allows for an immediate transfer of the retained data according to the provisions of the StPO and the herein provided proceedings regarding the access to data of a telecommunication by the competent authorities. The TKG, thus, refers to the provisions of the StPO, which – as a general rule – provides in its sect. 145 StPO that all data gained from certain investigation measures (such as access to data of a telecommunication, sect. 135 StPO) have to be stored within the prosecution department in the first place. In case of a trial these data have to be submitted to the court, so that from the moment on no

data may be kept by the prosecution department. Finally, the data of a telecommunication has to be deleted, when the trial has finished, if the telecommunication data is not required as evidence in another criminal procedure.[49]

(Q 34) Legal basis for the exchange of retained data with other member states

The present draft act does not provide any specific rules regarding the exchange of retained data with other EU Member States, other EFA Member States or third countries. It rather provides that the retained data must only be transferred to public authorities appointed by the provisions of the StPO, which does not contain any rules allowing for a transfer of retained data to the authorities of other countries. If hereby a transfer of retained data to foreign authorities (e.g. on the basis of an co-operation agreement) should be prevented, is still unclear. As this is a question of criminal law falling under the competency of the BMJ, it has not been considered by the present draft.

(Q 35) Bodies in charge of monitoring compliance with national rules

According to the present draft rules (sect. 102c sub. 1 last sentence TKG) the Data Protection Commission shall be responsible for the supervision of the provider's compliance with the provisions established for the security of retained data. In order to ensure data security the BMVIT may concretise the required standard of care by a regulation.

The proposed sect. 102c sub. 1 TKG refers to sect. 30 DSG 2000, according to which anyone shall have the right to lodge an application with the Data Protection Commission in case of an alleged infringement of his rights or obligations concerning him pursuant to the DSG 2000 by a controller or processor. The Data Protection Commission shall have the right to examine data applications in case of reasonable suspicion of an infringement of the rights and obligations mentioned in sub. 1.

- ***If transposition has been <u>accomplished</u>:***

General questions

5. Is there an English version of the texts available? If so: Please indicate the respective URL.

6. Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?

[49] For further information see *Reindl-Krauskopf*, WK-StPO § 145 [1] ss.

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important" matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/ administrative provisions, and**

   b) **whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.**

8. **Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?**

Dimension 1 (State - citizen)

9. **What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?**

10. **Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.**

11. **According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?**

12. **Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?**

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefor.**

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?**

16. **Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?**

17. **Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?**

18. **Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?**

19. **Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?**

20. **May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?**

21. **Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.**

22. **When do the accessing bodies have to destroy the data transmitted to them?**

Dimension 2 (State – economy)

23. **Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.**

24. **Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?**

25. **Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?**

26. **Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?**

27. **Which *additional* costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate *in total* from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?**

28. **Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?**

29. **What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?**

30. **Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.**

Dimension 3 (State – State)

31. **Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?**

32. **Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?**

33. **What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?**

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies dispose of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

No.

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

Yes, ECJ, C-189/09.

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

As to our knowledge data retained shall be stored within the sphere of the respective service provider. The providers of telecommunication services are however allowed to assign this task to external companies. As there is no special provision on this question (within the present draft rules), the general rules regarding the legitimate committing of data for service processing permission to employ processors, provided by sect. 10 ss. DSG 2000, apply in this context. According to sect. 10 DSG service providers are permitted to employ processors for their data applications insofar as the latter sufficiently warrant the legitimate and secure use of data.[50] The controller has to contractually obligate the processor to comply to these standards and to control the processors compliance by acquiring the necessary information about the actual measures implemented by the processor. The obligations of the processors are established by sect. 11 DSG 2000.

The storage of retained data at a centralised level is not provided by the law.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

By the present draft act no rules are provided prohibiting the storage of retained data outside the country, so that the general rules of the DSG 2000 apply. The DSG 2000 differentiates between cross-border transmissions of data, which is not subject to licensing (sect. 12) and such cross-border transmissions which are subject to licensing (sect. 13).

According to sect. 12 DSG 2000 the transmission and committing of data to recipients in Member States of the European Union is not subject to any restrictions in terms of sect. 13 DSG. This does not apply to data exchange between public sector controllers in fields that are not subject to the law of the European Union. As the retention of telecommunications data is subject to European law, this exception

[50] In the case of the processing of retained data the spezial guarantees provided by the proposed sect. 102c TKG will have to be taken into account.

does not apply, so that the storage of retained data in other Member States does not require specific licensing.

In respect to the exchange of retained data with recipients in third countries, no authorisation is required if this third country provides an adequate level of data protection.[51]

The prerequisite for every transborder exchange of data is the legality of a data application in Austria according to sect. 7 DSG 2000. Furthermore, transborder transfers of data require the written assurance of the foreign processor to the domestic controller to respect the obligations of a processor according to sect. 11 sub. 1 DSG 2000.

40. Which technical and/or organisational measures ensure in practice that

a) no data are retained beyond what is permitted?

As the Directive has not been transposed to Austrian law yet, it cannot be said which technical or organisational measures the service providers will in practice seize in order to ensure that no data are retained beyond what is permitted. The Austrian legislator, however, intends to simplify this task insofar as providers are conceded a period of one month to erase the retained data after the expiration of the six months retention period.[52]

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

According to the present draft act the direct access to data retained shall be stored in the sphere the providers, so that there is no possibility for State bodies to directly access these data. By what technical or organisational means the telecommunication service providers will ensure that the data can only be accessed on the basis of a court order, cannot be said yet.

c) data are not used for purposes other than those they are permitted to be used?

Since the Directive has not been transposed yet, there is no information available as to the subject of this question.

---

51 The countries that have an adequate level of data protection are to be enumerated in an regulation of the Federal Chancellor in accordance with sect. 55 sub. 1 DSG 2000. Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (DSAV), BGBl. II Nr. 521/1999.

52 Proposed sect. 102a sub. 8 TKG-draft.

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

Since the Directive has not been transposed yet, there is no information available as to the subject of this question.

e) data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?

Since the Directive has not been transposed yet, there is no information available as to the subject of this question.

f) the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?

Since the Directive has not been transposed yet, there is no information available as to the subject of this question.

g) sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?

As already pointed out in our answer to question 12, the present draft act provides that the transmission of the data retained from providers to public authorities will be effected via a newly created agency. The technical and organisational measures to be taken by this agency are to be specified by an administrative regulation of the competent ministry.

41. Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?

The control of the compliance with the rules on data security and the establishment and execution of effective measures to ensure the security of the retained data is, according to the draft act, the task of the Data Protection Commission, sect. 102c sub. 1 TKG).

According to sect. 12 DSG 2000 the Data Protection Commission has the right to examine data applications upon the application of a data subject in case of an alleged infringement and in case of reasonable suspicion of an infringement of the rights and obligations provided by the DSG 2000, which is also applicable on retained data. It can ask the controller or processor of the examined data application to give all necessary clarifications and to grant access to data applications and relevant documents. For certain data a prior checking is provided.

42. What technical (*de facto* and/or *de iure*) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?

According to the proposed sect. 94 sub. 4 TKG the transmission of the retained data shall be effected via the encrypted transfer of an e-mail containing a "comma-separated value"-file. The CSV-format describes to structure of a text file for the storage and the exchange of simply structured data. As this file format can be used with all major database systems, it brings the advantage that both providers and public authorities do not have to provide particular technical requirements.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

Since the Directive has not been transposed yet, there is no information available as to the subject of this question.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

(At the moment, we have no information on this issue.)

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

As mentioned in the introduction (questions 1-4), the first ministerial draft proposal for the implementation of the data retention Directive into Austrian national law has already provoked a broad public debate and therefore lead to a high public awareness to this issue. Since then, even the mass print media regularly reported about ongoing proceedings before the ECJ and other Members states concerning lawfulness of the Directive or the constitutionality of respective national transpositions. Hence, it can be said that there is a high level of awareness as to this topic and a clear scepticism towards the Directive and the retention of data for the

purposes of criminal prosecution without any specific reason, which goes through all political parties and all social groups.

