

REC'D SEP 30 2013

**Registrar Data Retention Waiver Request (2013 RAA)**

Complete this form to request a waiver of one or more of the data retention requirements specified in the 2013 Registrar Accreditation Agreement (RAA). ICANN's consideration of this request is made pursuant to sections 2, 3, and 4 of the Data Retention Specification to the RAA; a waiver is not automatically granted by submitting this form.

<b>Registrar name:</b>	<b>LEDL.NET GMBH</b>
<b>GURID (IANA ID):</b>	<b>809</b>
<b>Legal jurisdiction of registrar:</b>	<b>Austria / EU</b>
<b>Jurisdiction in which legal conflict has arisen:</b>	<b>EU</b>
<b>Contact person for this request:</b>	<b>Friedrich Ledl</b>
<b>Email address for contact person:</b>	<b>f.ledl@domainttechnik.at</b>
<b>Telephone number for contact person:</b>	<b>+43 6215 20888</b>

Registrar has determined in good faith that the collection and/or retention of the data element(s) specified in the Data Retention Specification to the 2013 RAA, noted below, violates applicable law based upon (check all that apply):

- ☐ a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that the collection and/or retention of any data element specified herein by Registrar is reasonably likely to violate applicable law (the "Opinion"); and/or
- ☒ a ruling of, or written guidance from, a governmental body of competent jurisdiction providing that compliance with the data collection and/or retention requirements of this Specification violates applicable law; and/or
- ☐ a data retention waiver determination previously granted by ICANN.

A copy of the Opinion and governmental ruling or guidance, as applicable, must accompany this waiver request. Please also include any documentation received by your registrar from any governmental authority related to such determination and complete the fields below.

**Cite and provide a copy of the relevant applicable law:**

**Article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights:**

**Right to respect for private and family life**

1. Everyone has the right to respect for his private and family
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

**Article 17 of the International Covenant on Civil and Political rights:**

- 1, No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Briefly describe the relevant applicable law in English (if the text of the law is not in English):

**Specify the allegedly offending data collection and retention elements:**

If this waiver request is not substantially based on a data retention waiver determination previously granted by ICANN (i.e., same law, same jurisdiction, same data retention requirement(s)), please explain the manner in which the collection and/or retention of such data is believed to violate applicable law, and provide a description of such determination and any other facts and circumstances related thereto:

[http://www.internetnews.me/wp-content/uploads/2013/07/20130606\\_Letter\\_to\\_ICANN.pdf](http://www.internetnews.me/wp-content/uploads/2013/07/20130606_Letter_to_ICANN.pdf)

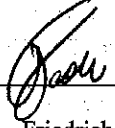
The proposed new data retention requirement does not stem from any legal requirement in Europe. It entails the extended processing of personal data such as credit card and communication data by a very large number of registrars. The fact that these data may be useful for law enforcement (including copyright enforcement by private parties) does not equal a necessity to retain these data after termination of the contract. Taking into account the diversity of these registrars in terms of size and technical and organisational security measures, and the chance of data breaches causing adverse effects to individuals holding a domain name, the ARTICLE 29 Data Protection Working Party finds the benefits of this proposal disproportionate to the risk for individuals and their rights to the protection of their personal data.

Secondly, the Working Party reiterates its strong objection to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights.

The fact that these personal data can be useful for law enforcement does not legitimize the retention of these personal data after termination of the contract. Because there is no legal ground for the data processing, the proposed data retention requirement violates data protection law in Europe.

Please note that prior to granting any data retention waiver, ICANN will post its preliminary determination on its website for a period of at least 30 calendar days.

Submitted by:

Signature:  Date: 30.Sept.2013

Print Name: Friedrich Werner Ledl Title: CEO

This form and accompanying materials may submitted by courier or fax to:

Attention: Registrar Accreditation Notices  
Internet Corporation for Assigned Names and Numbers  
12025 Waterfront Drive, Suite 300  
Los Angeles, California 90094-2536 USA  
Facsimile: +1 310 823-8649

If you wish to submit an electronic copy, please email attachments as PDF or DOC/x files to [RAAquestions@icann.org](mailto:RAAquestions@icann.org).

