14 'Electronic communications network' means '[…] transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed' .

15 Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108, 24 April 2002, pp. 33-50

16 Article 29 Working Party, Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, 26 September 2006, p. 3, available at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf.

17 Law 2006-64 of 23.01.2006 on the fight against terrorism, including provisions regarding security and border controls [Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrőles frontaliers], available at http://foruminternet.org/documents/lois/lire.phtml?id=998

18 http://www.edri.org/edrigram/number3.16/Italy

19 Article 29 Working Party, Opinion on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 21 October 2005, p. 9, available at http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf.

20 Proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, 21 September 2005, available at http://www.europa.eu.int/information_society/policy/ecomm/doc/info_centre/communic_reports/data_retention/retention_proposal_en_com_2005_0438.pdf.

21 A Committee composed of representatives of Member States and chaired by the representative of the Commission would assist the Commission in the revision of the Annex on a regular basis.

22 Art 132 Italian personal data protection code [Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali], available at http://www.garanteprivacy.it/garante/doc.jsp?ID=1105372

23 Section 63 of the Irish Criminal Justice (Terrorist Offences) Act 2005, available at http://oireachtas.ie/documents/bills28/acts/2005/a0205.pdf

24 http://www.edri.org/edrigram/number3.24/Poland.

25 The declarations of the 16 countries can be found at the end of the Directive.

26 Opinion of the Dutch Data Protection Authority [College bescherming persoongegevens (CBP)], Legislative proposal (Bill) for the implementation of the European Directive on Data Retention, Pertaining to the tender letter of 22 January 2007, 24 January 2007, p. 2

27 Article 29 Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 25 March 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf.

28 French decree no. 2006-358 regarding the retention of electronic communications data [Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques], available at http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSD0630025D

29 http://www.statewatch.org/news/2006/apr/eu-us-jha-7618-06.pdf

30 http://www.bitkom.org/files/documents/Stellungnahme_BDI_BITKOM_VATM_Vorratsdatenspeicherung_DE_05_08_05.pdf

31 See also the case in France where the French Association of Internet Access and Service Providers (AFA) announced that it would challenge the decree no. 2006-358 regarding the retention of electronic communications data before the 'Conseil d'Etat' http://www.afa-france.com/p_20060328.html

32 Council of the European Union, Statements, Council doc. 5777/06 ADD 1 (10 February 2006) available at http://register.consilium.eu.int/pdf/en/06/st05/st05777-ad01.en06.pdf

33 Commission Staff Working Document 'Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC EXTENDED IMPACT ASSESSMENT', 21 September 2005, available at http://www.statewatch.org/news/2005/oct/com-dataret-reg-ass-05.pdf, pp. 13-14

34 A Dutch Internet Service Provider, xs4all, counted that its traffic between 5 September 2005 and 14 June 2006 is 150.677.000.000.000 data packets, which are approx. 131.996.000 CD's. You can find the counter at http://www.xs4all.nl/bewaarplicht/

35 Judgement of the Court of Justice in Joint Cases C-317/04 and C-318/04

36 Directive 1995/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 0031 – 0050 (23 November 1995).

37 Other references:
[1] Walker, Clive – Akdeniz, Yaman: Anti-Terrorism Laws and Data Retention: War is over? In: Northern Ireland Legal Querterly, 2003/2, pp. 159-182
[2] Munir, Abu Bakar: Retention of communications data: Security vs Privacy. Paper presented at Oxford Internet Institute Conference: Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities, 8 September 2005, http://www.oii.ox.ac.uk/research/cybersafetyextensions/pdfs/papers/abubakar_munir.pdf [17.11.2005.]
[3] Kosta, Eleni – Valcke, Peggy: Retaining the Data Retention Directive. In: Computer Law & Security Report, 2006/5, pp. 370-380
[4] Munir, Abu Bakar – Yasin, Siti Hajar Mohd: Access to Communications data by public authorities. In: Computer Law and Security Report, 2004/3, pp. 194-199
[5] Memorandum of laws concerning he legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights, October 2003. Prepared by Covington & Burling LLP, http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf. [12.12.2006.]