Within both consultation processes an unusual high amount of responses has been transmitted. Among the critics of the Directive the most relevant groups were NGOs, such as data protection organisations (e.g. ARGE DATEN) and animal rights groups, journalist organisations and the lawyers' chamber. Especially the NGOs managed to motivate a high amount of individuals to support their point of view in a written form by sending a short response as well.

The non-governmental data protection organisations point out that the retention of telecommunication data of all users without any specific suspicion constitutes a massive infringement of civil rights, such as the respect of privacy, the right of data protection, the secrecy of telecommunications and the right to free speech as well as the presumption of innocence.[53]

Journalist organisations postulated that the implementation of the Directive had to respect the freedom of press. As mobile telephony and the internet are the most frequently used means of communications for journalists to procure information, a total traceability of these telecommunication technologies would put the journalists´ work in danger.[54]

Within the national debate also the lawyers' organisations played a strong and active role, as they heavily criticized the Directive per se and the Austrian ministerial draft in the media.[55] They put forward that the ministerial drafts did not respect the professional secret of lawyers and, therefore, constituted a threat for their profession. In addition they stated that the conditions under which access to the retained data is granted was not sufficiently determined.[56]

On the other hand the proposed draft rules were criticized as to narrow, in particular by the film and music industry. Intellectual property management agencies as AKM[57] or VDFS[58] deplored that the scope of access to retained data was to narrow, as it did not allow for access in order to investigate and prosecute intellectual property infringements.[59] According to VDFS,[60] the limitation of access to retained data for the purpose of serious crime leads to a weakening of the position of the movie industry. The growing number of intellectual property infringements

---

53 Stellungnahme von: ARGE DATEN, 3/SN-117/ME XXIV. GP, 2.

54 Österreichischer Journalisten Club, 2/SN-117/ME XXIV. GP, p. 2.

55 This critic has also been brought to public, see *Gegen Überwachung: Anwälte aller Länder, vereinigt euch*, Die Presse 2010/06/04; Irene Brickner, *Anwälte gegen Datenspeichern*, Der Standard 2010/10/02.

56 See e.g. Bürstmayr, *Vorratsdatenspeicherung: Gefahr für den Anwaltsstand? Europäische Präsidentenkonferenz 2010*, AnwBl 2010, 171.

57 The acronym AKM stands for „Autoren/Komponisten/Musikverleger".

58 VDFS is the acronym for „Verwertungsgesellschaft der Filmschaffenden", which is an Austrian intellectual property management agency for makers of creative films.

59 AKM - Autoren/Komponisten/Musikverleger, 148/SN-117/ME XXIV. GP.

60 VDFS - Verwertungsgesellschaft der Filmschaffenden, 174/SN-117/ME XXIV. GP, p. 3.

committed over the Internet can only be prevented if the courts have access to the names and addresses of the respective Internet users. Furthermore this limitation of the access to data retained causes a conflict with the protection of property, which also comprehends „intellectual property".[61]

46. Are there any obligations in your country to retain other personal data without a *specific* reason (e.g. passenger name records (PNRs), employment data, etc)?

The Austrian data protection law is governed by the principle that the storage of data is only permitted if there is a specific reason for it. Therefore, as a general rule, data may only be kept in personal form as long as they are needed for the purposes they were data collected for.[62] A longer storage period, however, can be stated in specific laws, particularly laws concerning archives. There are numerous provisions concerning archives in the diverse laws, which cannot be outlined at this point. Nevertheless, the retention of data without such a specific reason is alien to the Austrian law, as these telecommunication data are not archived for historical/scientific purposes.

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

The data retention Directive has not been implemented into Austrian law yet, so that no such data is available yet.

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

The data retention Directive has not been implemented into Austrian law yet, so that no such data is available yet.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

As we have already pointed out, there is a clear preference in the Austrian public that the field of the data retained as well as the retention period should be set as narrow and short as possible. One of the crucial points of this discussion is the limitation of the access to retained data. The Directive merely states that the data retained should be used in case of "serious crime", leaving the definition of this notion up to the Member States.

---

61 Stellungnahme von: VDFS - Verwertungsgesellschaft der Filmschaffenden, 174/SN-117/ME XXIV. GP, 4.

62 Sect. 6 DSG sub. 5 2000.

The first ministerial draft referred to sect. 17 SPG, which comprehends all criminal actions punishable with a maximum prison term for over one year. This would have widely opened access to retained data, even for the investigation, detection and prosecution of crimes which are commonly perceived as minor offences. This proposal has therefore been heavily criticised as to wide, although it has to be acknowledged that Austrian criminal law (sect. 134 and 135 sub. 2 StPO) allows for access to the data of a communication (even its content) under similar circumstances.

Another possible solution would have been to refer to the term "Verbrechen" (felony) provided by sect. 17 StGB. This term describes an intentional act, which is punishable with a maximum prison term for more than three years. This concept, however, seemed to be to narrow in some cases. Therefore, the BMVIT proposed in its draft to create a specific catalogue of criminal acts, which should allow for the access to retained data.

The Austrian legislator however decided to refrain from introducing such a catalogue, referring to the general requirements to access data of a communication provided by sect. 135 sub. 2 StPO instead.[63] Accordingly access to retained data underlies the same conditions that apply to the access to other data of a telecommunication. Thus, on the one hand, a certain level of uniformity regarding access to communication data on the basis of the StPO is achieved. On the other hand, it has to be pointed out that the Austrian legislator has opted for very low access requirements. Upon explicit consent of the subscriber, access to retained telecommunication data already has to be granted in case of criminal offences with a maximum prison term of more than six months. According tot he explanatory notes this shall enable the competent bodies to access retained data in order to prosecute crimes like "cyber-stalking" (sect. 107 para. 2 StG) and child pornography (sect. 207a para. 3 StGB).

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications:

63 See sect. 135 sub. 2a StPO.

Which data are – according to national (constitutional) law[64] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a *specific* reason?

Under Austrian law the fundamental rights protecting privacy, personal data and the secrecy of telecommunications are mainly provided by the ECHR, which forms part of Austrian constitutional law and the Staatsgrundgesetz[65] (StGG). In addition to these non exhaustive lists of fundamental rights additional rules apply, eg art. 1 DSG 2000 giving everybody a fundamental right to privacy ("Grundrecht auf Datenschutz").

The rules of the ECHR on the protection of privacy and family life (art. 8 ECHR) and the freedom of speech (art. 10 ECHR) shall not be presented in detail here as they are sources of international public law without any particular Austrian peculiarity.

The StGG provides for the inviolability of the home (art. 9), the protection of the secrecy of letters (art. 10) and the secrecy of telecommunication (art 10a). The latter has been specified by sect. 93 TKG providing the secrecy of a communication on the basis of an ordinary law.[66] The secrecy of telecommunication encloses the content of a communication as well as the fact that a communication has taken place (i.e. traffic data). The secrecy of communication (sect. 93 TKG) prohibits the wiretapping, recording, intercepting and other types of surveillance of a communication and the respective traffic und location data. Surveillance may however take place with the consent of all users involved in the communication, the court permission to install a trap and trace device on the phone of a user or an emergency being present.[67]

The fundamental right to protection of personal data is granted by sect. 1 DSG 2000, which has the status of a constitutional provision. The Austrian data protection law is inter alia governed by the purpose limitation principle (Zweckbindungsgrundsatz).[68] Therefore, under the current data protection law, it is not legal to store personal data without a specific reason.

---

64 In the following, „national (constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

65 Staatsgrundgesetz vom 21. December 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder, published in RGBl. Nr. 142/1867, lastly changed by BGBl. Nr. 684/1988.

66 Since the secrecy of telecommunication does not only concern vocal communication but also written messages that are transmitted via a means of telecommunication, the fundamental rights on the protection of secrecy of letters and the secrecy of telecommunication can overlap.