Encl: 06/06/2013 17:19:1630 - 06/06/2013

**ARTICLE 29 Data Protection Working Party**

Brussels, 06 June 2013

Dr. Steve Crocker and Mr. Fadi Chehadé  
Chairman and CEO of the Board of Directors  
Internet Corporation for Assigned  
Names and Numbers (ICANN)  
4676 Admiralty Way, Suite 330  
Marina del Rey, CA 90292-6601

By email to the Director of Board Support:  
diane.schroeder@icann.org

**Subject: Statement on the data protection impact of the revision of the ICANN RAA**

Dear Mr Crocker and Mr Chehadé,

In the context of ICANN's revision of the Registrar Accreditation Agreement (RAA) and the final **RAA Proposal**<sup>1</sup>, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 WP)<sup>2</sup> wishes to provide a harmonised statement concerning compliance with European data protection law.

Following up on our letter of 27 September 2012<sup>3</sup> and previous contributions to the process of collecting and disclosing WHOIS data<sup>4</sup>, this statement specifically addresses the legitimacy of the data retention obligation for registrars, contained in the new RAA.

The Working Party notes that ICANN has included a procedure for registrars to request a waiver from these requirements if necessary to avoid a violation of applicable data protection law. Such a waiver request can be based on written guidance from a governmental body of

<sup>1</sup> ICANN Proposed Final 2013 RAA of 22 April 2013, URL: <http://www.icann.org/en/news/public-comment/proposed-raa-22apr13-en.htm>

<sup>2</sup> The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The Article 29 Working Party is competent to examine any question covering the application of the data protection directives in order to contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents.

<sup>3</sup> Article 29 Working Party letter to ICANN, 26 September 2012, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926\\_letter\\_to\\_icann\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120926_letter_to_icann_en.pdf)

<sup>4</sup> URLs: [http://ec.europa.eu/justice\\_home/fd/privacy/docs/wpdocs/2012/06/20120606\\_letter\\_to\\_icann\\_en.pdf](http://ec.europa.eu/justice_home/fd/privacy/docs/wpdocs/2012/06/20120606_letter_to_icann_en.pdf) and <http://www.icann.org/correspondence/schaar-to-cert-22jun06.pdf> and <http://gnso.icann.org/correspondence/schaar-to-cert-12mar07.pdf>

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: [http://ec.europa.eu/justice/policies/privacy/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/index_en.htm)



competent jurisdiction providing that compliance with the data retention requirements violates applicable law.

In order to avoid unnecessary duplication of work by 27 national data protection authorities in Europe, with this letter, the Working Party wishes to provide a single statement for all relevant registrars targeting individual domain name holders in Europe.

The final proposed Data Retention specification roughly distinguishes between name and contact details for the domain name holder (specified in 1.1.1 to 1.1.7) and all other types of data a registrar might collect (specified in 1.2.1 to 1.2.3), such as logfiles and billing records containing the 'means and source of payment', logfiles about the communication with the registrar including source IP address, telephone number, e-mail address, Skype handle or instant messaging identifier, as well as the date, time and time zones of communications.

Registrars are required to keep the first category of personal data for a period of two years after the contract for the domain has been ended. The second category of personal data must be retained for six months after the contract has ended.

The first category of data includes payment data, defined as: *'card on file, current period third party transaction number, or other recurring payment data'*.

The proposed new data retention requirement does not stem from any legal requirement in Europe.<sup>5</sup> It entails the extended processing of personal data such as credit card and communication data by a very large number of registrars. The fact that these data may be useful for law enforcement (including copyright enforcement by private parties) does not equal a necessity to retain these data after termination of the contract. Taking into account the diversity of these registrars in terms of size and technical and organisational security measures, and the chance of data breaches causing adverse effects to individuals holding a domain name, the Working Party finds the benefits of this proposal disproportionate to the risk for individuals and their rights to the protection of their personal data.

Secondly, the Working Party reiterates its strong objection to the introduction of data retention by means of a contract issued by a private corporation in order to facilitate (public) law enforcement. If there is a pressing social need for specific collections of personal data to be available for law enforcement, and the proposed data retention is proportionate to the legitimate aim pursued, it is up to national governments to introduce legislation that meets the demands of article 8 of the European Convention on Human Rights and article 17 of the International Covenant on Civil and Political rights.<sup>6</sup>

The fact that these personal data can be useful for law enforcement does not legitimise the retention of these personal data after termination of the contract. Because there is no legal ground for the data processing, the proposed data retention requirement violates data protection law in Europe.

