Cybersecurity and the protection of personal data

Dániel Eszteri Ph.D.
Hungarian National Authority for Data Protection
and Freedom of Information

Conference Digital Economy, Prague
17. 03. 2016.

Definition of personal data

- Shall mean data relating to any natural (human) person directly or indirectly.
- E.g.: name, identification number, factors specific to his/her physical, physiological, mental, economic, cultural or social identity and conclusions drawn from them.
- Legal background for protection of personal data within the EU are national data protection acts of the Member States and the Data Protection Directive (95/46/EC).
- The new European data protection regulation (direct effect) will be adopted formally by the EU Council in 2016. The regulation will take effect after a two-year transition period.

Data processing in digital environments

Electronic, online processing of personal data related to:

- Large databases, Internet of things
- Social networking
- Consumer profiling for marketing purposes and online advertisement
- Big data analysis
- Cloud computing

Protection of personal data and IT security

- Data security: Data controllers (and within their sphere of competence data processors) must implement adequate safeguards and appropriate technical and organizational measures to protect personal data.
- Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.

Concept of data breach in the new EU regulation

- Definition of *‚data breach'*: national data protection laws of many Member States and the upcoming EU regulation also defines it.
- Data breach in a general term: Release of secure information to untrusted environment.
- Data breach from data protection point of view: unlawful processing or process of personal data, in particular: illegitimate access, alteration, transfer, disclosure, deletion or destruction, accidental destruction or damage.

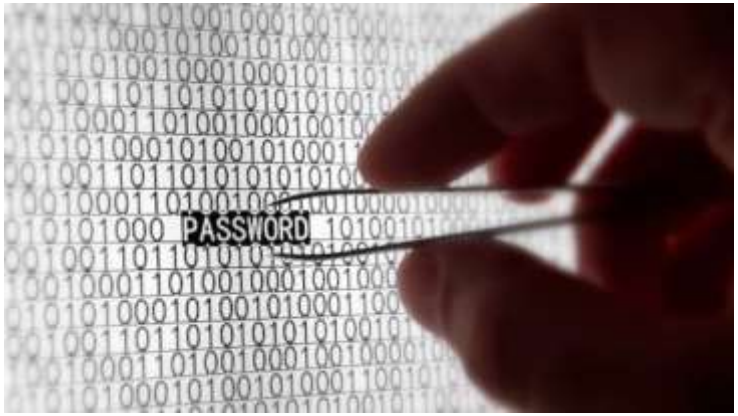
Legal consequences of a data breach

- The data controller shall provide information concerning the conditions and effects of the data breach and measures taken with a view to eliminate them → data subjects, DPA

- Data controllers shall keep records containing the personal data affected and the personal scope affected by the data incident, the time, circumstances and effects of the data incident and measures taken to eliminate thereof.

Crimes committed in IT environment and protection of personal data

- Convention on Cybercrime 2001
- Directive 2013/40/EU on attacks against information systems
- Breaching information systems, spreading malicious software, phishing, identity theft
- Motives: financial, economic, political, cyberbullying
- Cybercrime affects personal data of the victim in most cases
- Users: big responsibility, but lack of information



Privacy impact assessment (PIA) as tool for security

- The PIA is a process which evaluates and manages the privacy risks the intended data processing may trigger
- The PIA should, in general consist of

a) a scheme of data flow which enables to showcase the points where the data processing can be modified and the privacy (and data protection) vulnerabilities.

b) an analysis which states the compliance to technical and legal requirements and the adequate level of the protection of privacy

c) legal and technical solutions for mitigating privacy risks and if privacy intrusion occurs an action plan which contains measures which will minimize the negative effects, consequences (including data security issues!)

National Authority for Data Protection
and Freedom of Information

Thank you for the attention!

Dániel Eszteri

H-1125 Budapest, Szilágyi Erzsébet fasor 22/c.
H-1530 Budapest, Pf. 5.

Tel.: +36 391-1400

eszteri.daniel@naih.hu
www.naih.hu