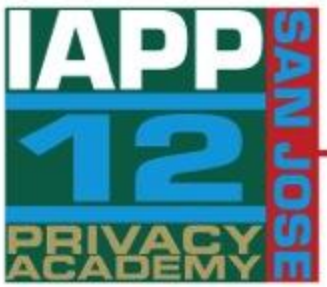
IAPP PRIVACY ACADEMY 2012

October 10-12
San Jose, CA

The HR Skinny:
Effectively managing international employee data flows



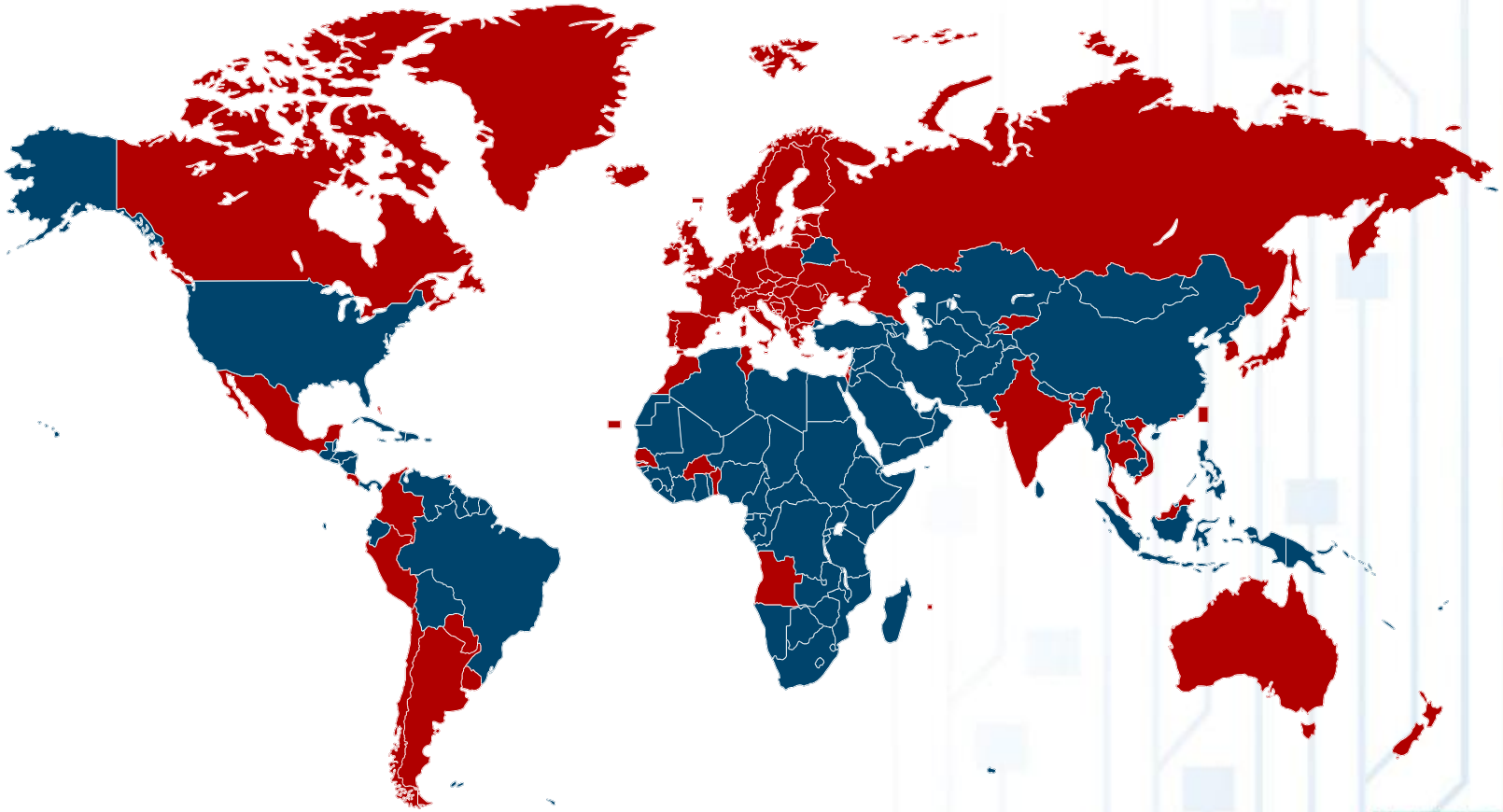
www.privacyassociation.org/academy

Topics we will cover today

- Laws affecting HR data flows
- HR international data protection challenges and strategic solutions
- Case study
- Key takeaways