<sup>5</sup> The European data retention directive 2006/24/EC imposes data retention obligations on providers of public electronic communication networks and services. Registrars are not such providers and are therefore not subjected to this European data retention obligation.

<sup>6</sup> Obligations with regard to the protection of personal data also follow from the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the UN Guidelines concerning computerized personal data files (1990).

In general, we repeat that the problem of inaccurate contact details in the WHOIS database cannot be solved without addressing the root of the problem: the unlimited public accessibility of private contact details in the WHOIS database. In that light, the Working Party welcomes the growing number of registries in Europe that are offering layered access to the WHOIS data.

Yours sincerely,

On behalf of the Article 29 Working Party,



Jacob Kohnstamm  
Chairman



Mag. Marian Maybach  
Dr. Mathias Görg LL.M.  
Mag. Konrad Lenneis  
Mag. Árpád Geréd  
Dr. Georg Zacherl

Internet Corporation for Assigned Names and Numbers  
12025 Waterfront Drive, Suite 300  
Los Angeles, California 90094-2536 USA

Vienna, June 10, 2014  
MM/AG/ICANN\_RAA

**2013 Registrar Accreditation Agreement (RAA)**  
**Legal Opinion pursuant to section 2 of the Data Retention Specification (DRS)**

Dear Sir or Madam!

**I. General Introduction:**

Any registrar entering into the 2013 Registrar Accreditation Agreement (hereinafter “the Agreement” or “RAA”) with the Internet Corporation for Assigned Names and Numbers 12025 Waterfront Drive, Suite 300, Los Angeles, California 90094-2536 USA (hereinafter “ICANN”) will be under the contractual obligation to collect and maintain certain types of data from registrants of a domain name including name and contact details of the domain name holder, logfiles and billing records containing the “means and source of payment”, logfiles about the communication with the registrar including source IP-address, telephone number, e-mail-address, Skype handle or instant messaging identifier, as well as date, time and time zones of communications as detailed in section 1. of the Data Retention Specification of the Agreement (hereinafter also “the Specification” or “DRS”).

The authors of this legal opinion were tasked to examine the compatibility of the Specification with Austrian law. As the result of that analysis this legal opinion will demonstrate that the DRS and its obligations on collection and retention of data

- violate applicable Austrian law
- violate applicable European law
- oblige registrars to commit acts which are in violation of and punishable by applicable law.

If any registrar determines that the collection and/or retention of any data element specified in the DRS violate(s) applicable law, registrar may in accordance with section 2. of the DRS provide written notice of such determination to ICANN and request a waiver from compliance with specific terms and conditions of the Specification (hereinafter also “Waiver Request”). Such Waiver Request can be based on a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that the collection and/or retention of any data element specified herein by Registrar is reasonably likely to violate applicable law.



The authors of this legal opinion, Marian Maybach<sup>1</sup> and Árpád Geréd<sup>2</sup>, each are founding partners of the Austrian law-firm Maybach Görg Lenneis & Partner Rechtsanwälte ([www.mglp.eu](http://www.mglp.eu)).

Marian Maybach was admitted to the bar in Vienna, Austria in 2002 and has a strong focus on data protection issues and many years of related experience in counselling and representing private individuals and companies, in particular in the pharma- and biotech-industry as well as in other industry sectors.

Árpád Geréd has worked as an associate at business law firms in Vienna since 2004 and was admitted to the bar in Vienna in 2009. He focuses on the support of businesses in the fields of IT- and technology, especially on the topics of Cloud Computing, E-Commerce and Smart Metering. Furthermore, he is a member of the board of the Vienna Centre for Legal Informatics, the EuroCloud.Austria and the Computer Measurement Group Austria and Eastern Europe.

The following legal opinion may therefore serve the purpose of enabling registrars within the jurisdiction of the Republic of Austria to draft and file (a) Waiver Request(s) to ICANN.

## II. Legal assessment of the Data Retention Specification:

### A. Protection of Personal Data:

#### 1. General Legal Framework in Austria:

The relevant EU-body of law on data protection law and related areas, in particular the **Directive 95/46/EC** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data was implemented in Austria through the Federal Act concerning the Protection of Personal Data ("*Datenschutzgesetz*", hereinafter "Austrian Data Protection Act" or "*DSG 2000*")<sup>3</sup>.

