

## Navigating the International Data Protection Maze

**Peggy Eisenhauer**  
Privacy & Information  
Management Services

### ● ● ● | About this Course

Four session program designed to:

- Introduce international data protection concepts
- Explore international regulation of employee background screening
- Consider application of the rules on US screening companies
- Offer compliance solutions and practical advice



## What It's Not

- Comprehensive information on all international laws that affect background screening
- Replacement for tailored legal advice
- Guaranteed to be accurate tomorrow

Disclaimer: Ms. Eisenhauer is admitted to practice law in Georgia USA. She is not authorized to practice law in any other country. The information contained in this course has been prepared for informational purposes only and is not legal advice. Participation in this program is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send us any confidential information.



*session one*

## Data Protection Basics



## The Business Reality

- Economic situation means less hiring, and a need to find the most capable, productive workers – yet candidates everywhere are more desperate for jobs
- Difficult and expensive to terminate workers outside the U.S.
- Foreign workers can create liability in the U.S.
- Global background screening provides path to reduce risk
- Complexity of laws and customs makes using a screening provider desirable



## The Legal Reality

- International privacy laws are inherently hostile to data collection and data processing
- Local laws in each country establish different requirements, with no harmonization in sight
- Data transfer restrictions make it difficult to export data across national borders
- Processors cannot make decisions without consent of the data owners
- Civil and criminal penalties may apply

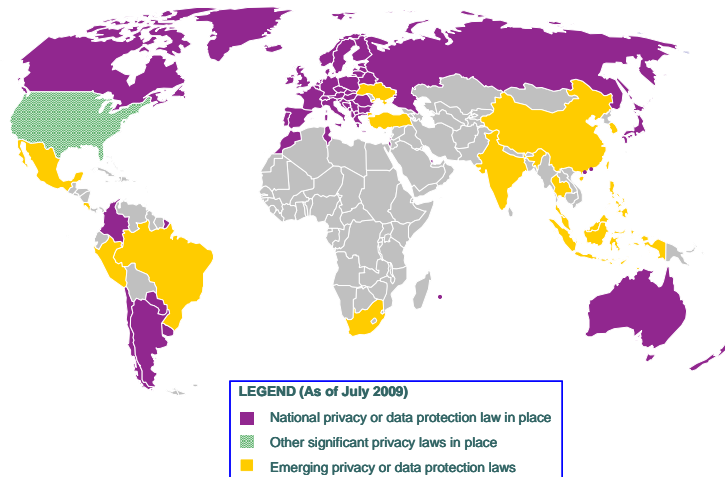


## Geography Matters

- The US has very complex privacy laws, but Europe and other international jurisdictions have very different – though equally complex – regimes
  - Comprehensive data protection laws
  - Independent privacy regulators
  - Works Councils and representative bodies
- Liability considerations make it difficult to use the same compliance processes in both the US and other countries



## A Global Perspective is Needed





## A Modern History of Privacy

- Throughout the 20th Century, government abuses sparked concerns in Europe and the US
  - Privacy and data protection were primarily concerned with protecting individuals from government surveillance and databases
  - Private databases regulated due to concern that the government could compel disclosure
- Early European laws and the US Privacy Act established in the mid-1970s



## A Modern History of Privacy

- 1980 OECD Principles laid foundation for broader or more consistent privacy legislation
  - Member countries have a common interest in reconciling fundamental but competing values such as privacy and the free flow of information
  - Avoid obstacles to trans-border data flows
  - Principles apply to public and private sector
- Direct marketing, telemarketing, and other annoyance issues rose in the 1980s and 1990s
- Identity theft became a significant driver at the turn of the century



## OECD Guidelines

In 1980, these principles were adopted by the Organization for Economic Cooperation and Development (OECD) in its “Guidelines for the Protection of Personal Data and Trans-border Data Flows.”

