Workshop: A Compliance Challenge – Data Protection and Privacy

Meike Kamp, LL.M., Desk Officer, Berlin Commissioner for Data Protection and Freedom of Information

Jessica Jacobi, Partner, Kliemt & Vollstaedt, Member Firm of Ius Laboris Network of Labour Law Firms

Melissa Lea, Chief Global Compliance Officer, SAP AG

Directive 95/46/EC: Data transfer to third countries and the future of data protection in the EU

Meike Kamp, LL.M.
Berlin Commissioner for Data Protection and Freedom of Information

Data transfer to third countries

- „Third Country“: Every country that is not EU Member State or EEA Member Country.
- Art. 25 (1) Directive 95/46/EC: Adequate level of data protection in the third country?
- EU-Commission´s Decisions recognizing the following countries as providing adequate level of data protection (Art. 28 (6))
  - Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, Australia, Andorra, Faeroe Islands, Israel
- Derogations from Art. 25: Data subject´s consent etc., Art. 26 (1) a)-f).

Data transfer to third countries

- Other instruments for data transfers:
  - Art. 26 (4): Model Contracts for the transfer of personal data to third countries ("Standard Contractual Clauses"):
    - Controller to controller (2001/497/EC)
    - Controller to controller (2004/915/EC)
    - Controller to processor (2002/16/EC)
  - USA **è** Commission Decision 2000/520/EC:
    - Safe Harbor Privacy Principles and related FAQ´s
  - Art. 26 (2): Binding Corporate Rules, Individual Contract / Ad-hoc Contract

The future of data protection in the EU

Review of the data protection legal framework

Commission Communication

COM(2010) 609

The Commission´s strategy

- **Strengthening individuals' rights**
  - Commission will consider
    - how to ensure a coherent application of data protection rules,
    - introducing a general principle of transparency,
    - modalities for a general personal data breach notification,
    - extending the power to bring action before national courts
    - extending the existing provisions on sanctions.
  - Comission will examine the concept of sensitive data and ways of clarifying and strengthening the rules of consent.

...

- **Enhancing the Single Market dimension**
  - By examining the means to achieve further harmonization.
  - By reducing the administrative burden on companies (notification system) and ensuring a true level-playing field.
  - By revising and clarifying the provisions on applicable law.
  - By examining elements to enhance data controllers´ responsibility.
  - By examining self-regulatory initiatives.
- **More effective enforcement of the rules**
  - By strengthening and further harmonizing the role and powers of Data Protection Authorities.

. . .

- **Revising data protection rules in the area of police and criminal justice**
  - Under the Lisbon Treaty, the EU now has the possibility to lay down comprehensive and coherent rules on data protection for all sectors, including police and criminal justice.
- **Ensuring high levels of protection for data transferred outside the EU**
  - By improving and streamlining procedures for international data transfers.
  - By clarifying the adequacy procedure.
  - By defining the core EU data protection elements for usage in all types of international agreements.

State of play

- Public consultation until the 15th of January 2011.
    - On the basis of the consultation the Commission will present proposals for a new general data protection legal framework in (the summer of) 2011, which will then need to be negotiated and adopted by the European Parliament and the Council.
- 24th of February 2011: Council conclusions on the Communication of the Commission.
- The Commission has not yet decided what legal instrument (directive or regulation) will determine the new legal framework on data protection.

Overview: Data Protection in the EU

Jessica Jacobi

Partner, Kliemt & Vollstaedt, Member Firm of
Ius Laboris Network of Labour Law Firms

Chronological Overview

- **2008 / 2009:** corporate spying scandals (Deutsche Bahn, Deutsche Telekom, LIDL, Schlecker, et.al.)
- **Sep 1, 2009:** the new Privacy Protection Law for Employees and the new § 32 BDSG are enacted
- **May 28, 2010:** the Minister of the Interior presents a new draft law
- **Aug 25, 2010:** the Federal Cabinett presents an amended draft law
- **Nov 25, 2010**: the Upper House (Bundesrat) debates the draft law
- **Dec 15, 2010:** the German Government presents a final draft
- **Feb 25, 2011:** the final draft is debated in Parliament and assigned to the Parliamentary Commission
- **Sep 2011:** the law was supposed to be enacted 6 months after passing Parliament in late March 2011.
- **End of 2011:** since debates are still going on, however, the law will probably not be enacted before the end 2011.

The new Data Protection Law - Content

- **General rule:** collection, process, and use of personal data must be necessary for performing employment relationship
- **Employer‘s right to ask questions**: the employer may only ask for the applicant‘s contact data and data that is necessary to decide whether an employment relationship shall be entered into.
- **Internet research (new):** personal data that is generally accessible may be collected, unless the data is from social network sites (e.g. facebook).

The new Data Protection Law - Content

- **Medical and other examinations**: only with the applicant's consent and only if necessary to decide whether specific job requirements are met.
- **Use of personal data**: to control an employee's behaviour and efficiency.
- **Video surveillance (new):** forbidden if done secretely or if it violates an employee's privacy; otherwise only if explicitely allowed by law.