67 Liebwald, *Die systematische Aufzeichnung der Daten über elektronische Kommunikation zu Überwachungszwecken - Richtlinie zur Vorratsdatenspeicherung 2006/24/EG*, jusIT 2010/27.

68 See sect. 6 DSG 2000. An inofficial translation of the DSG 2000 is available via http://www.dsk.gv.at/DocView.axd?CobId=41936.

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

The text of Art. 9 StGG does not provide for restrictions of the right to inviolability of the home, but declares the Act of 27th of October 1862 on the protection of domiciliary rights, in vigour since 18th of January 1863, as part of this provision.[69]

Art. 10 StGG provides that the confiscation of letters is, except in cases of a lawful imprisonment or the execution of a search warrant, only licit in events of war or on the basis of a judicial writ and in accordance with the law.

Art. 10a StGG provides that restrictions of the secrecy of telecommunication are only licit on the basis of a judicial writ and in accordance with the law.

Restrictions of to the fundamental right on the protection of personal data are (on the level of national constitutional law) governed by sect. 1 sub. 2 DSG 2000. According to this provision restrictions of the secrecy of personal data – insofar as it is not used in the vital interest of the data subject or with his consent – are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority. Restriction shall only be permitted based on laws. Further these restrictions have to be necessary for the reasons stated in art. 8 para. 2 of the ECHR. Such laws may provide for the use of data deserving special protection only if there is a substantial public interests. In addition they have to provide for suitable safeguards regarding 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.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

As the transposition process is still pending, there is no such jurisdiction yet.

53. Does national (constitutional) law safeguard an *absolute* limit as to the maximum degree to which public surveillance measures *collectively* may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

Such an absolute limit is neither part of existing constitutional law nor of the legal doctrine. The balance of interests has to be found on a case to case basis.

---

[69] Published in RGBl. 88/1862, changed by Gesetz vom 1. Oktober 1920, womit die Republik Österreich als Bundesstaat eingerichtet wird (Bundes-Verfassungsgesetz), BGBl. Nr. 1/1920 and Bundesgesetz vom 11. Juli 1974 über die Anpassung von Bundesgesetzen an das Strafgesetzbuch, BGBl. 422/1974.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

Professional groups like journalists, doctors or lawyers are protected by specific privileges concerning their duties to testify about data obtained in the course of their profession. However, these privileges are granted by ordinary law (f. e. § 31 Mediengesetz, "Redaktionsgeheimnis"). No specific, national fundamental rights exist on a constitutional level.

In a case decided by the Austrian Constitutional Court[70] the claimants had argued that certain provisions of the SPG on privacy had to be seen as specifically sensitive when individuals being objects of these provisions had professions where it happens on a regular basis that they are confronted with sensitive information. The Constitutional Court did not follow this argument.

It is however clearly seen that the protection of journalistic sources ("Redaktionsgeheimnis") is an outcome of art. 10 ECHR.[71] One can therefore argue[72] that a transposition of the directive without any specific guarantee for journalists and similar professional groups might be at risk of possibly infringing art. 10 ECHR as a "chilling effect" hindering sources to speak with journalists might occur.[73]

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national

---

70 VfGH 01. 07. 2009, G 147, 148/08, http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/8/0/CH0006/CMS1247635915839/spg_g147-08.pdf.

71 See in particular OGH, 16. 12. 2010, 13Os130/10g (13Os136/10i), https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20101216_OGH0002_0130OS00130_10G0000_000/JJT_20101216_OGH0002_0130OS00130_10G0000_000.html: "

72 See http://www.heise.de/newsticker/meldung/Oesterreich-Redaktionsgeheimnis-gilt-auch-fuer-oeffentliche-Aeusserungen-1155192.html for such an argument provided by one of the authors of this paper.

73 OGH, 16. 12. 2010, 13Os130/10g (13Os136/10i: "Sicherstellung von einem Medium recherchierten Materials stellt einen Eingriff in das Grundrecht auf Freiheit der Meinungsäußerung nach Art 10 Abs 1 MRK dar, ist doch der Schutz der Vertraulichkeit journalistischer Quellen eine der Grundbedingungen der Pressefreiheit und bildet somit einen wesentlichen Bestandteil der konventionsrechtlichen Garantie. Ohne solchen Schutz könnten Quellen abgeschreckt werden, Medien dabei zu unterstützen, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren („chilling effect"). Dies könnte zur Folge haben, dass die lebenswichtige öffentliche Funktion der Medien als „Wachhund" („public watchdog") beeinträchtigt und ihre Fähigkeit, präzise und verlässliche Informationen zu bieten, nachteilig berührt werden (EGMR 27. 3. 1996 [Große Kammer], Nr 17488/90, Goodwin gg Vereinigtes Königreich, ÖJZ 1996/28 [MRK]; 15. 12. 2009, Nr 821/03, Financial Times ua gg Vereinigtes Königreich, uva)."

(constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

Providers of telecommunication and internet services already store traffic data for operational and billing purposes. The duty to store this data longer than necessary causes additional investments and costs for the providers. This obligation affects the right of property protected by art. 5 StGG and art 1. Protocol 1 ECHR. These provisions not only cover cases of expropriation but also cases of restriction of the proprietor's right to dispose about his property, which is the case for the retention obligation under the Directive. Furthermore, the retention obligation affects the right to equality before the law, provided by art. 7 B-VG (general principle of equality), art. 2 StGG and art. 66 StV St. Germain, and the freedom to practise a trade or occupation based on art. 6 StGG.[74]

Art. 5 StGG as well as art 1. Protocol 1 ECHR contain formal reservations of statutory powers, so that restrictions may only be effected on the basis of statutory provisions. In addition, the restrictions have to serve public interests, must be proportional and must not affect the essence of the fundamental right.[75] The Austrian Constitutional Courts already clarified that the investigation of criminal actions by surveillance of telecommunication services (sect. 148a ss. StPO) constituted a task of public interest, which for reasons of effectiveness required the cooperation of the private telecommunication providers.[76] This jurisdiction may also be applicable on the obligation of telecommunication providers to store data for a certain period.

This infringement of the fundamental right of the telecommunication service providers can only be qualified as constitutional, if an adequate compensation is provided.[77] The Austrian doctrine deduces a right to adequate compensation directly of art. 5 StGG. According to the constant jurisdiction of the Austrian high courts (the Austrian Supreme Court, OGH, and the Austrian Constitutional Court, VfGH) a right to adequate compensation on the basis of art. 5 StGG is denied.[78] Although this jurisdiction has experienced severe criticism within the doctrine it has never been "formally" revised.[79] Nevertheless the Austrian jurisdiction grants a right to adequate compensation for the infringement of the right to property on the basis of

---

74 See Kastelitz, *Vorratsdatenspeicherung und Kostentragung – Grundrechtsfragen bei der Indienstnahme Privater zur Erfüllung öffentlich-rechtlicher Aufgaben*, jusIT 2010/28, pp. 67 s..

75 Walter/Mayer/Kucsko-Stadlmayer, *Grundriss des österreichischen Bundesverfassungsrechts* (10th edition, 2007), Rz 1485.

76 VfGH 27th of february 2003, G 37/02 et al., V 42/02 et al., available on the internet under: http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vfgh&Dokumentnummer=JFR_09969773_02G00037_01.

77 As to the concept of this term see answer to question 57.

78 For references see Kastelitz, *Vorratsdatenspeicherung und Kostentragung – Grundrechtsfragen bei der Indienstnahme Privater zur Erfüllung öffentlich-rechtlicher Aufgaben*, jusIT 2010/28, p. 68 fn. 29.