Laws affecting HR data flows

Global privacy snapshot



IAPP 12 SAN JOSE PRIVACY ACADEMY

Key concepts and principles of EU data protection law

EU Data Protection law safeguards the right to privacy of **data subjects** with respect to the **processing** of their **personal data** by **data controllers**

Data subject	**Identified or identifiable natural person** to whom the personal data relates
Processing	Any operation or set of operations performed upon personal data, whether or not by automatic means
Personal data	Any information relating to a **data subject**
Data controllers	Any 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

Personal data must not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection

Consequences of non-compliance in the context of employee data

- Potential for criminal liability and unlimited fines
- Civil proceedings and damages
- Risk industrial relations problems
- Potential breach of individual employment contracts
- Adverse publicity/ reputational risk
- Impact on ability to recruit

US concerns over HR data flows

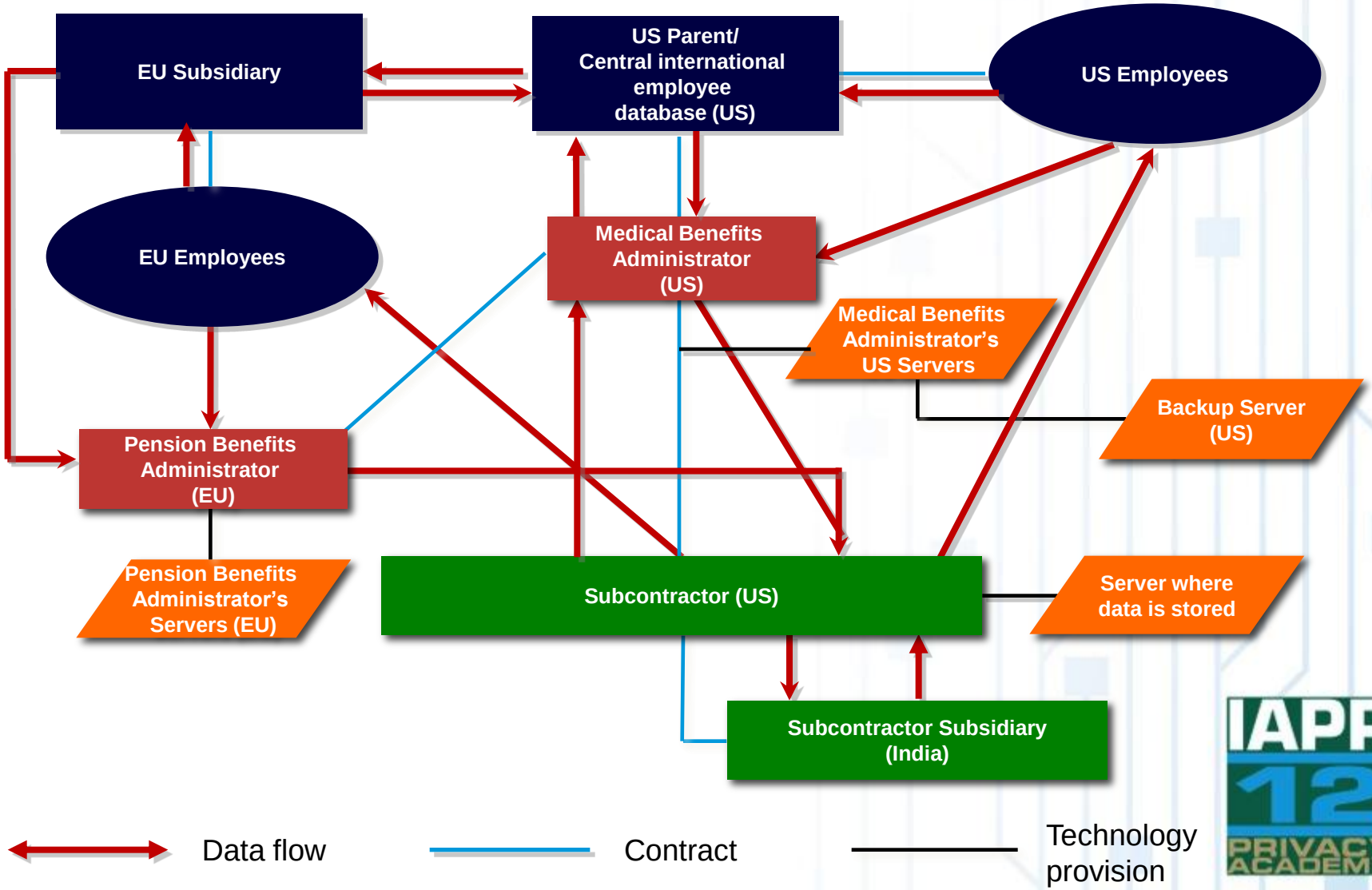
- US clients often restrict by contract the flow of personal information outside the US
- Concerns over access and control in outsourcing to other countries, specifically to India, which sometimes hampers use of less expensive outsourcing arrangements
- Only legal restrictions may lie in area of defence contracting – otherwise, generally over the issue of whether information is adequately secured under particular legal regimes (HIPAA, GLBA, etc.)