NATALIE FERCHER

National Implementation of the Data Retention Directive in Austria

1. Introduction

The Data Retention Directive[1] imposes obligations on providers to retain traffic and location data. The data in question relate to the use of mobile and fixed telephony as well as to the Internet communication of all users. The main aim is to ensure that data are available for the purposes of investigating, detecting and prosecuting serious crimes, as defined by national law.

This is obviously a paradigm shift. In 2002 there came into force the Directive on Privacy and Electronic Communication[2], whose aim was to ensure user privacy regarding specific risks arising from new technologies. As a general principle, the quantity of personal data necessary should be limited to a strict minimum, and so the existing legal framework explicitly protects citizens' privacy and personal data and provides for the deletion of traffic data once no longer needed for the purposes of conveying communication or billing.

The author works as research assistant at the Department of Information Technology Law and Intellectual Property Law, Vienna University of Economics and Business Administration

This paper will, firstly, give an overview of the current legal status in Austrian law to identify the problems which may arise whilst implementing the Data Retention Directive. Following a short overview of the Data Retention Directive, its implementation will then be discussed in detail.

2. The current legal status

Whilst implementing the Directive, the constitutional rights laid down in the Austrian legal system must always be kept in mind.[3] The most important of these are:

The fundamental right of respect for private and family life, as laid down in Article 8 of the European Convention on Human Rights (ECHR), which is constitutional law in Austria. In relation to privacy, also as established by Article 8 of the ECHR, it is particularly the factors of necessity and proportionality which are affected by the Data Retention Directive. This problem will be discussed later.

In the same context a further important human right is the fundamental right to data protection, which is regulated in the Federal Act concerning the protection of personal data – also constitutional law. §1 states: *"Everyone shall have the right to secrecy in respect of the personal data which concern him, and especially with regard to his private and family life, insofar as he has an interest which merits such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject."*[4]

The data subject in this context is any natural or legal person or group of natural persons whose data is processed, and so personal data includes all the information relating to data subjects who are identified or identifiable. Normally traffic data and location data identify one data subject, and so this rule applies.

The only prerequisite for this protection is that the data subject should have an interest meriting such protection - which is not the case when the data is generally available – such as the name and telephone number published in the public telephone book or when the data cannot be traced back to the data subject.

Everyone also has the right to obtain information as to who processes what data concerning him, the origin of these data, the purposes for which they are used, as well as to whom the data are transmitted. He also has the right to correct inaccurate data and the right to erase illegally processed data.

Restrictions to this fundamental right to data protection are allowed insofar as personal data is used in the vital interest of the data subject or with his consent. Restrictions are also permitted to safeguard the overriding legitimate interests of another person.

In the case of intervention by a public authority, the restriction shall only be permitted based on laws or statutes necessary for the reason stated in Article 8 of the ECHR. Even where restrictions are permitted, any conflict with fundamental rights is to be resolved by use of the least intrusive of all effective methods.

In this context the last fundamental right to be mentioned is "confidentiality of communications", as laid down in the Telecommunications Act.[5] Content data, traffic data and location data are subject to this, and every operator, together with all others involved in the operator's activities, are obliged to observe the confidentiality of the communication. Persons other than the user himself are not permitted to listen, tap, record, intercept or otherwise monitor communications and the related traffic and location data, nor to pass on related information without the consent of all users concerned.

The basic rules for collecting and processing data are also laid down in the Telecommunications Act.[6] This simply states that master data, traffic data, location data and content data may be collected and processed only for the purposes of providing a communications service. These data may only be used for marketing communications services or for providing value-added services or other transmissions with the consent of the data subjects, consent which may be withdrawn at any time. This is the general rule applying to all data.

Definitions of the relevant terms in Austrian law are laid down in the Telecommunications Act[7] where *"traffic data"* means any data processed for the purpose of the conveyance of a communication on a communications network or for the billing thereof. In fact, it is the same definition as is found in the Directive on Privacy and Electronic Communication. "*Traffic data*", therefore, includes active and passive user-numbers such as a telephone number, an email address or an IP address. *"Location data"* means any data processes in a communication network indicating the geographical position of the tele-communications terminal equipment of a user of a publicly available communication service.

