Ludwig Boltzmann Institute
Human Rights

Hannes Tretter

The right to data protection – the European and the Austrian approach

1. Introduction

Under the Ukrainian Data Protection Law "On Amendments to Certain Legislative Acts of Ukraine Concerning Improvement of the Institutional System of Personal Data Protection" which came into force on 1 January 2014, the Ombudsperson of Ukraine is defined as the authorised body for the personal data protection in the sphere of exercising control over observance of legislation on personal data protection – which extends as well to enterprises, organisations and institutions of private ownership and natural persons. This is surprising since data protection is not a classical task of an Ombud but handled by an independent data protection commission. Therefore, this important function is also new to the Ukrainian Ombudsman why our project is also dealing intensively with this topic in order to bring the Ukraine data protection law and practice into line with European standards and good practices.

To better understanding the background and importance of the right to data protection I would like to refer to its theoretical and dogmatic fundaments. It was a law review article written by the very famous US lawyers Samuel Warren and Louis Brandeis, which was published under the title "The Right to Privacy" already in 1890 (!) in the Harvard Law Review. It is said to be one of the most influential essays in the history of American law and is widely regarded to advocate a right to privacy, articulating that right primarily as a "right to be let alone". The article was directed against some new practices of business and media, namely the upcoming "yellow press", based on the evolution of the photography and the widespread circulation of newspapers, both of which have contributed to the invasion of an individual's privacy.

In the following, the "right to privacy", often also in terms of the "right to private life" or the "right to self-determination", became the theoretical and dogmatic fundament of today's right to protection of personal data. Its importance has dramatically increased, triggered by modern technologies which are used by states as well as by private enterprises to collect our personal data in order to more easily achieve their tasks and goals. Today, the saying "Nothing to hide – nothing to fear" is not any more true, if it ever was true. Today, state authorities and private enterprises do know nearly everything about us – about our identity, origin, status and residence, family and relationships, profession, assets and income, beliefs, preferences, interests, sexuality, behaviours and attitudes. Thus, we already became "transparent human beings" and are going to become "digitally affected and steered ones", sometimes being in fear to tread any paths that are surveilled or are dedicated to collect data. And maybe we will become in future "siliconised human beings", which means to get instrumentalized by the Silicon Valley – by Google, Facebook, Apple, Amazon & Co, which are providing us with selected and filtered information and advertisement, telling us on the iPhone or via "Google glasses" what to do, where to go, what to buy, what to believe, whom to trust, whom we should like and for whom to vote – and this so far without any independent control.

This is why we can say that data protection is a cross-cutting topic, relevant in nearly all aspects of daily life and has to be observed and applied whenever state authorities take legal actions, pass, amend or implement laws, or whenever we use the offers and goods and services of the private sector.

However, we would like to use the comfortable modern technologies without being in fear that our personal data are misused. This can be possible if all requirements of an effective protection of personal data are legally guaranteed and observed in practice. First and foremost, there must be a fair balance between the right to data protection and opposing rights and interests. Therefore, limitations of the right to data protection have provided for by law, and must be necessary within a democratic society and proportional to defend legitimate interests of the public as well as the rights and freedoms of others. Additionally, effective legal remedies and non-judicial monitoring have to be provided for in case of any violation of the right to data protection.

2. The European approach

This approach is reflected in Article 8 of the European Convention of Human Rights (ECHR) of the Council of Europe (CoE) which is guaranteeing, inter alia, the right to private life which is – according to the case-law of the European Court of Human Rights (ECtHR) – covering also the right to data protection as an inherent element. The right to data protection is also, but explicitly, guaranteed by Article 8 of the EU Fundamental Rights Charta (FRC). So far, the Court of Justice of the EU (CJEU) decided only recently on two spectacular cases in favour of the right to data protection, both based on claims of Austrian citizens: So, the Court annulled the EU Data Retention Directive because violating the right to data protection by collecting and storing personal communication and location data without any suspicion, and in the case of Max Schrems against Facebook the Court declared invalid the Safe Harbour Agreement between the EU and the US because of a lack of procedural guarantees.

Actually, the principal EU legal instrument is the Data Protection Directive 95/46/EC 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. The aim of adopting the Data Protection Directive was the necessary harmonisation of data protection law at the national level and to achieve comparable conditions for the free movement of data within the EU. The Data Protection Directive was designed to give substance to the principles of the right to privacy already contained in the Data Protection Convention 108 of the CoE, and to expand them. Corresponding to EU primary law in force at the time of the adoption of the Data Protection Directive, the material scope of the Directive is limited to matters of the internal market. Outside its scope of application are, most importantly, matters of police and criminal justice cooperation. Data protection in these matters arises from different legal instruments.

On 25 May 2018, a new legal act, the General Data Protection Regulation, adopted on 27 April 2016, will come into force which shall strengthen and unify data protection for individuals within the EU, and also addresses export of personal data outside the EU. The primary objectives of the Regulation are to give citizens back the control of their personal data (in particular the “right to be forgotten”) and to simplify the regulatory environment for international business by unifying the regulation within the EU. Additionally, there will be also a new Directive which applies to police procedures.

3. The Austrian Approach

It is important to mention that Austria had a Data Protection Act already since 1980, including a fundamental right to data protection, guided by Article 8 of the ECHR, although already explicitly including data processing by private controllers.

The provisions of the EU Data Protection Directive 1995 have been faithfully implemented by the Data Protection Act of 2000, trying to spell out also more explicit rules for balancing interests in difficult constellations.

Although Austria is a federal state, we have only one data protection authority, which is a federal authority. The competences for dealing with data protection complaints are split between the Data Protection Authority and the Administrative Courts. As the Austrian law 2000 is a so called „omnibus legislation", its present applicability extends to all processing of personal data within the entire sphere of the law. This means that it also covers processing of data for purposes of public security police or criminal justice and even the processing of data by secret service institutions. For the latter the law will probably be maintained also after the coming into force of the new EU general Regulation, as this area is not covered by any legal act of the EU, due to the lack of EU competence for such matters. Another matter which is covered by the Austrian Data Protection Act 2000, but not by the EU Regulation, is data protection for legal persons, which is in principle actually also guaranteed under Article 8 ECHR.

As we can see, there are some most challenging and future-oriented data protection topics to be dealt with in the course of this EU Twinning project – in order to find best fitting solutions for the Ukrainian partners on the path towards the EU.

Hannes Tretter

Junior Project Leader, Twinning project "Implementation of the best European practices with the aim of strengthening the institutional capacity of the Apparatus of the Ukrainian Parliament Commissioner for Human Rights to protect human rights and freedoms"

Scientific Co-Director, Ludwig Boltzmann Institute of Human Rights, Vienna, Austria

Professor for Fundamental and Human Rights Law, University of Vienna, Austria