Identification: AUT-2014-2-003

a) Austria / **b)** Constitutional Court / **c)** / **d)** 27.06.2014 / **e)** G 47/2012, G 59/2012, G 62,70,71/2012 / **f)** / **g)** / **h)** www.icl-journal.com; CODICES (German).

Keywords of the systematic thesaurus:

2.1.1.4.4 Sources – Categories – Written rules – International instruments – **European Convention on Human Rights of 1950**.
2.1.1.4.18 Sources – Categories – Written rules – International instruments – **Charter of Fundamental Rights of the European Union of 2000**.
5.3.32 Fundamental Rights – Civil and political rights – **Right to private life**.
5.3.32.1 Fundamental Rights – Civil and political rights – Right to private life – **Protection of personal data**.

Keywords of the alphabetical index:

Database / Data, personal, collecting, processing / Privacy, balance between rights and interests.

Headnotes:

Data retention may be a suitable means to control serious crime. However, whether it conforms with the requirements of data protection and with the right to respect for privacy depends on the conditions for the storage of such data, requirements governing their deletion, and measures in place to access the retained data.

Summary:

I. Article 102a of the Telecommunication Act of 2003 *(Telekommunikationsgesetz* 2003*)* obliged providers of public communication services to store certain categories of data from the time of generation or processing up to six months after the communication is terminated. The data were to be stored solely for the purpose of investigating, identifying and prosecuting criminal acts, which shall require, due to the severity, an order pursuant to Article 135 of the Code of Criminal Procedure *(Strafprozessordnung)* (hereinafter, "CCP").

According to Article 135 CCP, the information contained in such data must be given to prosecution authorities in specific cases and in accordance with national laws. The situations include: if the provision of such information was expected to help investigate a wilfully committed criminal act that carried a sentence of more than six months and the owner of the technical device which was or would be the source or target of data communication granted explicit consent. The data must also be surrendered to competent authorities if such information was expected help investigate a wilfully committed criminal act carrying a sentence of more than one year and it could be assumed based on given facts that the provision of such information would allow data about the accused to be ascertained. Alternatively, if, based on given facts, it was expected that the whereabouts of a fugitive or an absent, accused person who was strongly suspected of having wilfully committed a criminal act carrying a sentence of more than one year could be established.

According to Article 53.3a of the Security Police Act *(Sicherheitspolizeigesetz)*, police authorities are entitled to request information concerning the name and address of a user who was assigned an IP address at a particular time from providers of public communication services. They can make the request if the data serve as an essential prerequisite to counter a concrete danger to the life, health or freedom of an individual in the context of the first general obligation to render assistance, a dangerous attack or a criminal association, "even if the use of retained data is required for this".

Pursuant to Article 53.3b of the Security Police Act, police authorities are further entitled to require from providers of public telecommunication services information about location data and the international

mobile subscriber identity (IMSI) of the carried equipment of a person in danger or a person accompanying the person in danger, “even if the use of retained data is required for this”.

In spring 2012, subscribers to various communication services within the meaning of Article 102a of the Telecommunication Act of 2003 filed a request for constitutional review with the Constitutional Court. They maintained that the provisions governing data retention breached their constitutionally guaranteed rights. The applicants criticised that these provisions required the operator of their communication networks to store specified data without any concrete suspicion, irrespective of technical requirements or billing purposes, and regardless of, or even against, their will.

II. In November 2012, the Constitutional Court stayed its constitutional review proceedings. It referred to the Court of Justice of the European Union for a preliminary ruling as to the question whether the Data Retention Directive of 2006 was compatible with Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union. The reason for this request was that the Directive, if implemented into national law, would be incompatible with the fundamental rights to respect for private life pursuant to Article 8 ECHR and to protection of personal data set out in Article 1 of the Data Protection Act of 2000 (hereinafter, “CPA 2000”, *Datenschutzgesetz* 2000*)*. As a result, the Constitutional Court could be precluded from reviewing the legal regulations on data retention. On 8 April 2014, however, the Court of Justice of the European Union ruled that the Data Retention Directive was invalid. Consequently, there was no obstacle for the Constitutional Court to assess the provisions under review against the measure of the fundamental right to protection of personal data.

Pursuant to Article 1 CPA 2000, every person is entitled to secrecy for personal data concerning him or her, especially with regard to his or her private and family life, insofar as he or she has an interest worthy of such protection. Any restriction to this right must be based on laws necessary for the reasons stated in Article 8.2 ECHR. Going beyond Article 8.2 ECHR, Article 1.2 CPA 2000 requires that any law providing for the use of data worthy of special protection must provide suitable safeguards for the protection of the private interest in secrecy.

The Constitutional Court held that both the storage of personal data of the users of public communication services and the obligation to provide information about this data to police and prosecution authorities constitute an interference with the fundamental right to data protection and the right to respect for private and family life.

The Constitutional Court agreed that the provisions concerning the retention of data and information on retained data were, in principle, suitable to achieve the objectives mentioned in Article 8 ECHR, particularly the maintenance of public peace and order and the protection of rights and freedoms of others.

However, as the provisions under review did not establish any limitation relating to the seriousness of the offence that would justify interference with the fundamental rights of the individuals concerned, the Constitutional Court found that this interference was not proportionate to the aim pursued.

Moreover, the Constitutional Court established that the retention of personal data failed to satisfy the requirement of proportionality. The Court pointed out that this measure was particularly burdensome, given that, first, it concerned the exercise of fundamental rights, particularly the freedom of expression, information and communication. Secondly, the vast majority of the individuals affected were without previous criminal conviction. Lastly, a vast number of people could potentially have access to the stored data, which posed an increased risk of unauthorised access and abusive use of personal data.

However, the statutory rules regarding the data retention lacked appropriate measures to alleviate this interference, such as criminalising any improper use of retained data and ensuring that individuals affected could exercise their right to erase *vis-à-vis* providers of public communication services effectively.

Finally, with a view to the right of erasure, the national law did not provide any specifics that would address the requirement of a statutory regulation within the meaning of Article 1.2 CPA 2000. In particular, it was unclear if the data had to be deleted in such a way that the recoverability of the data was excluded.

Cross-references:

Court of Justice of the European Union:

- nos. C-293/12 and C-594/12, 08.04.2014, *Digital Rights Ireland Ltd et al.*

Languages:

German.