79 Walter/Mayer/Kucsko-Stadlmayer, *Grundriss des österreichischen Bundesverfassungsrechts* (10th edition, 2007), Rz 1482.

the general principle of equality provided by art. 7 B-VG ("Sonderopfertheorie").[80] For cases of expropriation the courts always grant compensation. In cases of a restriction of the use of one's property, which would be the case for the retention obligation under the Directive, it has to be differentiated between restrictions which trigger a duty of compensation and (minor) restrictions which have to be accepted without being compensated. It is estimated that the additional storage obligation may cause costs from 2 Euros/customer in the first year to 1 Euro/customer in the following years. Regarding these significant costs it would have to be considered unconstitutional to provide for on obligation to retain data without granting an adequate reimbursement.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

The present draft act provides a conclusive list of telecommunication providers underlying the retention obligation (sect. 102a TKG-draft). These providers have to retain closer specified telecommunication data for the purposes of investigation, detection and prosecution of serious criminal offenses. In addition, the TKG-draft allows access to retained data also in cases of emergency or where it is necessary to prevent a danger for the life, health and freedom of a person (see also answer to question 15). The role of the service providers is to retain the telecommunication data, even if these are not necessary for their operational purposes such as billing purposes, in a first step, and to transmit these data upon request.

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

As already pointed out in answer to question 55, a transfer of the public duty to retain telecommunication data to private parties without any compensation of the associated additional costs would constitute an infringement of the principle of equality before the law. Regarding the principle of proportionality it seems disproportional that providers have to bear the (significant) costs of the additional retention of data.

This, however, does not necessarily mean that providers have the right to full reimbursement of costs caused by obligation to retain telecommunication data. In order to facilitate administration of the compensation of the obligated parties the Austrian law provides for an "adequate indemnity" (angemessene Schadloshaltung, sect. 365 of the Austrian General Civil Code).[81] Therefore, in cases where it seems appropriate, the reimbursement can be effected on the basis of calculating average costs or as compensation at-large.

---

[80] For references see Kastelitz, *Vorratsdatenspeicherung und Kostentragung – Grundrechtsfragen bei der Indienstnahme Privater zur Erfüllung öffentlich-rechtlicher Aufgaben*, jusIT 2010/28, p. 68.

[81] Kastelitz, *Vorratsdatenspeicherung und Kostentragung – Grundrechtsfragen bei der Indienstnahme Privater zur Erfüllung öffentlich-rechtlicher Aufgaben*, jusIT 2010/28, p. 68, with further references.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

According to art. 65 B-VG the Federal President is authorised to sign international treaties in accordance with a respective recommendation of the Federal Government or a minister authorised by the Federal Government to make a recommendation in a certain issue. Under art. 50 B-VG some international treaties require the approval of the National Assembly (and in some cases of the Federal Assembly). This is true for political international treaties, international treaties changing or amending national law, and international treaties changing the contractual basis of the EU.[82]

International treaties have to be implemented into Austrian national law. This implementation can be effected by a special transformation or a general transformation. In case of a special transformation the Austrian legislator creates new national rules transposing the obligations provided by the international treaty. In this case, only the national rules regulate the rights and duties of the parties, whereas the parties cannot base claims on the text of the international treaty. In case of a general transformation the rules of the treaty are set into force as they are by a legislative act, so that individuals can, in principle, directly refer to the rules of the international treaty. If a generally transformed rule is directly applicable on national level depends on the level of determination of the granted rights (self-execution/non self-executing rules of public international law).[83]

The rules of the ECHR[84] have been adopted to Austrian law by general transformation through the constitutional act of 4th of march 1964.[85] According to art. II para. 7 of this act the ECHR has the status of national constitutional law. This means that the rules of the ECHR (and the ratified protocols 1, 4, 6, 7 and 13) are applicable as they are provided by the international treaty.[86] The fundamental rights provided by the ECHR are, therefore, on the same level as those provided by the Austrian StGG and other rules granting fundamental rights.[87]

---

82 For further information see e.g. Berka, *Verfassungsrecht – Grundzüge des österreichischen Verfassungsrechts für das juristische Studium* (third edition, 2010), nn. 261 ss..

83 For further information see e.g. Berka, *Verfassungsrecht – Grundzüge des österreichischen Verfassungsrechts für das juristische Studium* (third edition, 2010), nn. 248 ss..

84 Published in BGBl. Nr. 210/1958.

85 Published in BGBl. Nr. 59/1964.

86 For further information see e.g. Öhlinger, *Verfassungsrecht* (8th edition, 2009) p. 86.

87 For further information see e.g. Öhlinger, *Verfassungsrecht* (8th edition, 2009) pp. 86 ss..

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

There are no configurations where a Directive is conceded a particular status within the hierarchy of norms in Austria.

The transposition process is in most cases launched by a ministerial law proposal of the competent ministry. In case the competencies of different ministries are affected, these ministries have to cooperate in order to develop a common proposal. After this proposal has been submitted to the National Assembly, it is generally delegated to the competent committee, where it is discussed by representatives of the parties of the Parliament. It is then (possibly in an amended version) presented to the plenum of the National Assembly, where three readings of the law proposal are conducted; the third reading most commonly is waived.

After the law proposal has been adopted, it is passed on to the Federal Council (Bundesrat), which in the majority of the cases only has a suspensory veto against decisions of the National Assembly, except when its own competencies or the competencies of the Federal States are affected. If the Bundesrat endorses the law proposal, it is submitted to the Federal President, who by his signature certifies the constitutionality of the legislation process of the respective act. The prospective act is countersigned by the Federal Chancellor. The act, finally, has to be published in the Federal Law Gazette (Bundesgesetzblatt). If not stated otherwise, it becomes law the day after the publication.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

Austria's entry to the EU went hand in hand with a far-reaching transfer of legislative competences to the institution of the EU, by which several of the fundamental principles of the Austrian constitutional system have been affected. According to art. 44 sect. 3 B-VG a modification of the fundamental principles of the constitution require a national referendum.

According to ECJ decisions the whole EC Law (even secondary legislation) has primacy over state law, including constitutional law. Although this principle is not accepted by the jurisdiction of several Member States, the Austrian Constitutional Court has assumed this primacy in his decision VfSlg 15.427/1999 and VfSlg 17.065/2003.[88] Nevertheless it is commonly stated that this primacy does not regard the fundamental principles of the Austrian constitution, so that these fundamental principles are regarded as a barrier for integration.[89] According to this view a future

[88] Öhlinger, *Verfassungsrecht* (8th edition, 2009) n. 157.

[89] Öhlinger, *Verfassungsrecht* (8th edition, 2009) n. 158.

amendment of primary legislation leading to a change of one or more of the leading principles of the Austrian constitution would require a national referendum. If an act of secondary legislation leads to such a change, it would have to be considered null and void without a precedent referendum.[90]

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

As pointed out in answer to question 2, the transposition of the Directive in Austria affects the competencies of three ministries: The BMVIT (regulation of the duty to retain telecommunication data), the BMJ (responsible for the adaption in the field of criminal law – changes of the penal code and the criminal procedure code) and the BMI (security police). Regional territorial entities have no competencies regarding the transposition of the Directive.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

There are no national constitutional provisions specifically limiting the transmission of retained data to other countries. General rules apply.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

The main option is an ongoing public debate about the legal and political implications the transposition of the Directive will have when Parliament will finally start dealing with a proposal for the law developed by all three competent ministries.

[90] Öhlinger, *Verfassungsrecht* (8th edition, 2009) n. 158.

Balancing the interests in the context of data retention (INVODAS)

Austria

Prof. Dr. Nikolaus Forgó and Dr. Hartwig Gerhartinger

Part 2: Overarching issues and country-specific questions

A. General part (Questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

As already stated in the first questionnaire[1] Austrian constitutional law provides for the secrecy of a telecommunication (Art. 10a StGG). An intervention may only be effected on the basis of a court order in accordance with the law. Art. 10a StGG has been specified by sect. 93 TKG providing for the secrecy of a telecommunication on the basis of an ordinary law. Sect. 93 TKG generally prohibits the wiretapping, recording, intercepting and other types of surveillance of a communication and the respective traffic and location data. A surveillance measure may only be carried out with the consent of all users involved in the communication, the permission to install a trap and trace device on the phone of a user, or in case of an emergency being present.

