

Privacy and Protection of Personal Data in the EU Transfers of Personal Data to third Countries

European Commission

Hana Pecháckova/Dr. Barbara Rhode

**Directorate-General Justice, Freedom and Security,
Unit D5 – Data protection**

Eu Delegation to Japan, the Head of Science and Technology



European Commission

DG Justice, Freedom and Security

**International Workshop on Information Systems for Social Innovation 2009
Tokyo, Japan
30 September 2009**

Goal of the presentation

- **Explain** work of the European Commission in the field of data protection and privacy
- **Outline** current data protection and privacy legislation in the EEA including basic data protection principles
- **Explain** what is necessary for transferring data to third countries: example EU – Japan, adequacy procedure
- Next steps /solutions



EC legal framework

- Article 8 of the **Charter of Fundamental Rights** of the European Union establishes the right to the protection of personal data as a **fundamental right**;
- **Directive 95/46/EC** of 24th October 1995 concerning the protection of natural persons in respect of the processing of personal data and the free movement of such data (Data Protection Directive); *currently, online public consultation on the future of privacy & data protection has been opened*
(http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm)
- **Directive 2002/58/EC** of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); *currently undergoing a review*



EC legal framework

- Data Protection Directive transposed into 27 Member States (MS) national laws.
- Directive based on one of the principles of a functional internal market - i.e. free movement of goods, persons, services and capital.
- Based on this principle MS shall ensure that, among other things, also personal data should be able to **flow freely from one MS to another.**



Scope of Directive 95/46/EC

- Applies to the protection of **natural persons**, whatever their nationality or place of residence
- Applies to **private and public** sectors
- Applies to processing of personal data **whatever the technology used** (*technology neutral approach*)



Principles

- **Proportionality, purpose limitation**
 - Personal data must be collected for a specified, explicit and legitimate purpose
 - Not further processed in a way incompatible with those purposes
- “Rule of **privacy by design**”
- Data **minimisation**
- **Accurate** and kept **up to date**
- Data should be kept in a form which permits identification for no longer than necessary



Data processing must be *legitimate*

- Consent (freely given specific and informed indication) – *very challenging in new technologies and online services*
- Necessary for performance of a contract
- Necessary for compliance with a legal obligation of the controller
- Legitimate interests of the controller (balance of interest)
- Necessary in order to protect the vital interest of the data subject



Data Protection Authorities

- Fully **independent** supervisory bodies
- Responsible for **enforcing national legislation**
- **Powers** of investigation, intervention and to engage in legal proceedings or to bring violations to the attention of the judicial authorities



Article 29 Working Party

What is it?

- Independent advisory body composed of representatives of all EU Data Protection Authorities (DPA)

(http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm)

- Secretariat ensured by the European Commission (DG JLS)

What are its competences?

- It has an advisory role regarding data protection issues
- Issues opinions or recommendations on data protection which are soft law instruments (recent Opinions on search engines, online social networking, etc.)
- evaluates the level of adequate protection in 3rd countries



Transfers of Data – general issues

- Article 25 of the Data Protection Directive
- Data from EEA to third countries can be transferred **only** if the third country in question **ensures an adequate level of protection**.
- The **adequacy level is assessed in the light of all the circumstances surrounding a data transfer operation**, in particular, purpose of the operation, country of origin and of final destination, the rule of law, security measures, etc...
- If a third country does not afford an adequate level of protection, MS shall take the necessary steps to prevent any transfers
- The Commission may find that a third country ensures an adequate level of protection by reason of its domestic laws or international commitments – **“adequacy procedure”**



Adequacy – general issues

- Protection of personal data is a **fundamental right in the EU**
- Existence of **appropriate data protection rules** and **administrative capacity** in the third countries is of **horizontal importance** and a **condition for success in a number of policy areas**
- in view of **considerable benefits** it would bring, namely:
 - easier flow of personal data between the parties, **thus better business and administrative cooperation**;
 - **economy of trust**: development of e-commerce, since individuals will be more ready to buy on the internet marketplace if their data are protected and will not be abused;
 - **good governance**: respect for fundamental rights in the respective countries from undue private and public interferences
- The **level of protection has to be assessed in the light of all the circumstances** surrounding a data transfer (nature of data, duration, country of origin, country of final destination, rule of law, security measures)



Adequacy - legal steps

- The Commission has been granted the **power to determine, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into** (Article 25 (6) of Directive 95/46/EC).
- In order to initiate an adequacy finding procedure, an **official request** made by the representatives of the third country shall be lodged to the European Commission.
- The adoption of a (comitology) Commission decision based on Article 25 (6) of the Data Protection Directive involves:
 - a proposal from the Commission
 - an opinion of the Article 29 Working Party
 - an opinion of the Article 31 MS Committee delivered by a qualified majority of MS
 - a thirty-day right of scrutiny for the EP (to check if the Commission has used its executing powers correctly). EP may, if it considers it appropriate, issue a recommendation.
 - the **adoption of the decision** by the College of Commissioners.



Adequacy

- The Commission may find that a third country ensures an adequate level of protection.
- The effect of such a decision is that personal data can flow from the 27 EU MS and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.
- Japan has not yet been considered by the EU as a country providing an adequate level of protection with respect to the protection of personal data and fundamental rights of the persons relating to their private life.
- Therefore a transfer of data to this country from an EU country has to be carried out in pursuant to Article 26 of Directive 95/46/EC which implies a prior information/authorization by the national data protection authority.
- In order to show that the transfer provides appropriate guarantees to ensure the protection of the data subjects, this can be particularly be made by specific contractual arrangements, for instance by using the one of the standard contractual clauses models approved by the Commission.



“Adequate” 3rd countries

- The Commission's decision determining adequate protection **increases legal certainty** for companies in the EU and makes the export of personal data to the country concerned easier.
- Examples: Switzerland, Argentina, Isle of Man, the Bailiwick of Guernsey, the Safe Harbour, Canada, the Bailiwick of Jersey



Adequacy – conclusions

- The Commission launched a preliminary step to begin assessing the state of play in Japan
- Analysis has been prepared covering data protection and privacy legislation in Japan
- EU – Japan Business Dialogue Roundtable discussed personal “data protection regime”, Tokyo, 3-4 July 2008
- BDRT recommended that two authorities should work together to ensure an international equal, transparent and secure data protection regime between EU and Japan
- Commission is preparing a Progress report for the BDRT
- Commission intends to improve the co-operation in the field of the protection of personal data and data transfers and to work towards the free movement of personal data between the EU and Japan according to the highest international standards.
- The Commission is considering carrying out an in-depth analysis in order to have a complete picture of Japanese data protection laws and possibly launch an adequacy finding procedure.
- Nevertheless, this initiative should be supported by the Japanese counterpart.
- In order to initiate an **adequacy finding procedure**, an **official request** made by the representatives of Japan shall be lodged to the European Commission.



Thank you very much for your attention!

Questions?

Web site:

http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

or

hana.pechackova@ec.europa.eu

