Dr. Attila Péterfalvi:

National regulations and international challenges in the field of data protection in Hungary

National Authority for Data Protection
and Freedom of Information

I International Forum on Privacy and Data Protection

19.05.2021

National Authority for Data Protection and Freedom of Information

Historical background of the Hungarian legislation

Adoption of the first data protection act in Hungary (and in the Central-Eastern European region!): Act LXIII of 1992

Historical backgrounds:

- Change of the political system – from communist dictatorship to democratic Rule of Law
- Comprehensive amendment to the Constitution of Hungary, 1989
- Introduction of the new constitutional rights (including: right to privacy, right to know)
- New democratic institutions (system of democratic „checks and balances") to guard the new rights (constitutional court, ombudsman, state audit office etc.)

.

National Authority for Data Protection
and Freedom of Information

3 specific features of the Hungarian modell:

1. Data protection and Freedom of Information as „two sides of the same coin”

2. Transition from an ombudsman-model to a strong authority

3. Supervision of the state security agencies and control of classified data
   Legal instruments for supervision:
   - Investigation
   - Administrative proceedings for data protection
   - Administrative proceedings for the control of classified data
   - Data protection audit

National Authority for Data Protection and Freedom of Information

Legal background of the data protection and freedom of information in Hungary

1. **The Fundamental Law of Hungary**

Section (3) and (4) of Article VI

(3) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest.

(4) The application of the right to the protection of personal data and to access data of public interest shall be supervised by an independent authority established by a cardinal Act.

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**)

3. **Act CXII of 2011 on Informational Self-determination and Freedom of Information**

Contents:

- general rules on data protection and freedom of information
  - *x* except: the data processing activity falling under the scope of the GDPR
- legal status & organisational framework of the NAIH
- procedural rules
- Implementation of the **Law Enforcement Directive** and the rules of the national security services and the data process of national defence

Independence of the Authority

Legal status of the Authority:

The DPA is an **autonomous state administration organ**. [Section 38 (1) Act CXII of 2011]

Its **independence is ensured** in practice by the followings:

- The allocation of financial and human resources
- The use of the DPA's resources
- The staff management
- The budget

National Authority for Data Protection and Freedom of Information

Challenges I.
Assisting SMEs in applying the GDPR - the STAR II project

The application of the GDPR in practice means a major challenge to all those concerned.

Compliance with the GDPR requires the shaping of a proper data processing practice. Proper practice, however, has also to be maintained. New processes, methods and good practices have to be introduced.

- Aim of assisting SMEs in applying the GDPR
- Taking the sturcture and needs of SMEs into account, the project helps the enterprises in question shape an appropriate practice.
- NAIH was operating a hotline for SMEs between 2019 and 2020. This period the kkvhotline@naih.hu of the NAIH provided information for SMEs throughout the European Union in respect of the interpretation and proper application of the GDPR.
- On the basis of the questions and issues raised by the SMEs, a handbook has been compiled which is accessible and usable throughout the EU.

Challenges II.
Use of Artificial Intelligence

New technologies: opportunities and risks

Referring to the White Paper of the Commission of the European Union on reliable artificial intelligence: an **AI system must ensure in every stage of its life cycle that individuals have full disposal over their own data and that their data cannot be used to cause them harm**.

According to the territorial scope of the GDPR: **EU citizens' personal data should only be processed** – Big Data, AI, etc. - **where data protection is at European level** (for example problems of privacy shield mechanism).

„GDPR Article 3
Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Thank you for your attention!

Dr. Attila Péterfalvi, President
Honorary University Professor

H-1055 Budapest, Falk Miksa street 9-11.
1363 Budapest, Pf.: 9

Tel.: +36 1 391-1400
Fax: +36 1 391-1410

peterfalvi.attila@naih.hu
ugyfelszolgalat@naih.hu

www.naih.hu