The fundamental principle with regard to the legitimacy of processing of personal data is stated in Art 1 of the Austrian Data Protection Act in the form of a constitutional provision.

#### **Fundamental Right to Data Protection**

Art 1. (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject<sup>4</sup>.

<sup>1</sup> <http://www.mglp.eu/en/team/marian-maybach>

<sup>2</sup> <http://www.mglp.eu/en/team/arpad-gered>

<sup>3</sup> <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597>

<sup>4</sup> All English translations of the German version of the *DSG 2000* were taken from the homepage of the Austrian Data Protection Authority; <http://www.dsb.gv.at/DocView.axd?CobId=41936>.





Any processing of personal data is therefore - at first - generally unlawful in Austria, unless the controlling party can rightfully put forward a specific legal basis for the intended use of data of the concerned data subjects.

The European Data Protection Supervisor<sup>5</sup>, the Article 29 Data Protection Working Party as well as national European data protection authorities, such as CNIL in France have all raised serious concerns regarding the compliance of the Registrar Accreditation Agreement with European data protection law<sup>6</sup> which are to a large extent equally applicable within the Austrian legal system.

Furthermore, the Austrian Data Protection Act not only protects the data of private individuals but also of legal persons, e.g. corporations, partnerships etc. giving a much wider scope of application to its provisions than in most of the other (European) countries.

**Preliminary result:** Processing of personal data, be it from natural or legal persons, is generally unlawful in Austria unless justified by a specific legal basis for the intended use of data.

## 2. Legal Basis to Process Personal Data under the Austrian Data Protection Act:

In this section the possible bases for lawful processing of personal data and their applicability to the DRS shall be examined.

Art 8 of the Data Protection Act states the different legal bases which would be in principle available for a registrar to legitimize the processing and collection of personal data as it is required by the DRS:

### **Interests in Secrecy Deserving Protection for the Use of Non-Sensitive Data**

Art 8. (1) Interests in secrecy deserving protection are not infringed when using non-sensitive data if

1. an explicit legal authorisation or obligation to use the data exists; or
2. the data subject has given his consent, which can be revoked at any time, the revocation making any further use of the data illegal; or
3. vital interests of the data subject require the use; or
4. overriding legitimate interests pursued by the controller or by a third party require the use of data

(2) The use of legitimately published data and only indirect personal data shall not constitute an infringement of interests in secrecy deserving protection. The right to object to the use of data legitimately published pursuant to § 28 remains unaffected.

(3) Interests in secrecy deserving protection are not infringed according to para. 1 sub-para. 4, in particular if the use of data

1. is an essential requirement for a controller of the public sector to exercise a legally assigned function or

---

<sup>5</sup> [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-04-17\\_EDPS\\_letter\\_to\\_ICANN\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2014/14-04-17_EDPS_letter_to_ICANN_EN.pdf)

<sup>6</sup> <https://www.icann.org/en/system/files/files/waiver-request-ovh-sas-27jan14-en.pdf>





2. is performed by a controller of the public sector in fulfilment of his obligation to provide inter-authority assistance or
  3. is required to protect the vital interests of a third party or
  4. is necessary for the fulfilment of a contract between the controller and the data subject or
  5. is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and if the data were collected legitimately or
  6. concerns solely the exercise of a public office by the data subject.
  7. in case of catastrophe, to the extent required to assist the persons directly affected by the catastrophe, to locate and identify persons missing or dead and to inform next of kin; in the very last case § 48a para. 3 applies.
- (4) The use of data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offences, as well as data concerning criminal convictions and preventive measures does not without prejudice to para. 2 infringe interests in secrecy deserving protection if
1. an explicit legal obligation or authorisation to use the data exists; or
  2. the use of such data is an essential requirement for a controller of the public sector to exercise a legally assigned function;
  3. the legitimacy of the data application otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests in secrecy deserving protection and the manner of use safeguards the interests of the data subject according to this Federal Act or
  4. the transmitting of data is made for a report to an institution in charge of prosecution of a reported criminal act (or criminal omission).

Upon thorough analysis of the subject matter of the RAA and the related facts and interests of the respective parties, to the extent they are known and/or accessible for the authors of this legal opinion, none of the above legal bases stated in Art 8 of the Austrian Data Protection Act can reasonably be applied to legitimize the processing of data under the DRS.