Elsewhere…

- Canada, Australia and elsewhere:
  - Patriot Act concerns continue to exist
  - Issues prompt contractual limitations on transfer of data to the US
  - Systems must be configured to ensure that access to data is not provided that is otherwise restricted or must be unavailable from the US

HR international data protection challenges and strategic solutions

Employee data flows can become complex and difficult to manage

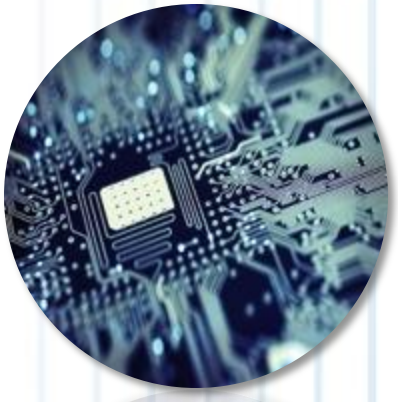


Data protection challenges fall into three broad categories

Legal

Administrative

Technical



IAPP 12 SAN JOSE PRIVACY ACADEMY

Legal solutions focus on either 'adequate protection' for personal data

Legal

- Potential routes to 'adequacy':
  - Member of the European Economic Area
  - European Commission finding of adequacy e.g. Canada
  - US safe harbor
  - Model contractual clauses
  - Binding corporate rules

…or identification of an exemption

Legal

- Possible exemptions:
  - 'Mere' transit en route to another EEA country
  - Consent of the data subject obtained
  - Transfer is **necessary**:
    - to perform a contract with data subject
    - to take steps, at data subject's request, with view to entering into contract with him
    - to conclude contract between data controller/data subject, entered into at request of data subject
    - in the interests of data subject
    - in connection with legal rights/public interest

Adequacy options: pros and cons

Legal

- Safe harbor:
  - Pros: automatic authorisation for signatories
  - Cons: only covers transfers to US and not applicable to all sectors
- EU model contractual clauses:
  - Pros: straightforward to implement
  - Cons: many sets required by multinationals
- Binding corporate rules:
  - Pros: effective solution for multi-nationals
  - Cons: cumbersome, expensive and time-consuming to implement

Outsourcing and sub-contracting HR data

Legal

- Companies are looking to shift the burden of responsibility concerning privacy
- BUT responsibility for privacy cannot be outsourced:
- If you permit the collection of information about individuals under your organization's name or authority, you cannot blame sub-contractors for their failure to adequately protect the privacy of individuals
- Organizations remain responsible for the information processed by third parties on their behalf
- Thinking about strategies to minimize the need to collect, send or disclose personal information to other parties, or anonymize the data will help reduce the pain of dealing with the security and privacy review
- Most important, use suppliers already approved for the purpose you require – minimize the number of suppliers we share information with, and simplify your life