The last term to be mentioned is *"master data"*. This term covers all those personal data required for establishing, processing, modifying or terminating the legal relations between the user and the provider. This includes, for example, surname and forename, residential address, subscriber number, information concerning the type and content of the contractual relationship and financial standing.

The Telecommunications Act also includes special rules regarding traffic data (§ 99). Except for those cases regulated by law, traffic data must not be stored and is to be erased or made anonymous after the termination of the connection. If required for the purpose of subscriber billing, the operator is allowed to store traffic data up to the end of the period during which the bill may be lawfully challenged or payment pursued.

In general, location data other than traffic data may be processed only if they are made anonymous or if users have given their consent, consent which may be withdrawn at any time.

The operator is, therefore, only allowed to process data if a legal obligation in national law exists, and in practice, the most relevant such obligation is found in the Code of Criminal Procedure. Operators are obliged to provide information regarding master data, traffic data and content data, but only under specific preconditions. This obligation exists only as long as the data actually exist. There exists neither an obligation nor any legal opportunity to retain data in advance or to intercept it.

According to these rules, the operator is obliged to provide information where there is good reason to suspect that someone is, deliberately, about to commit a crime which is subject to a prison sentence of more than six months.

To recapitulate, we can see that the current position in Austria is that the retention of traffic data and content data without a material reason (e.g., a court order) or the consent of the relevant person is, in general, prohibited. This situation is diametrically opposed to that required in the Data Retention Directive.

3. A short overview of the Data Retention Directive[8]

The Directive aims to harmonise the provisions of member-states concerning obligations on providers to retain certain data generated or processed by them. Only providers of publicly available electronic communications or telecommunications networks are addressed by the directive. The aim is to ensure that data is available for investigating, detecting and prosecuting serious crime, as defined by each member-state in its national law.

In the writer's personal view, the list of data to be retained is, in reality, very extensive. It contains telephony and internet traffic data as well as location data which will identify the user's fixed and mobile communication equipment.

Member-states may choose a retention period of between 6 months (the minimum) and 2 years (the maximum), and it is also left to member-states to decide what procedure is to be followed and what conditions must be fulfilled to obtain access to retained data, although it is emphasised that such laws or actions must fully respect fundamental rights.

The obligation to retain data will result in a substantial number of new databases. There is a considerable risk that those databases could be misused by different interest groups - for example, for commercial use or data-mining in general – and so the Data Retention Directive does introduce certain rules on data security together with minimum data security principles. Most of these are, in fact, already covered by the existing legal framework.

The Directive also imposes numerous duties and costs on providers. There will be costs involved in respect of additional infrastructure and human resources, costs associated with adapting and amplifying the existing system, costs involved in storing and processing data and in dealing with enquiries. These costs will, in particular, depend on the scope of the national data security requirements, the retention period and the amount of data to be retained.

The Directive should be incorporated into national law no later than the 15th of September, 2007, although Austria, together with many other member-states, has stated that it will postpone implementiing this Directive on the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months – that is, until the 15th of March, 2009.

4. Problems concerning national implementation

In respect of implementing the Directive, special attention needs to be given to potential problems connected with fundamental rights.

Regarding the right to privacy, as established by Article 8 of the ECHR, it is those factors of necessity and proportionality which are principally in question. Interference by a public authority is allowed only if it is in accordance with the law and if it is necessary in a democratic society in the interests of national security, public safety etc. The Commission argues that the Directive is in line with the ECHR, in that the limitations of the rights guaranteed under Article 8 of the Convention are considered to be proportionate and necessary to meet the legitimate objectives of preventing and combating serious crime. In this view the Directive would have a clear and limited purpose: retention would only apply to listed categories of data, and with a limited period of retention. However, the question of whether this is really the case does need to be asked, since this argument does not sound very convincing.[9]

It appears quite easy for "criminals" largely to circumvent the retention of data - for example, by opting for a non-European provider or by using an Internet café or public 'phone-box. Does this still mean that provisions are necessary?

This is not exclusively an Austrian problem. Since the ECHR applies in all member-states, this has also been discussed at European level. The Convention is a part of the constitutional law of Austria, and so an appropriate solution must be found.