The DRS does neither stem from any legal requirement in Europe<sup>7</sup>, nor by any national legislation measure in Austria providing a potential legal ground to be invoked by a controlling party.

The ICANN itself is a legal entity incorporated under US-laws having no normative power and/or status with regard to any data processing in and/or via Austria. Consequently, the RAA is to be viewed as an agreement under civil law between the respective contractual parties and does not create any statutory rights or obligations (on third parties) to be considered within the framework of Austrian data protection law.

A potential legal basis for the processing of data could be the *"overriding legitimate interests of the controller or a third party"* pursuant to Art 8 para. 1 sub-para. 4 of the *DSG 2000*:

The authors of this legal opinion fully share the view expressed by the Article 29 Data Protection Working Party that even if personal data such as e.g. credit card and communication data of a large

---

<sup>7</sup> statement of the Article 29 Data Protection Working Party, Ref. Ares(2013)1791630-06/06/2013, page 2.



number of registrars may be useful for law enforcement (including copyright enforcement by private parties), this does not equal a necessity to retain these data after the termination of the contract.

The Working Party's assessment and argument that the benefits would be disproportionate to the risk for individuals holding a domain name, also taking into account the diversity of registrars in terms of size and technical and organisational security measures, are conclusive and equally applicable within the Austrian legal framework.<sup>8</sup>

The legal basis that the processing of data is "*necessary for the fulfilment of a contract between the controller and the data subject*" (Art 8 para. 3 sub-para 4 of the *DSG 2000*) cannot be successfully invoked since the processing resulting from the DRS is presumably going beyond such statutory purpose and is rather targeted for (different) interests of ICANN and/or other third parties who are not covered by this statutory provision in Austria.

**Preliminary result: Processing of data under the DRS cannot be legitimized by any of the legal bases stated in Art 8 of the Austrian Data Protection Act. Thus processing of data under the DRS would be unlawful under Austrian law.**

### 3. Declaration of Consent:

The aim of this section is to examine, whether a declaration of consent to be requested from the data subjects may serve as a legitimate means to comply with Austrian data protection requirements under Art 8 para 1 sub-para 2 *DSG 2000* and thus allow the DRS to be lawfully implemented in Austria.

The Austrian Supreme Court has over the years issued various decisions on the required form and elements of a declaration of consent in order to be legally effective for the processing and transmission of personal data<sup>9</sup>.

Indispensable elements of a valid consent are in any case (i) that the purpose(s) of the processing and/or transmission of data is/are described in an explicit and understandable way, and (ii) that the recipients and the countries they are located in are made transparent to the data subject, all at the time the declaration of consent is given. These court decisions substantiated the general principles of a fair use of data stated in Art 6 of the Austrian Data Protection Act.

## Part 2 Use of Data Principles

Art 6. (1) Data shall only  
1. be used fairly and lawfully;

---

<sup>8</sup> statement of the Article 29 Data Protection Working Party, Ref. Ares(2013)1791630-06/06/2013, page 2.

<sup>9</sup> 7 Ob 170/98w; 7 Ob 326/98m; 4 Ob 28/01y, 6 Ob 16/01y, 4 Ob 179/02f, 4 Ob 221/06p; 2 Ob 1/09z.



2. be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further uses for scientific and statistical purposes are permitted subject to § 46 and 47;
  3. be used insofar as they are essential for the purpose of the data application and are not excessive in relation to the purpose;
  4. be used so that the results are factually correct with regard to the purpose of the application, and the data must be kept up to date when necessary;
  5. be kept in a form which permits identification of data subjects as long as this is necessary for the purpose for which the data were collected; a longer period of storage may be laid down in specific laws, particularly laws concerning archives.
- [...]

As not all of the required elements are given within the context of the DRS, a declaration of consent of the data subject cannot serve as a legal basis to render the intended collection of data legitimate.

Furthermore, a data subject may withdraw its consent at any time with the consequence that any further use, including retention, of the data would be inadmissible.

**Preliminary result: A declaration of consent cannot constitute a legal basis for the implementation of the DRS. Any such declaration may be withdrawn, rendering the further processing of data of the relevant data subject unlawful.**

#### 4. Notification Requirements to the Austrian Data Protection Authority:

Art 17 of the Austrian Data Protection Act states notification requirements for data controllers before commencing data applications. Only in case of standard applications and certain other instances enumerated in the statute, a notification to the authority is not required.