IAPP 12 SAN JOSE PRIVACY ACADEMY

Administrative solutions focus on…

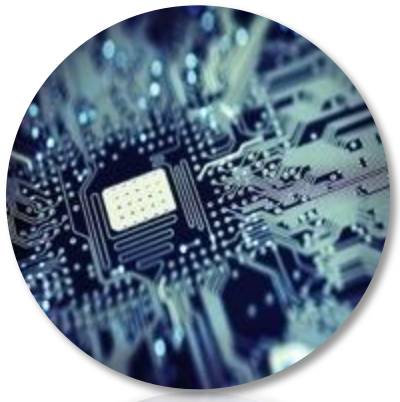
Administrative

- Training Human Resources:
  - to identify and transfer **only necessary personal data** at all times
  - when/where to obtain **employee consent**
  - to understand scope of existing employee consent and when to seek further consent
  - to **which jurisdictions** your organisation may transfer personal data
  - on **which database/server(s)** employees' personal data should be stored
  - to **implement processes** for regular audits and correction or deletion of employee data

IAPP 12 SAN JOSE PRIVACY ACADEMY

Technical solutions focus on…

Technical

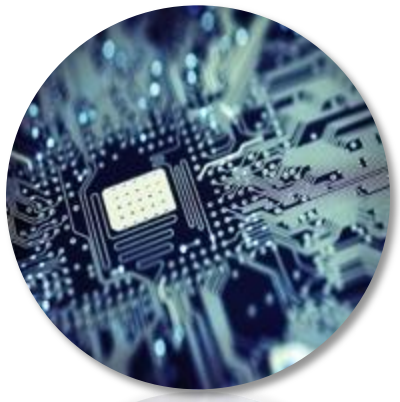


- Consideration of IT systems and architecture:
  - location of servers - can transfer be avoided?
  - implementation of systems that facilitate easy identification of **only relevant employee data**
- Removal of personal data:
  - by **data sanitization/obfuscation**
  - when is data reasonably anonymized or 'pseudonymous' in hands of third parties?

IAPP 12 SAN JOSE PRIVACY ACADEMY

International IT issues in HR Privacy

Technical

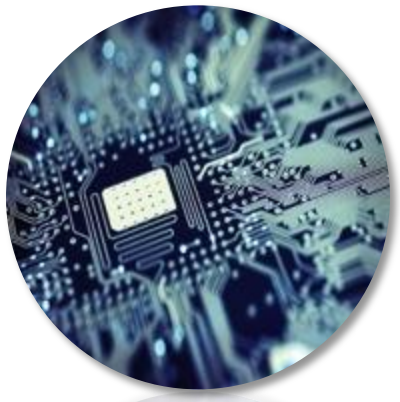


- Information is mobile:
  - Employees may be able to see data on systems located in other countries, and in general employees are often able to see far more than they 'need'
  - Important information systems are often in the US, or are backed-up in the US (disaster recovery sites, for example)
  - A lot of information is 'portable' – contained on laptops, USB devices or PDAs used by executives, sales and field technicians who move around the country and cross the border every day
- Conflicting and 'combining' application of laws and standards:
  - Breach notification laws
  - Differences in approaches to consent, notice

IAPP 12 SAN JOSE PRIVACY ACADEMY

Complications of the cloud/centralization of employee data

Technical

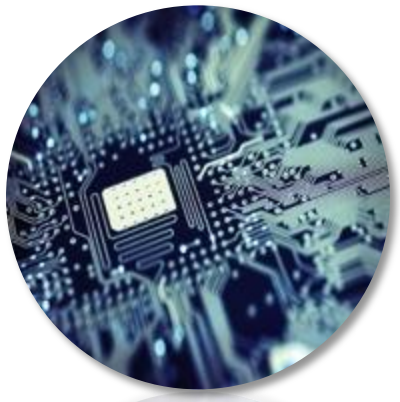


- Certain types of data may trigger specific obligations under national or local law
- Clients will face issues with putting HR data into the cloud:
  - Organizations may be unaware they are even using cloud-based vendors
  - Due diligence still required as in any vendor relationship
  - Data security is still the responsibility of the customer organization
  - Service level agreements need to account for access, correction and privacy rights
- Data Transfer:
  - Cloud models may trigger international legal data transfer requirements
  - Contractual or legal prohibitions on transfer may be unknowingly violated