Further difficulties arise in implementing the Directive in respect of the fundamental right to data protection. Where a public authority intervenes, a restriction can only be permitted based on laws necessary for the reasons stated in Article 8 of the ECHR. This also applies to the necessity and proportionality of the provisions laid down in the Directive, as discussed earlier.

Even where restrictions are permitted regarding Article 8 of the Convention, any intervention into fundamental rights should only use the least intrusive of all effective methods. According to one opinion,[10] data retention as required by the Directive is not the least intrusive of all effective methods: options which already exist are, in this opinion, sufficient to achieve the goals of the Directive. In the light of this conflict, it appears that the most important provisions of the Directive should be implemented by constitutional law. Constitutional law is accorded higher status due to the fact that is harder to amend. An amendment to a national constitutional provision requires a two-thirds majority in Parliament, with at least half of the members both present and voting.

A further problem relates to the costs of the equipment necessary for data retention as well as to ongoing expenses. The Austrian Constitutional Court [Verfassungsgerichtshof], which has supreme jurisdiction over constitutional cases, decided a few years ago that constitutional law is contravened if there is no cost reimbursement for the providers.[11] It is very likely that the same rule will apply to the reimbursement of providers' costs which emerge from the provisions of the Data Retention Directive.

A further important issue to be discussed is the meaning of the term "serious crime" (as used in the Directive) should mean in Austrian law. Normally, serious crime would mean a crime which is subject to a life sentence or to a prison sentence exceeding three years.[12] However, some opinions hold that this is insufficient and state that the legislator should detail such crimes in an exhaustive list. This particular problem will be discussed later.

5. First draft of the Amendment to the Telecommunications Act

In May 2007 the Minister of Transport, Innovation and Technology published a first draft of the amendment to the Telecommunications Act.[13] The definition of the data to be retained is the same as laid out in the Data Retention Directive, and, although Austria is not yet obliged to implement the provisions of the Directive regarding "Internet data", the ministry has already included all the definitions concerning Internet data in this draft. In addition , data are to be retained for a period of six months dating from the termination of the communication.

According to Article 1 of the Directive data has to be available for investigating, detecting and prosecuting serious crime, and each member-state is obliged to define what the term "serious crime" should mean. The Ministry of Transport, Innovation and Technology has suggested in its draft that this should cover actions which are subject to a prison sentence of m ore than one year[14] No regulations applying to expenses are scheduled, although the accompanying letter[15] states that "the expected costs cannot yet be estimated".

> Prior to thel 21st of May everyone had the opportunity to comment on this draft. Many institutions of different kinds did so and almost al criticised the draft. Most of the institutions stated that the definition of serious crime should be more rigorous, although opinions differ as to the way this should be done. The "Bundeskanzleramt – Verfassungsdienst"[16], for example, pointed out that, according to the constitutional law (§ 1 of the Data Protection Act as well as Article 8 of the EHCR), the definition should only include crimes related to organised crime and terrorism (§§ 278 to 278d of the Criminal Code). In their opinion, it should also be possible to include crimes subject to a life sentence or to a prison sentence longer than three years.[17]

A further main concern is that there are no regulations regarding expected costs which should unquestionably be included in the Telecommunications Act. "Telekom Austria"[18] estimated their additional costs at about €4.5m.[19], and they also pointed out that it would be necessary to incorporate data retention into constitutional law.
Even the Finance Minister has voiced his concern that the costs which may emerge cannot yet be estimated, and that he cannot, therefore, consent to the Amendment until the problem is resolved.[20]
The Ministry of Home Affairs is the only institution which would prefer a retention period of a minimum of 1 year. They contend that, since the crimes involved are often linked to foreign countries, a 6 month period could be too short.[21]
As mentioned earlier, data regarding Internet access, Internet telephony and Internet email is already included in the draft. The accompanying letter states that this serves only for clarification purposes and to avoid legal uncertainties. However, the opposite is the case, since the regulation of the obligation to retain data does not explicitly exclude "Internet data", and so no-one knows how to cope with these regulations should they come into force. The Provincial Parliament of Vienna, and many others, indicated that it would be more rational to exclude all mention of "Internet data" from this draft and to regulate this later.[22]
Yet another serious concern of the Austrian Data Protection Commission is that there is no particular penalty to be applied when this law is broken. The draft merely states that, when someone does not retain the necessary data, in spite of his obligation to do so, he should pay a fine of up to €37.000. According to the Data Protection Commission, it is unclear how this could possibly be controlled, although the most important point is that a penalty regarding illegal access to retained data is missing and should also be included.[23]
By way of summary, statements relating to the Telecommunications Act Draft criticise this first attempt. In particular, the definition of "serious crime" caused great dispute among Austrian scholars due to its current incompatibility with constitutional law.
A further major problem is that the constitutional problems in connection with Article 8 of the EHCR and § 1 of the Data Protection Act have not been addressed or discussed in any way.
The Minister of Transport, Innovation and Technology announced that he will revise this draft once more and will take a closer look at the regulations of other Member-states. It is, therefore, highly likely that this draft will be changed in some way or ways.