The new Data Protection Law - Content

- **Use of positioning systems (new):** only in order to ensure employee‘s safety or for coordination reasons.
- **Use of biometry (new):** only for authorizational or identificational reasons if proportionate.
- **Preventing crimes** (new): employers may collect and synchronize data in order to automatic data synchronisation only in order to disclose or prevent crimes or serious breach of duty.

Data Protection in a Multinational Company

Melissa Lea
Chief Global Compliance Officer, SAP AG

ACC EUROPE
Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

SAP

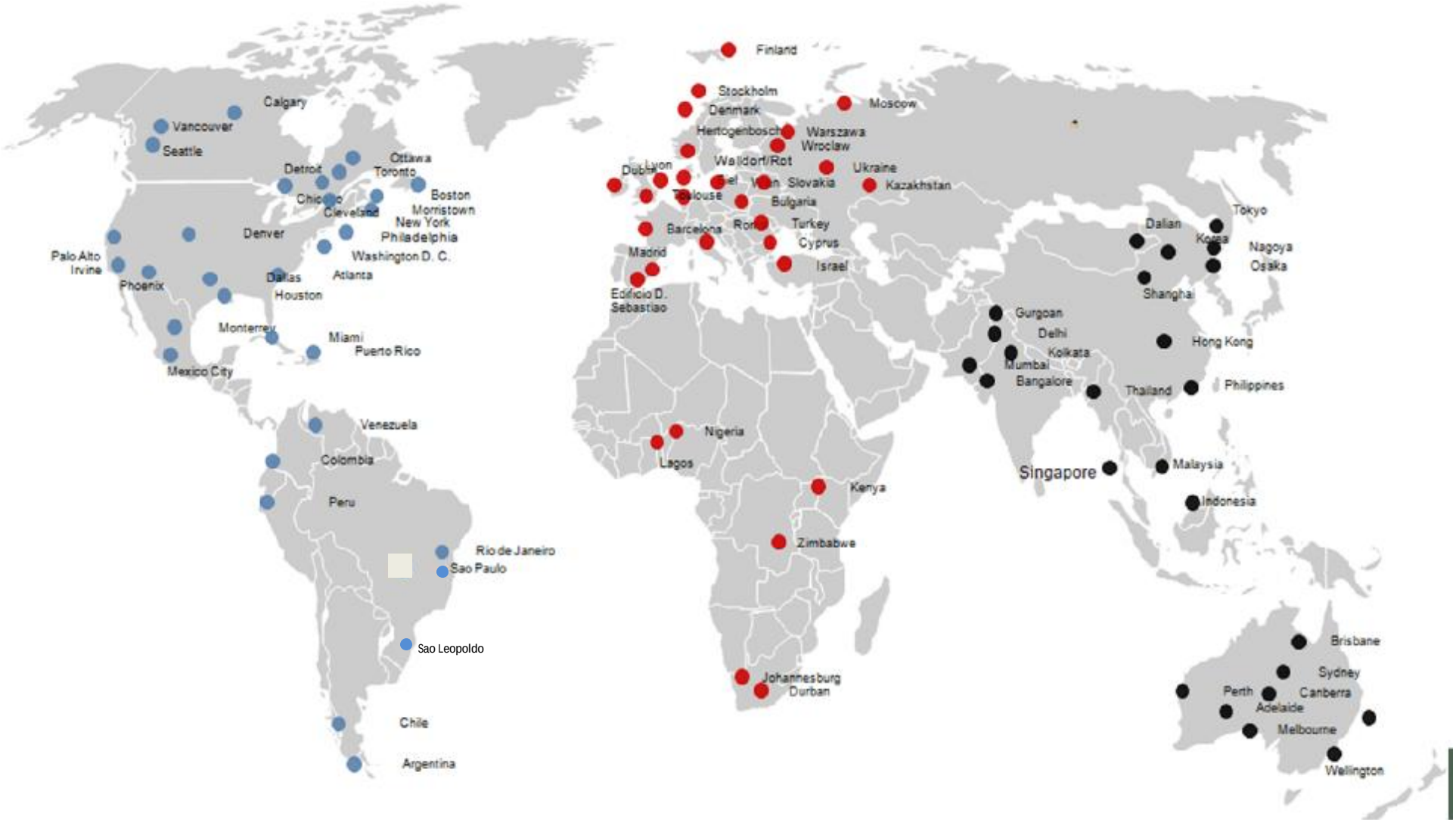
1972	Employees:	9	Customers:	5+
	Countries:	1	Countries:	1

ACC EUROPE
Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

SAP

2011	Employees:	50,000	Customers:	105,000+
	Countries:	60+	Countries:	120+



Case Study # 1a, Q1: Data Transfers

Company X is established in Germany and engages Company Y – based in the USA – for maintenance work on the company´s CRM-System. Since Company Y gets access to the CRM-System, hence access to personal customer data, Company X is interested to comply with data protection rules. They ask you for help.