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability



## OECD Principles

- **Collection Limitation Principle**

Personal data should be collected for legitimate purposes, by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject

- **Data Quality Principle**

Personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete and current



## OECD Principles

- **Purpose Specification Principle**

The purposes for which personal data are collected should be specified at the time of collection, and use limited to the fulfillment of those purposes and other compatible purposes

- **Use Limitation Principle**

Personal data should not be used or disclosed for any purpose other than the original one without the consent of the individual or the authority of law



## OECD Principles

- **Security Safeguards Principle**

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure

- **Openness Principle**

Practices and policies with respect to personal data should be transparent. Means should be readily available of to establish the existence and nature of data processing as well as the identity and usual residence of the data controller



## OECD Principles

- **Individual Participation Principle**

An individual should have the right to know if a controller has information relating to him, and to have access to such data. An individual also should have the right to have his data corrected, amended or erased

- **Accountability Principle**

Data controllers should be accountable for complying with measures which give effect to the principles



## Europe at a Glance





## EU Data Protection Countries

Austria	Latvia	Plus EEA Members
Belgium	Lithuania	• Iceland
Bulgaria	Luxembourg	• Lichtenstein
Cyprus	Malta	• Norway
Czech Republic	Netherlands	<b>Switzerland is <u>not</u></b>
Denmark	Poland	<b>part of the EU or the</b>
Estonia	Portugal	<b>EEA but its law is</b>
Finland	Romania	<b>recognized as</b>
France	Slovakia	<b>adequate and it also</b>
Germany	Slovenia	<b>recognizes the US-</b>
Greece	Spain	<b>EU Safe Harbor</b>
Hungary	Sweden	<b>program through a</b>
Ireland	United Kingdom	<b>separate treaty with</b>
Italy		<b>the US</b>



## Different Paths

- European law is based on the protection of fundamental human rights
- US law is based on checks and balances
- Four cornerstones to the US approach
  - Freedom of expression
  - Robust public record
  - Private sharing of data
  - No tolerance of information misuse
- However, there is a common root – a fear of government misuse of personal data



## Different Results

- US system: government use of data is restricted, private use is okay unless harmful or covered by sector specific law
- European system: no one can collect or use data unless permitted by law



## EU Legal Regime

- E.U. Data Protection Directive 95/46/EC, supplemented by other Directives:
  - E-Privacy Directive, 2002/58/EC
  - E-Commerce Directive, 2000/31/EC
  - Distance Contracts Directive, 97/7/EC
- Specific national laws on data protection, consumer protection, employment and general civil law
- Guidance from the Article 29 Working Party
- Guidance from national data protection authorities



## EU Legal Regime

- Enacted in 1995, effective 1998
- Each country has its own national data protection law – EU Directive sets the floor
- Laws establish obligations of “data controllers”
- Laws prohibit transfers of data to other jurisdictions unless “adequate level of protection” is guaranteed or another exception applies
- US is not adequate, but enforcement was limited until 2001
- Enforcement today is very aggressive, large fines and disruptions of data flows



## Controllers and Processors

- **Controller**

A data controller determines the purposes and means of the processing of personal information

- **Processor**

A data processor processes personal data on behalf of the controller

- Every instance of processing of personal information has at a least one controller
- All controllers also process data
- Processors rely on instructions from the controller
- Controllers and processors have different obligations over the personal information



## Data Protection Authorities

- DPAs are independent supervisory authorities chartered to enforce data protection laws
- In the EU, the Article 29 Working Party contains a representative of each national DPA
  - Publishes guidance about how to interpret and implement the Directive
  - Gives the EU Commission its opinions on the level of protection in third countries
  - Advises the Commission on proposed amendments to the Directive and additional measures needed to safeguard the rights and freedoms of natural persons



## Personal Data: The E.U. Definition

- “Personal data” means any and all information relating to an identified or identifiable natural person (“data subject”)
- An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- Does not distinguish “consumer data” from “professional” or “business” data – even my title and address at work are covered



## Processing

Processing means any and all operations taken on personal data, including the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, disclosure by transmission, dissemination or making available in any other form, linking, alignment or combination, blocking, erasure or destruction of personal information



## Sensitive Personal Information

- Sensitive data elements are subject to additional privacy laws, but the data elements that are classified as “sensitive” vary from country to country
- In the US, Social Security numbers and financial information are considered highly-sensitive
- In EU, “*special categories of data*” refers to sensitive personal characteristics, such as race, sexual orientation, labor union membership and criminal history
- Health information is considered sensitive everywhere