6. Summary

Generally speaking, the objective of harmonisation has not been achieved. Too many elements are left to the individual decisions of member-states, which will inevitably lead to diverging national rules and interfere with the functioning of the internal market.
Nevertheless, at this point member-states are obliged to implement the Data Retention Directive. In Austria – and, no doubt, in many other member-states also – there exists the overriding problem that, first of all, an amendment to the constitutional law will probably be necessary.
A first Draft of the Telecommunications Act has been published by the Minister of Transport, Innovation and Technology, a draft which has been criticised from almost every side, especially regarding the definition of "serious crime". Most of these statements relating to the Draft of the Telecommunications Act demand some limitation to the definition of the term "serious crime", so that the obligation to retain data is closely connected to crimes involving terrorism and organised crime.
Moreover, this draft does not take into account various constitutional problems which have to be resolved, in the absence of which the new law would be in serious danger of being rejected by the Constitutional Court [Verfassungsgerichtshof].
Since the minister responsible announced a review of the Amendment, a clear and final statement concerning the implementation of the Data Retention Directive is not yet possible.

Notes

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerns the processing of personal data and the protection of privacy in the electronic communication sector.
3 Otto, Gerald – Seitlinger, Michael: Die „Spitzelrichtlinie". Zur (Umsetzungs)Problematik der Data Retention Richtlinie 2006/24/EG. In: Medien und Recht 2006/4, pp. 227–234
4 See § 1 Federal Act concerning the Protection of Personal Data.
5 See § 93 Telecommunications Act. This act can be found under http://www.ris.bka.gv.at/englische-rv/ [05.06.2007.] as well as the Data Protection Act
6 See §§ 96-102 Telecommunications Act.
7 See § 92 Austrian Telecommunications Act..
8 For further details see also In: Liebwald, Doris: The New Data Retention Directive. In: Medien und Recht 2006/1, p. 49
9 Ibid.
10 Otto, Gerald – Seitlinger, Michael op. Cit. p. 227.
11 VfGH 27.2.2003, G37/02ua, V42/02ua.
12 See § 17 Abs 1 Criminal Code.
13 See this draft (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061/imfname_076383.pdf [04.06.2007.]
14 See § 102a Draft Telecommunications Act in conjunction with § 17 Security Police Act [Sicherheitspolizeigesetz]; §§ 107 and 107a Criminal Code are also explicitly included.
15 See http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061/imfname_076384.pdf [05.06.2007.]
16 The „Bundeskanzleramt – Verfassungsdienst" is a section of the Federal Chancellery. The main task is to examine the drafts of new federal statutory provisions.
17 See this statement (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061_10/fname_078873.pdf [04.06.2007.]
18 The "Telekom Austria" is Austria's largest telecommunications operator.
19 See their statement (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061_36/imfname_079854.pdf [04.06.2007.]
20 See the statement of the Ministry of Finance (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061_24/imfname_078967.pdf [05.06.2007.]
21 See the statement of the Ministry of Inner Affairs (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061_25/fname_078966.pdf [04.06.2007.]
22 See for his statement (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061_03/fname_078854.pdf [05.06.2007.]
23 See the statement of the Data Protection Commission (in German only) http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXIII/ME/ME_00061_31/imfname_079536.pdf [05.06.2007.]