The secrecy of telecommunication thus does not only encompass the content of a communication but also the fact that a communication has taken place (i.e. traffic data).

It is however doubtful if these provisions can serve a basis for a right to communicate anonymously in the sense that the State has to guarantee means of anonymous telecommunication by the law or in the sense that providers have to offer ways to communicate anonymously. At the same time there are no rules that would generally prohibit that anonymous telecommunication takes place.

2. Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country. How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are

[1] See our answers to questions 50 and 51 of the first questionnaire.

the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?

The provisions transposing Directive 2006/24/EC were enacted by the Austrian National Parliament in April/May 2011.[2] There has been a very heated controversy as to the constitutionality of data retention as a whole and the concrete proposal presented by the competent ministry. This debate led to some modifications of the text in the last moment. However only some changes reflect the data protection concern brought forward by the critics, such as e.g. the introduction of a (rather limited) four-eye-principle for access to retained data. Some other mechanisms that had been proposed in the draft rules, e.g. setting up of a "clearing-agency" have been deleted from the text of the law. We will analyse these changes in detail in answer to question 9 of this questionnaire.

After the laws had passed with the votes of the governing parties some of the opposition parties announced their intention to file constitutional complaints against these, as soon as the rules are in force (Die Grünen) or even before the entry into force (BZÖ), which is possible under Austrian constitutional law, if the complaint is supported by a third of the Members of the Parliament. However, the necessary amount of supporters was not achieved, so that there is no case pending at the moment at the Constitutional Court.

It needs to be noted, however, that the legally relevant provisions of the Austrian Telecommunications Act have not entered in force yet but will do so in April 2012 only. It is foreseeable that the constitutionality of the provisions will be tested soon after its applicability.

Despite all the controversy there is currently hardly any public discussion on the topic. This is not only true for possible modifications to the data retention model but also for the quick-freeze method, which has been put forward by some data protection experts as a possible alternative.[3] The reason for this silence might be that the opponents of data retention hope that there will be new developments on a European level before the data retention regime enters into force on 01.04.2012.

3. In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution

---

2 See Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, of 18.05.2011, published in BGBl. I Nr. 27/2011, also available at: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2011_I_27, and Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Sicherheitspolizeigesetz geändert werden, of 21.05.2011, published in BGBl. I Nr. 33/2011, also available at: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2011_I_33/BGBLA_2011_I_33.pdf.

3 See e.g. http://www.unwatched.org/20110307_Experten_raten_zu_Quick-Freeze.

of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?

Sect. 90 TKG establishes information duties for providers of a telecommunication service. According to sub. 7 such providers are obligated upon written request of the competent courts, prosecutors or criminal police (sect. 76a sub. 1 StPO) to provide information as to the master data (sect. 92 sub. 3 para. 3 TKG) of a person under suspicion of having committed a crime. This applies mutatis mutandis to the request of the security authorities in accordance with sect. 53 sub. 3 para. 1 SPG. According to sub. 6 telecommunications service providers may be requested to transfer master data to administrative authorities in cases of administrative offences committed via a public telecommunications network.

According to sect. 53 sub. 3a SPG operators of public telecommunications services and other service providers have to provide the following information to the security police, if certain facts justify the assumption of a specific hazardous situation and they need this data as an essential prerequisite in order to fulfil their duties assigned by the SPG. These are:

- the name, address and the telephone number of a particular subscriber (para. 1),
- the IP address to a particular message and the time of submission (para. 2) as well as
- the name and address of a user, the IP address was assigned to a specific date (para. 3)

In case of a present danger to the life or health of a person, the security authorities are entitled to request information on the location data and the International Mobile Subscriber Identity (IMSI) of the person in danger. The security authority shall take the responsibility for the legal admissibility of the request for information and is obligated to submit respective documentation to the providers within 24h.

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

The right to refuse to testify in court is regulated in sect. 157 StPO. Sub. 1 of sect. 157 StPO, defining the constellations in which a person may refuse to give evidence in court. These exceptions can be divided into four groups for the purposes of this questionnaire.

The first exception regulated in sect. 157 sub. 1 para. 1 StPO addresses cases in which the witness would have to expose him-/herself or a near relative to the risk of prosecution. The first exception to the duty to testify shall prevent an unconstitutional (Article 6 ECHR) forced self-incrimination.

The second exception to the duty to testify aims to protect the confidentiality of information that a person has given to a member of a certain profession underlying a professional secret (sect. 157 sub. 1 para. 2 to 4 StPO). According to this provision the following persons are entitled to refuse to give testimony about specific information. These groups are:

- defence counsels, attorneys, patent attorneys, notaries and accountants (para. 2),

- psychiatrists, psychotherapists, psychologists, probation officers, registered mediators and staff of recognized facilities for psychosocial counselling and care (para. 3)

The right to remain silent granted to attorneys, notaries and accountants serves the protection of their clients from unconstitutional self-incrimination and therefore has its basis in the constitutionally guaranteed right of the defendant to a defence.

It is important to underline that the right to refuse to testify only covers information that the mentioned persons gained in their professional capacity, which corresponds to their professional obligation of secrecy. It covers information that the client has committed to his counsel, notices of third parties, or the defence counsel and the information was gained in this capacity.

The third exception covers publishers, media workers and employees of a media company or media service on issues that concern the person of the author, sender or informant of contributions or records relating to communications, which they received as an outcome of their media-related activity (para. 4).

Finally sect. 157 sub. 1 para. 5 StPO gives voters the right to refuse to give evidence about how they have exercised their vote in an election that has legally been declared to be secret.

In order to guarantee these rights to refuse to testify sect. 157 sub. 2 StPO prohibits measures to circumvent them. Some examples for an illicit circumvention would be the confiscation of documents or of information stored on disks as well as the questioning of the assistants or persons to be trained. Furthermore, it would be illicit to question witnesses who were accidentally present at the moment the client disclosed confidential information to the counsel. Interception of telecommunications or the installation of spyware is forbidden for the same reasons.

This shows that the prohibition to circumvent the rights of a person to remain silent has a rather wide scope. It therefore can be argued, that accessing retained telecommunication data, which contains such protected information, is similarly

prohibited. Otherwise the client's ability to mount a defense could be seriously damaged.

This is however only true for the constellations mentioned in sub. 2 to 5, whereas sect. 157 sub. 2 does not prohibit the circumvention of sect. 157 sub. 1 para. 1. As a result the right to refuse to testify in cases of possible self-incrimination provided by 157 sub. 1 para. 1 StPO is not protected by a prohibition on use of retained data.

5. Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?

The newly introduced sect. 94 sub. 4 TKG provides the main terms for the transfer of retention data to the entitled bodies. Accordingly the transfer shall be effected via a "technically advanced ("technisch anspruchsvoll")" encrypted transfer of a "comma-separated value"-file (with exceptions in cases of emergency). The CSV-format describes to structure of a text file for the storage and the exchange of simply structured data. More detailed provisions relating to the syntax of the data fields and encryption, storing and forwarding of data and the detailed regulations concerning the storage of the protocols made in accordance with sect. 102c TKG may be specified by ordinance of the Federal Minister for Transport, Innovation and Technology in consultation with the Federal Ministers of Interior and Justice. The Parliament needs to receive a report on the regulation. However the competent ministry has not issued a corresponding regulation so far.

6. Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.

As the data retention legislation has not come into force so far, there is no information to this question available at the moment.

B. Country-specific questions

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

According to Austrian constitutional law the intervention in the constitutionally guaranteed rights by the legislator is only permissible if the legislator pursues a legitimate aim. The means used to achieve that aim have to be purposeful and the intervention has to be proportional.