## Special Categories of Data

- Special Categories of Data may only be processed if the data subject has given explicit consent *or* the processing is specifically allowed by law
- Special categories of sensitive personal data include: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, and data relating to offenses, or criminal convictions



## Consent

- For consent to be real, it must be “freely-given” and “unambiguous” – but there is no consensus on these definitions
- Individuals must also be able to withhold (or revoke) consent, with no adverse consequences
- In an employment context, consent is almost never considered freely-given, due to the subordinate nature of workers to employers
- Therefore you can only process Special Categories of Data if the law specifically permits the processing



## Other Controller Obligations

- Register data processing activities with the DPA
- Notify works councils of HR data processing
- Ensure that data collection is fair and lawful
- Comply with purpose & use limitations, retain personal data only as long as needed for the original purpose
- Maintain appropriate security, manage processors
- Respect individual rights of access, correction, blocking
- Export data to other countries only if authorization for the transfer exists



## Database Registration

- Prior to undertaking any processing, data controllers must notify the DPA and provide a description of the processing that can be included in the public registry
- Registration must include details of transfers outside the EEA
- DPAs audit companies against the registrations



## Privacy Notices

- Data controllers must provide all the information needed for the data subject to make informed decisions regarding the processing
  - The purposes of the processing
  - The recipients or categories of recipients of the personal data
  - Rights of choice, access, correction
  - How to exercise rights
  - Countries of transfer (if outside the EU/EEA)
  - Any additional relevant information



## Data Subject Access

- Access by individuals to personal information held about them is an almost absolute human right
- Right extends to “corporate” records, such as potential ratings, reviews, *etc.* although companies may redact information as needed to protect the privacy rights of the sources
- Access rights are critical to supporting other data subject rights, such as objection, correction and blocking



## Purpose & Use Limitation

- Personal data may only be used for the purpose specified in the privacy notice, other “compatible” purposes, and as required by law
- Data may not be retained longer than as needed for the purpose specified
- All secondary uses/disclosures require additional notice and consent
  - Data subjects have the right to block all secondary uses/disclosures



## Information Security

- Controllers must implement reasonable technical and organizational security measures to protect the confidentiality and integrity of personal data
- Controllers must also oversee data processors
  - DPs must be reputable and have the ability to provide adequate security for the personal data
  - Data controllers must enter into a written agreement with every data processor that safeguards the data protection principles
- Many DPAs have issued specific security rules



## Data Integrity, Proportionality

- Data controllers may only process personal data if it is adequate, relevant, and not excessive
- Data must be of appropriate quality – accurate, complete and current
- All data collection and processing must be proportional – if you only need name/address, you may not ask for birth date and national ID number



## Data Transfers

- “Transfer” means the physical movement of personal data to a recipient outside the country
- “Transfer” also means the communication of personal data to such a recipient via (e.g.,) remote access
- Controllers may freely transfer personal data to other controllers and processors within the EU/EEA and to countries whose privacy laws have been declared adequate
  - Switzerland, Canada, Argentina



## Data Transfers

- Controllers may transfer personal data using an approved mechanism
  - To a recipient in the US that is in the Safe Harbor
  - To any recipient, pursuant to a Model Contract
  - Using approved Binding Corporate Rules
  - With the unambiguous consent of the data subject
  - Upon authorization of the applicable DPA
  - Using one of the narrow derogations
    - Necessary for performance of a contract
    - Defense of legal claims
    - Vital interest of data subject



## Data Transfers

- Data processors cannot transfer personal data unless instructed to by a controller – the controller authorizes the transfer and takes other steps necessary (such as revising the privacy notice, amending its DPA registration, etc.)
- Data processors cannot make any decisions about the methods or location of the processing – only controllers can make these decisions!