In the given case, the data application within the scope of the DRS will – on the basis of the facts accessible to the authors of this legal opinion – require a registrar to notify the processing and also the transmission to the Austrian data protection authority. The question of lawfulness of the data application and the transmission of data will therefore have to be ultimately decided by the Austrian authorities. Non-compliance with notification requirements can lead to administrative fines in the amount of up to € 10,000.-.

#### 5. Legal Consequences of Data Protection Violations:

According to its Art 52, breaches of the *DSG 2000* are subject to administrative fines of up to € 10,000.-. Certain offences, such as intentionally transmitting data in violation of the rules set forth in the Data Protection Act, are punishable by a fine of up to € 25,000.-. However Data protection breaches can in case of intentional behaviour under particular circumstances also constitute criminal offences. Companies who are not compliant are also exposed to civil law claims and injunction measures of competitors.

**Result: Processing of personal data in Austria, be it from natural or legal persons, is generally unlawful unless justified by a specific legal basis for the intended use of data. None of the legal bases stipulated in the Data Protection Act, including a declaration of consent, may serve to legitimize**



the processing of data under the DRS. Austrian registrars could be under the obligation to notify the Data Protection Authority of the processing and the transmission of data on the grounds of the DRS, lest they be subject to administrative fines. However as the implementation of the DRS itself does not comply with applicable Austrian data protection law, any Austrian registrar obeying the DRS would risk administrative fines, civil law suits or injunctive measures.

## B. Other Legal Rules on Data Retention:

### 1. Introduction:

As has been demonstrated above, the obligations set forth in the DRS do not comply with the Data Protection Act. It shall thus be examined, whether other relevant legal rules on data retention exist in Austria and whether they would allow for a legal implementation of the DRS in Austria

On May 3, 2006, the **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 (herein after “Data Retention Directive”)<sup>10</sup> entered into force.

This Directive obliged member states to provide for legal grounds upon which telecommunications data has to be stored for a minimum of 6 months and at most 24 months and provided to police and security agencies, if certain requirements are met. Austria transposed the Data Retention Directive in 2011 by means of an amendment to the Austrian Telecommunications Act (“*Telekommunikationsgesetz*”, hereinafter Telecommunications Act or TKG 2003)<sup>11</sup> which entered into force on February 21, 2012.

Before detailing the provisions of the *TKG 2003* relevant to data retention it should be noted that the *TKG 2003* only applies to operators of public telecommunication networks and services. Thus the Telecommunications Act does not apply to registrars in general but only to those who also act as access-, e-mail or telephony providers. As a consequence the *DSG 2000* alone is applicable to all other registrars.

Furthermore, retention of personal data, as a type of processing of personal data, falls under the rules of the *DSG 2000*, as outlined above. Austrian courts have upheld this dependency by restrictive interpretation of legal rules which so not explicitly grant the right to collect and retain personal data, but may be interpreted in such way. E.g. in its ruling dated September 14, 2011, 6 Ob 104/11d<sup>12</sup>, the Austrian Supreme Court decided that while Art 18 of the Austrian E-Commerce Act may oblige providers to divulge the name and address of users, this provision does not entitle the providers to collect and retain such data unless the requirements of the *DSG 2000* are met. Therefore even such

---

<sup>10</sup> <http://eur-lex.europa.eu/legal-content/EN/ALL/?jsessionId=XYIRThkMypHQz2TChfNxGFq7HRy2qvPf10b1tLp6qnwVD0KKJDJp!1306593838?uri=CELEX:32006L0024>

<sup>11</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849>

<sup>12</sup> [https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT\\_20110914\\_OGH0002\\_00600B00104\\_11D0000\\_000](https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20110914_OGH0002_00600B00104_11D0000_000)





registrars, to whom the *TKG 2003* is applicable, are allowed to collect and retain personal data only to the extent that the *TKG 2003* explicitly creates exceptions to the *DSG 2000*.

**Preliminary result:** Even within the scope of the Telecommunications Act the rules of the Data Protection Act need to be obeyed, unless the Telecommunications Act explicitly stipulates exceptions.

## 2. Data Retention Rules of the TKG 2003:

In this section it shall be examined, whether the *TKG 2003* stipulates exceptions to the *DSG 2000*, due to which the Specifications could be legally applied in Austria.