IAPP 12 SAN JOSE PRIVACY ACADEMY

BYOD: Bring your own device

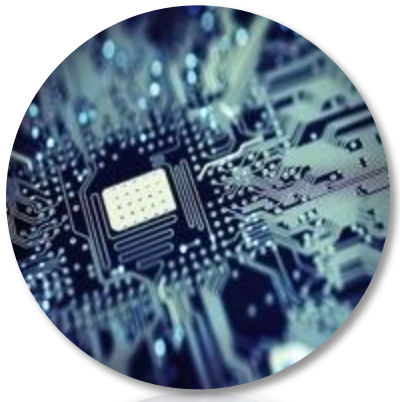
Technical



- Personal Data of employees is at risk on BYO devices managed by the organization and create issues over where data is flowing, and how it is protected
- In the excitement to use iPads, it must be remembered that this must be dealt with just as any other data flow

Privacy risk assessment and data flow mapping

Technical



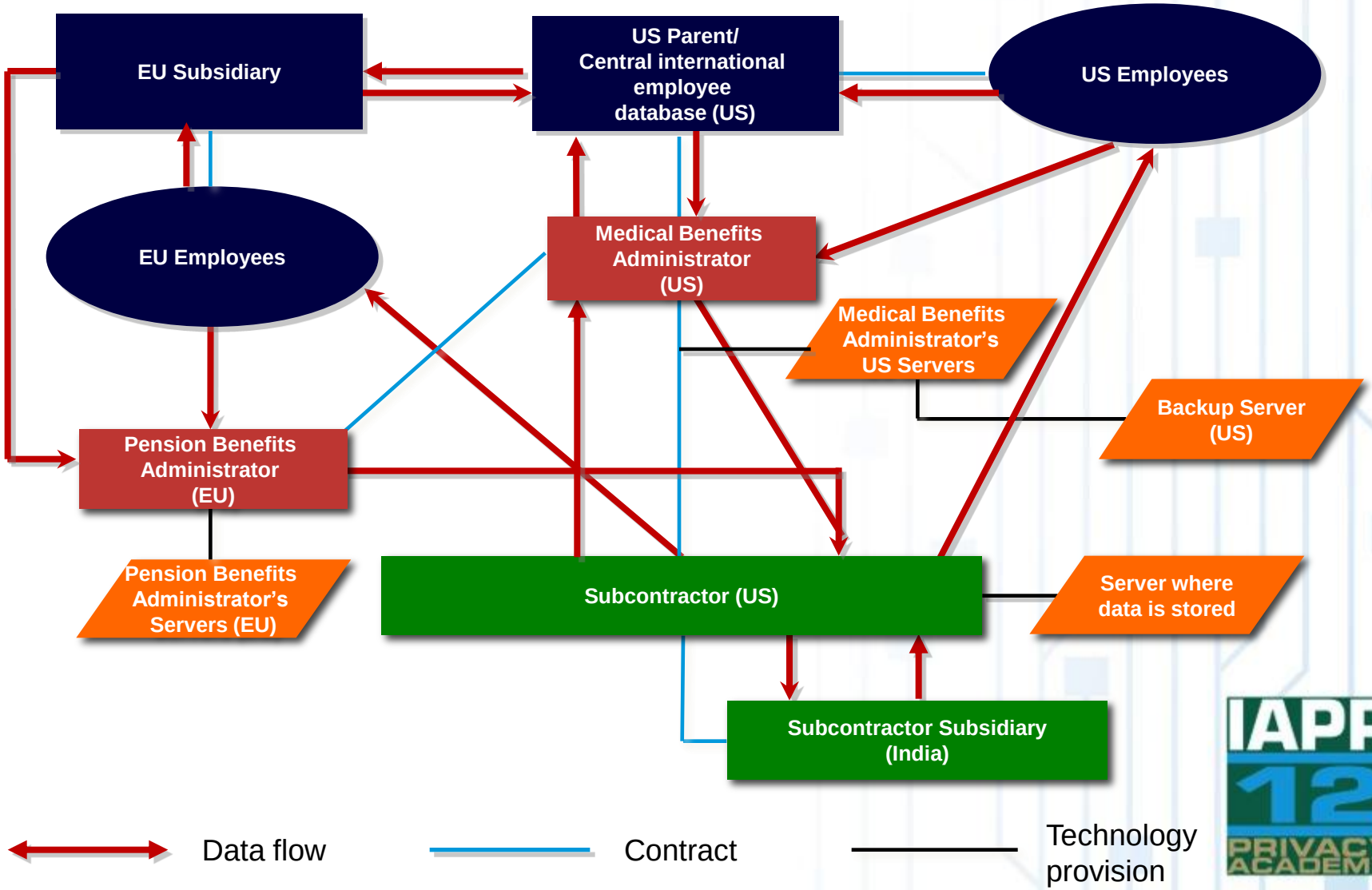
- A privacy risk assessment (PRA) is a best practice, designed to identify and document risks at each stage of a project or initiative affecting personal data
- All of these must be linked to legitimate business purpose
- Residual risk must be accepted by someone having authority to do so
- Data Flow Diagram or Table
  - Identifies how HR data flows through a system
  - Keep in mind this can mean different channels – web, phone, mail
  - Should identify mechanisms for protecting the personal data
  - Should identify what personal data is going through the system
- Different from a regular 'IT' data flow:
  - Focus is on what personal data is flowing through which jurisdictions, and which entities have control