## Safe Harbor Basics

- US Department of Commerce created a series of documents that describe privacy principles similar to those in the Directive
- EU agreed that companies that self-certify that they are following principles are in an adequate safe harbor
- FTC agreed that not following a self-certified standard is unfair and subject to enforcement



## Safe Harbor Steps

- Implement privacy program and maintain documentation
- Public annual self-certification via US Dept. of Commerce website
- Subject to enforcement FTC, DOT or other approved statutory body – EU authorities retain jurisdiction over HR data
- Commerce publishes lists of self-certified and non-compliant organizations



## Model Contracts

- Controllers can provide for adequate protection by executing contracts containing certain safeguards
- Model contract language was approved by the European Commission for controller-to-controller and controller-to-processor transfers
- DPAs approval is automatic if the model contract form is used
- Model form can likely be modified somewhat, as long as basic provisions remain intact



## Model Contracts

- Data exporters and importers provide notice, access, choice, etc. – all as defined by local law
- Both data exporter and data importer are liable to the data subject for illegal data flows
- Enforcement in the EU, by applicable national authorities
- Issues related to onward transfer exist if the importer shares data with others that are not parties to the contract
- Data subject consent is still required for transfers of sensitive data



## Binding Corporate Rules

- Controller corporate family implements internal privacy program across EU and non-EU affiliates
- Program contains appropriate protections for data subjects and other required controls
- One “lead” DPA blesses the program and seeks approval from other applicable DPAs
- Holy Grail for internal company transfers, but lengthy approval process means that companies must use model contracts or Safe Harbor during the approval process



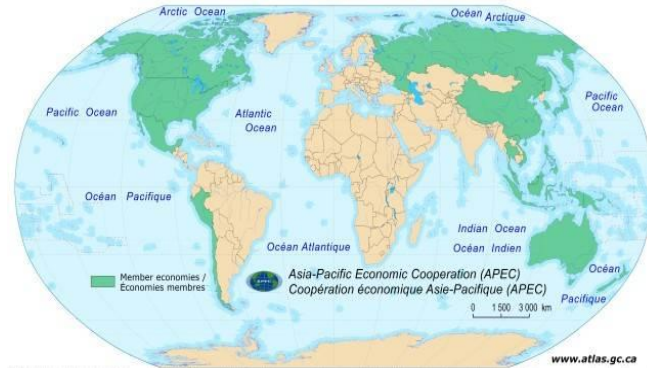
## Outside of Europe

- Many countries have enacted comprehensive laws: Paraguay, Argentina, Peru, Chile, Hong Kong, Australia, New Zealand, Tunisia, Russia, Japan...
- Most of these laws are based on the OECD principles and the EU Directive, but not all data protection laws are “adequate” to the EU authorities
- Canada’s law is adequate, as are the laws in Argentina and Switzerland
- APEC provides an alternative OECD-based model



## APEC: 21 Member Economies

The word 'economies' is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities.



## APEC Member Economies

Australia	Japan	Singapore
Brunei	Republic of Korea	Chinese Taipei
Canada	Malaysia	Thailand
Chile	Mexico	United States
People's Republic of China	New Zealand	Viet Nam
Hong Kong, China	Papua New Guinea	
Indonesia	Peru	
	Philippines	
	Russia	



# APEC



The APEC Privacy Framework is intended to encourage the development of appropriate information privacy legislation and to ensure the free flow of information in the Asia-Pacific region.

## **APEC Privacy Principles**

- Preventing harm
- Notice
- Collection limitation
- Uses of personal information
- Choice
- Integrity of personal information
- Security safeguards
- Access and correction
- Accountability

47



# Key APEC Concepts

- Goal is to balance the benefits to individuals and societies from data flows with the needs to protect privacy
- Legislation and enforcement should focus on harmful uses of information
- Controller accountability enables global data flows
- Proportionality limits some personal rights (e.g., access, accuracy) – even security obligations should be proportional to the sensitivity of the data



## APEC Cross-Border Rules

- Cross-border privacy rules envision matching corporate policies against APEC Principles
- Companies commit to honoring obligations of local laws
- Functionally similar to EU BCRs
  - Company procedures demonstrate capacity to honor rules
  - Procedures are reviewed and recognized by an accountability agent
  - Complaints handled by agent and/or government agencies

49



## Session1 Conclusions

- OECD Principles set basis for international data protection laws
- Data protection laws establish standards of “fair” and “proportional” data processing
- Notice and consent provide backbone for individual rights
- Purpose and use limitations must be strictly respected
- Privacy concerns trump business desire for robust use of personal data