- *Q1: Do you consider the transfer from X to Y to be a "controller to controller" or a "controller to processor" transfer? What is the difference between the two concepts, why is it important to assess and what are the key criteria to differentiate between a controller and a processor? Please discuss.*

Case Study # 1a, Q2: Data Transfers

- Data can only be transferred to a non EU/EEA country, if the recipient can provide for an adequate level of data protection (Directive 95/46/EC). Since Company Y did not join the Safe Harbor Framework, you decide to use the Standard Contractual Clauses approved by the EU Commission to comply with the obligation. There are different types of clauses:
  - Standard Contractual Clauses (controller to controller transfers) (Commission Decision of 27 December 2004 (2004/915/EC)
  - Standard Contractual Clauses for the transfer of personal data to third countries (Commission Decision of 15 June 2001 (2001/497/EC))
  - Standard Contractual Clauses (processors) (Commission Decision of 27 December 2001 (2002/16/EC)
  - Standard Contractual Clauses (processors) (Commission Decision of 5 February 2010 (2010/87/EU)
- *Q2: Based on the conclusion you made answering Q1 on the previous slide, what Clauses would you choose to use? Is it necessary that the competent Data Protection Authority gives authorization for the data transfer, if*
  - *Standard Contractual Clauses are used without changes?*
  - *the clauses of Different Standard Contractual Clauses are mixed in a contract?*
  - *the parties negotiate an individual contract that comprises some of the clauses approved by the EU Commission?*

Case Study # 1a, Q3: Data Transfers

- *Q3: Given the fact that Company Y is to be considered as a processor, is it necessary to conclude a separate controller to processor contract under the German Data Protection Act in addition to the agreement upon the Standard Contractual Clauses?*

Case Study # 1b: Data Transfers (Q1 and Q2)

Company X is established in Germany and engages Company Y, also based in Germany, for maintenance work on the company´s CRM-System. Company Y subcontracts its Sister Company Z, which is based in the USA.

- *Q1: Is it possible to use the new Standard Contractual Clauses 2010/87/EU as such when personal data is transferred from an EEA-based controller to an EEA-based processor and then to a Non-EEA-based subprocessor?*
- *Q2: If not, what different ways can you think of, to provide for legal grounds for the transfer? Is the authorisation of the competent Data Protection Authority mandatory in these cases? Please discuss.*

Case Study # 2 – Implementation of a HRIS (Human Resource Information System) With the Consent of the Works Council

Manufacturer of cars XY whose headquarter is located in Detroit, MI (USA). The US parent company is certified under the US-EU Safe Harbor Principles. The German operations are employing 1,200 employees in one large production site outside Frankfurt. They have elected a works council.

The International Legal Counsel, located in Detroit, announces that a worldwide HRIS (Human Resources Information System) will be implemented at the US headquarter. This system will include information about employees' performance as a basis for the bonus payment they may be receiving.

He sends over a spreadsheet with numerous data to be sent over regarding all German employees - by the end of the following week at the latest.

- **How do you proceed?** Discuss typically arising problems.
- **Time Management** – Create realistic expectations at the HQ. Share your experiences.
- **Legal Evaluation** – By In house or external counsel? Questions: Kinds of data to be transferred? Legal basis for transfer of data? Is single employee consent necessary in addition to a works council agreement? Do employees receive a written notice of transfer of their personal HR data into the US? Discuss your experience and opinions.
- **Negotiations With The Works Council** – with or without external counsel present during the negotiations? Should the works council be provided with as much or as little information as possible? Do you approach the works council with a written draft of a works council agreement, or rather informally with a call to the works council chairperson? What are your experiences regarding the timing of the negotiations? How to avoid having to go into legal proceedings (*Einigungsstelle*, re-conciliation board)? Discuss the pros and cons of the various approaches.
- **Further Issues** – Feedback to International HQ regarding necessary local differences and data that cannot be transferred (if any)? Issuing a notice to all employees regarding the transfer of their personal data to the US? Technical follow-up with the payroll provider if a monthly update of all data for the US is requested. Discuss typical problems.

Case Study # 3: Investigation into Suspected Individual Misconduct

- You work in the legal department for a Germany-based multinational company. The U.S. legal authorities contact your company's U.S. subsidiary and request information about suspected insider trading. They show you records to prove that one of your Germany-based employees purchased shares in one of the companies you recently acquired, and it appears he made the purchase right before the acquisition was announced. The employee is a member of your company's Mergers and Acquisitions team.
- You interview the employee. He tells you that he believes his trading activities are his private business. He will not answer to you or anyone at the company for his private business decisions. In the meantime, the US authorities request all of this employee's emails and other electronic data to aid in their investigation. The employee refuses to give consent.
- What do you do? Would your approach be different if the questions were raised by the French authorities, or the German authorities?

Advanced Case Study (Optional): Transfer Instrument or Mechanism

Your company (with domicile in Germany) is part of a group of affiliated companies which are partially third country-based. Each company is independent and equal-leveled with no corporation to a parental company. The group wants to build up a joint network with shared applications, administrations and databases. This includes controller-to-controller data flows as well as controller-to-processor data flows.

- *Q3: What data transfer instrument or mechanism would you recommend? Please discuss.*