The retention of telecommunication data constitutes an intervention in several fundamental rights, in particular the fundamental rights to privacy. The prevention and prosecution of terror and serious criminal offences are legitimate aims that may justify an intervention in the citizens´ privacy rights. However, it may well be doubted, whether the measures established by the Austrian rules transposing the

Directive are purposeful as they may be circumvented by criminals rather simply, e.g. by choosing a non-European provider, using cryptography, going to an Internet cafe, resorting to prepaid services, a public phone box etc..

Furthermore the retention of telecommunication data of the whole population without any cause or suspicion cannot be considered proportional in the current form taking into account that it constitutes a massive intervention in the privacy rights of the population. On the one hand, the massive retention of telecommunication data may enable to create a very clear and complete profile of a person's life. On the other hand, the retained data may in many cases contain sensitive data, since not only the content of a communication but also the fact that a communication has taken place can reveal sensitive information. Accordingly the retention of these data bears a considerable risk for the aggrieved party. Even though the Austrian law provides for several technical and organisational measures in order to ensure the security of retained data, these risks can only be minimized but not excluded.

Weighing the potential risks for the aggrieved party and the potential (but doubtful) advantage, the storage of comprehensive telecommunication data for a period of 6 months is to be considered in our view as a disproportional intervention of the right to privacy. It, therefore, shall at least be sought to lower the risks for the public by shortening the retention period. A possible alternative to data retention would be the "quick-freeze" method, as under this method data will only be stored when there is a concrete suspicion.

8. **Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.**

   The principle of proportionality is the main principle when assessing the constitutionality of a norm restricting fundamental rights. In many cases the legislator pursues legitimate aims by providing for suitable measures to put them into practice. The legislator, however, has to weight the legal reasoning for legislation (benefit for the public) with an assessment of its effects on fundamental rights. The proportionality test shall not only ensure that the legislator intervenes into the fundamental right in the least intrusive way, but it shall also ensure the essential content of each fundamental right.

9. **In April/May 2011, the Austrian Parliament passed legislation transposing the Directive 2006/24/EC (amending the TKG 2003, the StPO 1975 and the SPG). Please describe – on the basis of questions 7 to 35 of the first questionnaire – how the provisions adopted differ from the draft legislation described in your answers to the first questionnaire (please reply question by question).**

   (Q 7) Type of provisions transposing the Directive

   The rules transposing the Directive are simple acts of the Austrian parliament. Certain primarily technical or organisational aspects may be regulated by a regulation of the competent ministries (*Verordnungsermächtigung*, power to issue

statutory instruments).[4] A respective regulation regarding the security of retained data has been by the BMVIT.[5]

(Q 8) Terms defined in art. 2. para 2. of the Directive also defined within the national law transposing the Directive

No changes compared to the first report.

Dimension 1 (State – citizen)

(Q 9) Data to be retained

No changes compared to the first report.

(Q 10) Retention of electronic data beyond the data retained in accordance with the Directive

No changes compared to the first report.

(Q 11) Purposes of the data retention

According to the draft rules, it was still unclear which criminal offenses were to be considered as "*serious*", as the draft act (sect. 102a sub. 1 last sentence and sect. 102b sub. 1 last sentence TKG-draft) only referred to a at the time not existing catalogue of criminal offences within the StPO.

In the final text of the law, sect. 102a sub. 1 TKG last sentence and sect. 102b sub. 1 TKG last sentence refer to criminal offences, which allow for a court order according to sect. 135 sub. 2a StPO. This newly introduced provision refers to sect. 135 sub. 2 para. 2 to para. 4 StPO that regulate the conditions under which data of a telecommunication may be disclosed.

Sect. 135 sub. 2 para. 2 StPO states that data of a telecommunication may be disclosed in case of an intentional criminal act, which is punishable with a maximum prison term of more than six months, provided that the owner of the electronic device that has been or will be the origin or destination of a message, expressly consents.

According to sect. 135 sub. 2 para. 3 StPO data of a telecommunication may be disclosed, if this may induce the investigation of an intentional criminal act, which is punishable with a maximum prison term of more than one year, provided that there are certain facts that make it assumable that hereby the data of the accused can be determined.

---

4 See e.g. sect. 94 and sect. 102c TKG 2003.

5 Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO). The text is available under: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2011_II_402/BGBLA_2011_II_402.pdf. For further information please see Gerhartinger, *Österreich: Durchführungsverordnungen zur Vorratsdatenspeicherung erlassen*, ZD-Aktuell 2012, 02729.

According to the newly introduced para. 4 data of a telecommunication may be disclosed, if it is to be expected that hereby the halt of a fleeing or absent defendant, who is strongly suspected to have committed an intentional criminal offence punishable with a maximum prison term of more than one year can be determined.

(Q 12) Retention and/or transmission of sensitive data

The initial version of the second draft act contained no special rules regarding the retention and/or transmission of "sensitive data". Due to severe criticism brought forward within the consultation process by, in particular, the Austrian bar association[6] as well as journalist organisations[7] it was planned to introduce a new sub. 5 to sect. 93 TKG, according to which it was not allowed to circumvent the journalist's privilege (sect. 31 Mediengesetz)[8] as well as other statutory confidentiality obligations (protected by the right to refusal to give evidence according to sect. 157 StPO) by the transmission of data on the basis of the TKG.

In order to guarantee this, it was planned to establish a new independent agency by order of the competent ministries (BMVIT and BMI), that would have rendered the retained data anonymous before submitting it to the demanding authority, if the subscriber belonged to a protected group listed on a blacklist.[9] The transmission of retained data to the demanding authority should only be permissible in accordance with sect. 144 sub. 3 StPO. Thus, retained data of e.g. a lawyer or a journalist should only be accessed if these persons themselves are under suspicion.

The corresponding provision within the final text of the law, however, only states that editorial secrecy (§ 31 Mediengesetz) and other confidentiality and professional secrecy obligations established by federal laws as well as the prohibition of their circumvention under sect. 144 and sect. 157 sub. 2 StPO have to be respected. In addition it is stated that the provider shall not be responsible to examine the concrete facts.

Although the access to retained data is now provided by a central body, the Federal Computing Centre of Austria (Bundesrechenzentrum GmbH, BRZ),[10] that logs all access requests automatically, so that the data protection commission as well as the legal protection officer can easily access the log-data, there are no special mechanisms in place regarding the access to retained data belonging to members of the mentioned groups.

---

6 Österreichischer Rechtsanwaltskammertag, 65/SN-117/ME XXIV. GP, pp. 4 s..

7 Österreichischer Journalisten Club, 2/SN-117/ME XXIV. GP, p. 2.

8 Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz - MedienG), published in BGBl. Nr. 314/1981, lastly changed by BGBl. I Nr. 8/2009.

9 Potential members of the protected groups, however, will not be automatically inserted into this list, but rather have to register in advance.

10 http://www.brz.gv.at/Portal.Node/brz/public/en.

(Q 13) Retention period

No changes compared to the first report.

(Q 14) Authorities allowed to access retained data

No changes compared to the first report.

(Q 15) Use of the retained data

No changes.

(Q 16 and 17) Requirements

The requirements for access to retained data are defined by sect. 102b sub. 1 TKG. Two issues changed. The first change has become necessary due to the newly introduced definition of the term "serious crime". The second change brings a specification of how the court order has to be achieved. The draft version only stated that data retained may only be accessed upon court order. According to the present text of the law, access to retained data is granted on the basis of an ordinance of the prosecution that needs to be approved by the court ("gerichtlich bewilligten Anordnung der Staatsanwaltschaft").

(Q 18) Information about the access to retention data

The reference to the provisions of the StPO regarding the information rights of the aggrieved party as to a data transfer effected in accordance with sect. 102b sub. 2 TKG have remained unchanged.

Further information rights are provided by sect. 98 sub. 2 TKG that has also remained unchanged.

