EU Data Protection Law Requirements for Cloud Computing Agreements

Dr. Thomas Helbing

IT / Privacy Lawyer

www.thomashelbing.com

Overview

1. EU Data Protection Directive
2. Contracts and Security Measures
3. Data Export to Third Countries

1) EU Data Protection Directive
a) Introduction

- Directive 95/46/EC
- Harmonized framework
- Addressed to EU member states
- Different implementations in national laws
- Different interpretation by national authorities and courts

1) EU Data Protection Directive
b) Overview

- Definitions ("Personal Data", "Processing")
- Principles and legitimacy of data processing
- Applicable national laws
- Rights of data subjects
- Confidentiality and security
- Notifications
- Remedies, liability and sanctions
- Data export to Third Countries
- Supervision

1) EU Data Protection Directive
c) Scope of Application

- *This Directive shall apply to the processing of personal data (…)*
  Article 3 (1)
- *'personal data' shall mean any information relating to an identified or identifiable natural person*
  Article 2 (a)
- *'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, (...), such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;*
  Article 2 (b)

1) EU Data Protection Directive
d) Controller / Processor

- *'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.*
  Article 2 (d)
- *'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.*
  Article 2 (d)

2) Contracts and Security Measures
a) Security Measures

- Controller remains responsible for compliance
  - … *controller must … choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.* Article 17 (2)
- Security measures
  - *controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access … and against all other unlawful forms of processing.* Article 17 (1) 1
  - *measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.* Article 17 (1) 2

2) Contracts and Security Measures
b) Contracts

- Article 17 (3) (4):
  - Written controller-processor agreement required
  - Mandatory provision: processor shall act only on instructions of controller
  - EU-Processors: Security measures as defined by law of country where processor is established to be observed

3) Data Export to Third Countries
a) Overview

- Data export to non-EU/EEA countries: „adequate level“ of data protection to be ensured, Article 25 (1)
- Exceptions: Switzerland, Canada, Argentina, Guernsey, the Isle of Man and Jersey
- Instruments
  - EU Standard Contractual Clauses
  - Safe Harbor (for US only)
  - Binding Corporate Rules

3) Data Export to Third Countries
b) Standard Contractual Clauses (1)

- Data Exporter and Data Importer enter into contract with set of EU standard clauses
- EU clauses may not be altered
- Registration / notification to DPAs
- Different sets for controller-controller and controller-processor transfers
- Updated controller-processor set applicable from 15 May 2010

3) Data Export to Third Countries
c) Standard Contractual Clauses (2)

- Subcontracting scheme (from 15 May 2010).
  - Data Importer uses sub-contractor (PaaS, storage, maintenance etc.)
  - Subcontracting requirements
    - Data Exporter to consent
    - Data Importer to impose terms of Clauses to sub-contractor

3) Data Export to Third Countries
d) Safe Harbor

- Only for US organizations
- Declaration to comply with Safe Habor Principles
- Supervision of the US Department of Commerce
- Onward-Transfer Principle in case of disclosures to third parties

3) Data Export to Third Countries
e) Binding Corporate Rules

- Group-wide privacy policy that has to comply with certain EU requirements
- To be legally binding internally and externally
- All group member ensure adequate level of data protection

➔ only applicable to intra-group transfers

Thank you for listening…

Dr. Thomas Helbing (Attorney at Law)
Treffauer Straße 28, 81373 München, Germany

Web: www.thomashelbing.com
Mail: helbing@thomashelbing.com
Phone: +49 (0) 89 39 29 70 07

VISIT OUR WEBSITE
www.thomashelbing.com/en