Art 99 of the Telecommunications Act provides the rules by which traffic data, which is also considered personal data in Austria, may be processed.

### Traffic Data

Art 99. (1) Except in the cases regulated by this Act, traffic data must not be stored or transmitted and shall be erased or made anonymous after termination of the connection. The permissibility of further use of traffic data transmitted in accordance with Par. 5 shall be based on the provisions of the Code of Criminal Procedure [*Strafprozessordnung, StPO*] as well as the Security Police Act [*Sicherheitspolizeigesetz, SPG*].

(2) The operator of a public communications network or service shall store traffic data to the extent required for the purposes of retail or wholesale billing. The traffic data are to be deleted or made anonymous as soon as the payment process has been completed and the charges have not been contested in writing within a period of three months.

[...]

The amount of stored traffic data must be restricted to what is absolutely necessary.

(3) Processing of traffic data must be restricted to persons who handle billing or traffic management, fault recovery, customer enquiries, fraud detection or marketing communications services or provide value added services, or have been commissioned by these persons, and must be restricted to what is absolutely necessary.

[...]

(5) Traffic data may be processed for information purposes with regard to the following:

1. data on communications pursuant to Article 134 No. 2 Code of Criminal Procedure [*Strafprozessordnung, StPO*];
2. access data, even those stored as retained data pursuant to Article 102a Par. 2 No. 1, Par. 3 No. 6 lit. a and b or Article 102a Par. 4 Nos. 1, 2, 3 and 5 for a maximum of six months prior to the query, to courts and public prosecutor's offices in accordance with Article 76a Par. 2 StPO;
3. traffic data and master data in cases where it is necessary to process traffic data for this purpose and for the provision of information on location data to competent law enforcement agencies pursuant to the Security Police Act [*Sicherheitspolizeigesetz, SPG*] in accordance with



Article 53 Par. 3a and 3b SPG. In cases where it is not possible to determine a current location, the cell ID of the last communication registered for the communication equipment may be processed, even in cases where access to data retained in accordance with Article 102a Par. 3 No. 6 lit. d is necessary for this purpose;

4. access data, even in cases where these data were retained in accordance with Article 102a Par. 2 No. 1 or Article 102a Par. 4 Nos. 1, 2, 3 and 5 no more than three months prior to the query, to competent law enforcement agencies pursuant to the Security Police Act [*Sicherheitspolizeigesetz, SPG*] in accordance with Article 53 Par. 3a No. 3 SPG.<sup>13</sup>

Rules on data retention and provision of retained data are stipulated in Art 102a and 102b of the *TKG 2003*.

#### Data retention

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

[...]

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

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

(9) With regard to retained data transmitted in accordance with Article 102b, the claims to information on this use of data shall be based solely on the provisions of the Code of Criminal Procedure [*Strafprozessordnung, StPO*]

#### Provision of information on retained data

Art 102b. (1) Information on retained data may be provided solely on the basis of a court-approved order from the public prosecutor's office for the investigation and prosecution of criminal acts whose severity justifies an order pursuant to Article 135 Par. 2a Code of Criminal Procedure [*Strafprozessordnung, StPO*].

<sup>13</sup> All English translations of the German version of the TKG 2003 were taken from the homepage of the Austrian Regulatory Authority for Broadcasting and Telecommunications; <https://www.rtr.at/en/tk/TKG2003>.



(2) The data to be stored pursuant to Article 102a are to be stored in such a way that they can be transmitted without delay to the competent authorities pursuant to the provisions of the Code of Criminal Procedure [*Strafprozessordnung, StPO*] and in accordance with the procedures set forth in the Code of Criminal Procedure for the provision of information on communications data.

(3) The data is to be provided in an appropriately protected form in accordance with Article 94 Par. 4.

According to these Articles, traffic data may only be stored for a limited time as well as only for certain purposes, namely billing as well as investigating, identifying and prosecuting severe criminal acts. If stored for billing purposes, use of the retained data is restricted to internal personnel. Data stored for law enforcement purposes may only be provided to certain authorities and solely on the basis of a court-approved order from the public prosecutor's office.

Thus the Specification once again does not fulfil the legal requirements for data retention as it does not fall under any of the stipulated purposes, nor does it restrict access to the retained data as prescribed by law.

**Preliminary result:** While the Telecommunications Act stipulates some exceptions to the Data Protection Act, allowing for additional legal retention of data, the exceptions are restricted to certain purposes, of which none applies to the DRS.