As there is no prior notification of the aggrieved party, Austrian law provides for the information of a third party, the so called legal protection officer (*Rechtsschutzbeauftragter*), who has to control the ordinances of the prosecution department as well as the court orders and their execution (sect. 147 StPO).[11] Therefore, the legal protection officer has to be informed about all steps within this procedure.[12] The legal protection officer will also be responsible to supervise and control orders, approvals and authorisations as well as the execution of the disclosure of data retained on the basis of sect. 135 sub. 2a StPO.

(Q 19) Information about the data accessed

There are no changes compared to the first report.

---

11 For further information see Reindl-Krauskopf, *WK-StPO*, §§ 146, 147 [1 ss.].

12 For further information see Reindl-Krauskopf, *WK-StPO*, §§ 146, 147 [6 ss.].

(Q 20) recourse

There are no changes compared to the first report.

(Q 21) Legal provisions protecting the data retained against unauthorised access in a particular way (not technical or organisational)

The security of the retained data is regulated by the proposed sect. 102c TKG. This provision largely corresponds to the draft version.

One of the major changes is the introduction of a four-eye-principle for the access to retained data.[13] This shall be ensured that not a single person acting independently can access this data. A similar four-eye principle will also apply to queries for access to retained data by security authorities.[14]

Furthermore there has been a slight change in sect. 102c sub. 2 TKG regarding the duty of logging the access to retained data. The present text specifies that the log files have to be stored unalterably. In addition the content of the access log files has been enlarged by introducing para. 2 to sect. 102c sub. 2 TKG. Accordingly the provider has to store the file reference indicated by the demanding authority in case of a demand on the basis of sect. 99 sub. 5 para. 3 and 4 TKG.

(Q 22) deletion of transmitted data

No changes.

Dimension 2 (State – economy)

(Q 23) Private bodies/enterprises obligated to retain data

No changes compared to the draft rules.

(Q 24) Exceptions from the general obligation to retain data

No changes compared to the first report.

(Q 25) Data categories that had to be retained before the Directive?

No changes.

(26) Data security (other than in Q 21)

No changes.

(Q 27) Additional costs of the implementation

There is no data available yet on this issue.

---

13 See sect. 102c sub. 1 TKG.

14 http://www.parlament.gv.at/PAKT/VHG/XXIV/UEA/UEA_00638/imfname_216117.pdf.

Within the explanatory notes to the text of the law the BMVIT estimated the costs of the providers for the implementation of the necessary technical infrastructure to 15 million Euros, calculating about 1 Euro per end user extension.[15]

(Q 28) Reimbursement for obligated parties

According to sect. 94 sub. 1 TKG providers are obliged to provide the infrastructure necessary to observe telecommunication and to access retained data under the StPO. Sect. 94 sub. 2 TKG states that providers have to contribute to the observation of communications as well as to the access to data of a communication transfer and the access to retained data. For each of these obligations an adequate reimbursement of costs is provided in the respective provisions, i.e. providers receive reimbursement of their investments effected (sect. 94 sub. 1 TKG) as well as reimbursement of the continuous costs generated by the transfer of information to the authorised bodies (sect. 94 sub. 2 TKG). The conditions and terms of these reimbursements are to be specified by regulations of the competent ministries.

The present text specifies in sect. 94 sub. 1 TKG that the providers have to be reimbursed 80% of the costs (staff costs and administrative expenses) necessary to provide the infrastructure for the observation of telecommunication including the access to retained data under the StPO. (See also answer to question 11 of the 2nd questionnaire).

(Q 29) Rules governing the cooperation

No changes.

(Q 30) Sanction or obligations in case of an infringement

The present text of the law as well as the former draft act provide primarily administrative sanctions in case of an infringement of data retention provisions. These sanctions are introduced into the general catalogue of sanctions for infringements of the TKG provided in sect. 109 sub. 3 and 4 TKG. For most offences the law provides for an administrative fine of up to 37.000,00 Euros.

This is the case if the provider

- contrary to sect. 99 sub. 5 TKG discloses information about traffic data or processes traffic data for disclosure purposes (para. 21);

- contrary to sect. 102a TKG does not retain data, unless the necessary investment costs have not been paid according to a regulation adopted on the basis of sect. 94 sub. 1 TKG have been settled (para. 22);

- contrary to sect. 102a sub. 8 TKG does not delete retained data (para. 23);

---

15 For further information see http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf, pp. 1 s..

- contrary to sect. 102b TKG discloses data without judicial authorization (para. 24);

- contrary to sect.102b TKG transmits data in unencrypted form over a communication network (para. 25);

- contrary to sect. 102c TKG does not log or does not provide the necessary information.

Providers may be punished with an administrative fine of up to 58.000,00 Euros if he does not provide the technical facilities according to sect. 94 sub. 1 TKG, unless the necessary investment costs have not been paid according to a regulation adopted on the basis of sect. 94 sub. 1 TKG have been settled.

In addition to these new provisions the general provisions of the DSG 2000 have to be taken into account. According to sect. 33 sub. 1 DSG 2000 a controller or processor who has culpably used data contrary to the provisions of the DSG 2000, shall indemnify the data subject pursuant to the general provisions of civil law. The claim for appropriate compensation for the defamation suffered shall be brought against the controller.

Dimension 3 (State – state)

(Q 31) Public body responsible for establishing the contact with the party retaining

The present text of the law does not provide for one single public body responsible for establishing the contact with the providers retaining data, but rather leaves it up to all the public bodies entitled to access retained data, such as police, prosecutions agency and courts, to send a request to the provider.

(Q 32) Regional entities granted their own rights to of access

No changes.

(Q 33) Rules governing the co-operation among the different bodies

No changes.

(Q 34) Legal basis for the exchange of retained data with other member states

No changes.

(Q 35) Bodies in charge of monitoring compliance with national rules

No changes.

10. Is the constitutionally fixed limitation to a conferral of national sovereignties to the EU in any way binding for representatives of your country in EU organs and institutions (e.g. the Council of Ministers, the European Council) when

exercising their functions in the adoption and execution of an EU legislative act?

In order to compensate the transfer of legislative competences to the European level, which constituted a fundamental change of the democratic and the federal principles of the Austrian Constitution, the Austrian constitutional legislators introduced several provisions that should preserve the rights of the Austrian parliament (parliament of the federal and provincial assemblies).

The representation of Austria at the European institutions is regulated by the art. 23a to 23k of the Austrian Constitution (Bundes-Verfassungsgesetz, B-VG). According to art. 23e B-VG the competent member of the federal government shall without delay inform the National Council and the federal council about all projects within the European Union and afford them the opportunity to express their opinion.

If the competent member of the federal government is in possession of an opinion by the national council about a project which shall be passed into federal law or which bears upon the issue of a directly applicable juridical act concerning the matters which would need to be settled by federal legislation, the member is bound this opinion during EU negotiations and voting. Deviation is only allowed for imperative foreign and integrative policy reasons.

If the competent member of the federal government wishes to deviate from the national council's opinion, the National Council shall again be approached. As far as the juridical act under preparation by the EU would signify an amendment to existing federal constitutional law, a deviation is at all events only admissible if the National Council does not controvert it within an appropriate time (art. 23e sub. 3 B-VG). Art 23 sub. 4 B-VG contains a respective provision for binding legislative acts on affecting the competences of the federal council.

11. **Please describe the applicable rules on reimbursement of costs in detail. In which form and to which extent (completely, certain percentage of the full costs, lump sum, mere depreciation of book-entry items on tax return) are the costs reimbursed? How and by whom (government authority, provider) are the amounts to be reimbursed calculated? How are the specific data retention costs delimited against the costs for the general storage equipment and the general data storage process used in the context of service provision, billing and related business activities?**

According to sect. 94 sub. 1 TKG providers are obliged to provide all facilities necessary to monitor communication and to provide information about communications including retained data. The required facilities are to be specified by regulations of the competent ministries issued on the basis of sect. 94 sub. 3 and 4 TKG. According to sect. 94 sub. 1 TKG providers will be reimbursed 80% of their costs (personnel and operating expenses) for providing these facilities.