Case study

Location and transfer of employee data

- US parent company has EU subsidiary
- Both use a central international employee database located in the US
- US database includes personal data about employees' medical benefits claims history: sent to US benefits administrator
- Pension benefits provided for EU employees by EU subsidiary of benefits administrator: data sent from EU subsidiary to EU pensions administrator
- Data sent from US medical and EU pension benefits administrators to shared US subcontractor
- US subcontractor sends data to its Indian subsidiary

Examination of HR international data flows



What is the best strategic solution for the group?

- Conduct privacy risk assessment that involves:
  - Data flow mapping
  - Identification of optimal combination of legal, administrative and technical solutions
  - Relevant factors will include:
    - personal data itself
    - scope for relocation of databases/servers e.g. to UK or Canada
    - potential for obfuscation of personal data
    - involvement of third parties (e.g. outsourced services)
    - budget
    - timetable

Key takeaways

- Not ‘one size fits all’
- Combination of solutions:
  - Legal: adequate protection vs exemption
  - Administration: implementation of legal strategy
  - Technical: geographic location of IT systems and potential data minimisation
  - Implications of cloud computing
- Importance of privacy risk assessment and understanding the flow of data across borders and through entities

Speakers

Heather Sussman,
Partner

McDermott Will & Emery LLP

Constantine Karbaliotis,
Americas Privacy Leader

Mercer

Sharon Tan,
Partner

McDermott Will & Emery UK LLP

IAPP SAN JOSE 12 PRIVACY ACADEMY

Appendix

Legislation Overview

Region	Regulations
Europe	▪ Privacy Directive ▪ Rules over 'export' of personal data
Asia-Pacific	▪ APEC Privacy Framework ▪ National privacy laws (such as in Japan, Australia, New Zealand)
Canada	▪ Federal (PIPEDA) private sector privacy legislation ▪ Some provincial regulations (British Columbia, Alberta, Quebec, Ontario in health)

US	▪ HIPAA/HITECH in place to govern use of health-related PI
	▪ Federal Trade Commission (FTC) has responsibility under other legislation to protect consumer privacy:
	  ▪ FTC Act – to enforce privacy statements under the unfairness and deceptive practices provisions
	  ▪ Gramm-Leach-Bliley Act -- FTC enforces rules concerning financial privacy notices and safeguarding of personal information
	  ▪ Fair Credit Reporting Act – governs credit reporting practices
	  ▪ Children's Online Privacy Protection Act – providing parental control over collection of children's information
	▪ Safe Harbor provides mechanism for bringing PI from Europe to comply with EU Directive
	▪ 45 US states have enacted privacy legislation to require notice of privacy breaches

EU data protection principles

1. Process personal data **fairly and lawfully**
2. Collect personal data only for **specified, explicit and legitimate purposes** and not further process such data in any manner incompatible with those purposes
3. Collect and store personal data only to the extent that is **adequate, relevant and not excessive** in relation to the purposes for which it is collected and processed
4. Ensure that all personal data held is **accurate** and, where necessary, kept up to date
5. Do not keep personal data in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the data was collected or for which it is processed
6. Process personal data only in accordance with the rights of data subjects
7. Implement **appropriate technical and organizational security measures** to protect personal data against unauthorized or unlawful process and accidental loss, destruction or damage
8. **Do not transfer personal data outside the European Economic Area unless the recipient country ensures an adequate level of protection**