### 3. Consequences of Violations:

According to Article 109 (3) *TKG 2003*, any violation of Articles 99, 102a or 102b of the Telecommunications Act is considered an administrative offence and subject to finest of up to € 37,000.-.

Resulting from the explanations above, any Austrian registrar who complies with Art 1.1 or 1.2 of the DRS will find itself in violation of the DSG 2000. Additionally, any registrar to whom the Telecommunications Act applies will find itself in breach of the TKG 2003 as well.

**Result:** The rules of the Data Protection Act, with which the DRS is incompatible, apply even to registrars who fall within the scope of the Telecommunications Act. The exceptions to the Data Protection Act set forth in the Telecommunications Act are restricted to certain purposes, of which none applies to the DRS. Registrars, to whom the Telecommunications Act applies, and who implement the DRS would therefore be subject to administrative fines as well as exposed to civil law claims and injunction measures of competitors.



### C. Developments in Data Protection Legislation:

As the DRS does not comply with existing Austrian legal rules, it should be examined whether there are any developments in the near future due to which any of those rules would be amended.

In its decision dated April 8, 2014, C-594/12<sup>14</sup>, the European Court of Justice has declared the Data Retention Directive invalid, effective from the date the directive entered into force. The court reasoned that *"by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data."*

One of the national courts asking the European Court of Justice to examine the validity of the directive was the Austrian Constitutional Court (*"Verfassungsgerichtshof"*, VfGH), which has before it several constitutional actions brought by more than 11,000 applicants. Those actions seek the annulment of the provision of the *TKG 2003* which transpose the Data Retention Directive into Austrian law. The request of the VfGH for preliminary ruling was in particular based on the question, whether the Data Retention Directive is compatible with the Charter of Fundamental Rights of the European Union (*"Charter"*)<sup>15</sup>. Already in his request the *Verfassungsgerichtshof* took the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them.

It is therefore very likely that the relevant provisions of the *TKG 2003* will be annulled by the VfGH. As a consequence the legal possibilities for the retention of personal data would be much narrower, than they are now, since then even fewer exceptions would exist to the fundamental rule of Art. (1) *DSG 2000*, according to which processing of personal data is at first generally unlawful in Austria. Therefore the results of this legal opinion would be enforced by such annulment.

In this context it should be noted that according to the European Court of Justice for a regulation to comply with the Charter, it *"must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."* The DRS does not contain any such rules or safeguards. Therefore even if it was otherwise compatible to Austrian, application of the DRS would still not be legal due to these shortcomings.

**Result:** The only foreseeable change in legislation in the near future is the possible annulment of the data retention provisions of the *TKG 2003*. Such annulment would further restrict the legal possibilities for data retention and thus enforce the results of this legal opinion.

---

<sup>14</sup>

<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130de3f99dbbcf699478886ebd95af8b2bb3b.e34KaxiLc3eQc40LaxqMbN4OaNqPe0?text=&docid=153045&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=35879>

<sup>15</sup> [http://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](http://www.europarl.europa.eu/charter/pdf/text_en.pdf)





### III. Summary:

On the basis of the publicly accessible information with regard to the Data Retention Specifications of the Registrar Accreditation Agreement of 2013, the processing and transmission of personal data under this Agreement is reasonably likely not in compliance with the statutory requirements of the Austrian Data Protection Act. In those cases where the Austrian Telecommunications Act is applicable to registrars, they would find themselves in breach of the rules of that law as well.

The different legal bases to process personal data which are in principle available under Austrian law do not apply to the given case. The Specifications do in particular not stem from any legal requirement in Europe or Austria respectively, nor would e.g. a declaration of consent render the projected uses of the personal data legitimate. Furthermore none of projected uses correspond to the uses set forth in the Telecommunications Act.

By conducting their business in line with the provisions of the Agreement, Austrian registrars therefore run the risk to be subject to administrative fines or other measures of the Austrian (data protection or telecommunications) authorities and could at the same time be exposed to civil law suits and/or injunctive measures of the concerned data subjects and/or competitors of the registrars, including cease and desist claims and/or claims for damages.

Austrian registrars should therefore request and be granted a waiver from compliance with section 1 of the Specification.

Yours sincerely,

Marian Maybach

Árpád Geréd