The Federal Minister for Transport, Innovation and Technology (BMVIT) in agreement with the Federal Minister of the Interior, the Federal Minister of Justice and the Federal Minister for Finance, has to define the basis for calculating this

percentage, as well as the procedures for asserting this claim for compensation. This has to be mainly based on the economic reasonableness of the expenses, on a possible interest of the concerned contractor on the services to be provided, on any of the necessary technical capabilities as well as the simplicity and affordability of the necessary procedure.

This cost sharing rule corresponds to the decision GZ 37/02 of the Austrian Constitutional Court of 27.02.2003 (VfSlg 16 808), in which the passing on of all costs for the provision of surveillance devices and the exclusion of any reimbursement of costs to the telecommunications operators had been declared as being unconstitutional.

12. **Have the technical and organisational measures necessary to implement the legal requirements regarding data security (as set out in your answers to question 21 and 26 of the first questionnaire) been standardised or specified by regulations (e.g. issued by the BMVIT) or administrative guidelines (e.g. issued by the competent supervisory authority or)? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.**

    In particular: do they provide for measures in one or more of the following areas:
    - **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**
    - **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**
    - **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**
    - **access logging**
    - **secure (irreversible) deletion after expiry**
    - **error correction mechanisms (e.g. hash functions, checksums)**
    - **secure data transmission (cryptographic security, postal delivery)**
    - **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**
    - **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**
    - **staff training/internal control mechanisms to ensure compliance with the law and other rules**
    - **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or to any data processing (in electronic communications)?

Some technical and security standards for the transfer of traffic data, location data, master data and retained data according to the provisions the StPO and the SPG are laid down in sect. 94 sub. 4 TKG. Accordingly the transfer of these data has to be effected using a transfer technology, which guarantees for the identification and authentication of sender and recipient and ensures the integrity of the data transferred. Furthermore retained data shall be submitted in an encrypted "Comma Separated Value (CSV)" file.[16]

The security standards (data security, logging, statistics) for retained data are regulated by sect. 102c TKG. Retained data (data exclusively stored on the basis of sect. 102a sub. 2 to 4 TKG-draft) shall be labelled and underlie stricter access and security standards. Therefore it is important that retained data is distinguishable from the data stored in accordance with the sect. 96, 97, 99, 101 and 102 TKG (sect. 102c sentence 1 TKG).

This provision has been significantly modified since the first draft, taking into account the decision of the German Federal Constitutional Court Federal Constitutional Court, 1 BVR 256/08 dated 02.03.2010 regarding the implementation of the Data Retention Directive in Germany. Accordingly requests regarding retained data at the providers shall be possible only for specially authorized employees in compliance with the four-eye principle. Thus, every access to retained data at the provider requires the authorisation by two employees especially authorized to do so. However it is not necessary that the authorization is made simultaneously by both persons, so that the authorization by the second person can also be done later, obviously meaning after the data had been accessed, what significantly weakens the effect of the four-eye principle. In the explanatory notes to sect. 102c sub. 1 TKG the Austrian legislator underlines however that an internal system to ensure effective control of the responsibility has to be established. The Austrian legislator did however not regulate in detail by which technical and organisational measures these requirements are to be achieved by the providers. It rather takes a technology-neutral approach by stating that the providers have to foresee adequate technical and organisational measures in order to fulfil these requirements. It is however stated that these requirements can be regulated in a more detailed way by the competent BMVIT. The BMVIT issued respective regulations in December 2011.[17]

---

16 Sect. 94 sub. 4 TKG, however, provides an exception for the transmission of data in the cases of sect. 98 and sect. 99 sub. 5 para. 3 and 4 TKG as well as for the transmission of location data according to sect. 134 ss. StPO.

17 Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO). The text is available under: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2011_II_402/BGBLA_2011_II_402.pdf. For further information please see Gerhartinger, *Österreich: Durchführungsverordnungen zur Vorratsdatenspeicherung erlassen*, ZD-Aktuell 2012, 02729.

According to sect. 102c sub. 2 TKG providers have to keep protocols about every access to data as well as every request and every transfer of retained data. These protocols have to contain specific data about the authority requesting access to these data and the specific purpose of the request, the file number in case retained data are accessed by a security agency, the date of the request as well as the date and time of transfer, the retained data accessed, the person to whom the data pertains and the unique ID of the person accessing the data within the sphere of the provider.

These protocol data have to be transferred to the data protection commission as well as to the BMJ upon request. Furthermore these data have to be transferred to the BMJ annually on the 31st of January. The protocol data have to be stored for three years form the end of the retention period of a specific data.

The compliance to these rules is controlled by the data protection commission (sect. 30 DSG 2000).

13. **Which EU legislative acts and international (multilateral) treaties on cross-border co-operation in data retention issues (including both rules specifically designed for data retention as well as general rules applicable to data retention) apply to your country? Have bilateral agreements been concluded on data exchange with the U.S. (as far as they are relevant to data retained under Law 32/2008)? May the entitled bodies of the foreign country request the data from the providers directly, or is there an Austrian authority handling such requests?**

The international cooperation in matters concerning the activity of the security police and the criminal police are governed by the Polizeikooperationsgesetz (PolKoG), which mainly transposes the legal acts passed by the council in the respective fields. One of these acts is the Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

In order to facilitate their cooperation Austria and the USA have concluded an agreement on enhancing cooperation in preventing and combating serious crime in November 2010.[18] This agreement mainly provides for possibilities on automated querying of dactyloscopic data and DNA profiles. Should the automatically queried data show a match further personal data and other data relating to the reference data shall be supplied. This shall be governed by the national law, including the legal assistance rules, of the requested party. The agreement still has to be ratified by the Austrian parliament.[19]

The laws transposing the Directive give no clear answer whether or not foreign authorities are entitled to request data retained directly from the providers.

---

18 http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01388/imfname_229301.pdf.

19 The legislative process can be followed under: http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01388/index.shtml#tab-Uebersicht

According to the wording of the present text of the law access to retained data is granted only on the basis of an ordinance of the prosecution approved by the court for the purpose of investigating and prosecute criminal offences, which justifies a court order according to sect. 135 sub. 2a StPO ("gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere ein Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässt").

14. Are there any *external* bodies responsible for supervising that the bodies entitled to obtain access to the data retained (police etc) act within the law? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

According to sect. 147 StPO all ordinances of the prosecution department and the court orders granting access to retained data on the basis of the StPO as well as their execution are to be controlled by the so-called legal protection officer (*Rechtsschutzbeauftragter*). In order to enable the legal protection officer to fulfil this task he has to be informed about all steps within this procedure. This duty to inform shall serve as an adjustment for the fact that the aggrieved has no information rights prior to the demanding bodies' access to retained data.[20]

Furthermore, the legal protection officer has the right to examine all the findings upon completion of the investigative measure before these are introduced to the file (sect. 147 sub. 4 StPO). The legal protection officer is also entitled to request the cancellation of findings or parts of them (sect. 139 sub. 4 StPO) in case these requirements are not met and to control the proper destruction of these results.[21]

According to sect. 47a StPO the legal protection officer and his substitutes are appointed by the BMJ upon a joint proposal of the President of the Constitutional Court, the Chairman of the Ombudsman and the President of the Austrian Bar Association for a period of three years. The proposal must contain at least twice as many names as persons appointed. Sub. 4 of that provision states that the law enforcement officer is independent in the exercise of his office and to any directions bound.

This legal framework is intended to provide for a "completely independent" work of the legal protection officer in the sense of art. 28 sect. 1 sub. 2 of the Directive 95/46/EC.

---

20 For further information see Reindl-Krauskopf, *WK-StPO* §§ 146, 147 [12 ss.].

21 See Reindl-Krauskopf, *WK-StPO* §§ 146, 147 [15 ss.].