Morgan Lewis

GETTING THE DEAL THROUGH

A Road Map for Employer Data Privacy Issues

Presented by:
Mark Zelek, Partner, Miami
Nicholas Thomas, Partner, London
Bela Pelman, Of Counsel, Moscow
Felipe Alice, Associate, Houston

April 18, 2013

European Data Privacy – The Landscape

- European Data Protection Directive 1995
  - Minimum standards that apply across EU
  - Planned overhaul
- Implemented by local legislation in each member state
  - For example, UK Data Protection Act 1998
  - Member states free to provide enhanced protection
  - Laws therefore differ from jurisdiction to jurisdiction
- Enforcement by local Information Commissioner

Enforcement Powers of Information Commissioners

- Wide ranging investigatory powers including right to inspect or seize data and/or devices, enter property, and demand oral/written explanations from data controller
- Financial penalties to reflect severity of breach
  - E.g. France (€1,500,000); Italy (€300,000); Germany (€300,000); Netherlands (€78,000); Poland (€26,000); Spain (€600,000); UK (£500,000)
- Criminal offense in some countries punishable by fine and/or imprisonment
  - E.g. France up to five years, Germany up to two years, Netherlands up to six months
- Injunctions/court orders to prevent processing in question

Which Organizations Are Covered by EU Data Protection Law?

- Organizations established in the EU that process personal data in the context of the activities of that establishment
- Organizations not established in the EU but in a place where an EU member state's national law applies by virtue of international public law, e.g., foreign embassies
- Organizations not established in the EU but that make use of equipment (automated or otherwise) situated within the EU, unless the data is in mere transit through the EU

The Basics – Key Terms

- Data controller
  - Decides how the data is processed
- Data processor
  - Processes the data for a data controller
- Processing
  - Obtaining, retaining, using, and accessing
  - Employees, ex-employees, candidates, and secondees

The Basics – Key Terms (Cont.)

- Personal data
  - Processed electronically or in a “relevant filing system”
  - Employees’ names, addresses, and bank details
- Sensitive personal data
  - Employees’ ethnic origin, religion, health, or sexual life
- Relevant filing system
  - Information relating to individual is readily accessible
  - In practice, most HR files and email in/outboxes will be covered

Processing and Record-Keeping Requirements

- Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Using and Storing Employees' Personal Data – Best Practices

- Personal data statement in contract and/or handbook
- Regularly request information on changes to personal data, e.g., home addresses
- Keep data secure
  - Hard-copy data: locked filing cabinets
  - Electronic data: password protected
  - Ensure limited access to authorized persons
  - Make authorized persons aware of data protection obligations
- Sickness records will be "sensitive personal data"
  - Consider storing differently or restricting access to records

Record-Keeping During and After Employment

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
  - Six years after employment ends for employees
  - Six months after rejection for unsuccessful candidates
- Other legislation may require different, shorter time periods
  - Working Time Regulations 1998, applicable tax legislation
- Records must be permanently destroyed or deleted
  - Put beyond use

Monitoring at Work

- Monitoring
  - Emails and Internet use
  - Telephone calls
  - CCTV
- Occasional monitoring
  - Address a particular problem/concern
- Systematic monitoring
  - Routine monitoring of all employees/category of employees

Monitoring – Best Practices

- Carry out an impact assessment
  - Is monitoring justified?
  - Purpose of the monitoring
  - Likely benefits
  - Likely adverse effects
  - Alternatives
- Key policies should refer to possibility of monitoring
- Tell employees unless covert monitoring can be justified
- Restrict access to monitored information to authorized employees only

Data Subject Access Requests

- Tactical tool used against employers prior to litigation
- Written request by employee
- Payment of appropriate fee (currently £10 in UK)
- Response within relatively short time frame
- The employer must inform the employee whether his/her personal data is being processed
- If so, the employer must:
  - Provide a description of the personal data, the purposes for which it is processed, and to whom the data has been or may be disclosed
  - Supply the personal data to the employee in an “intelligible form”

Transfer of Data to Outside EEA

- Rights of data subject must be “adequately protected”
- Employee appraisal data, location of email server, cross-border litigation, etc.
- EU Commission findings of adequacy
  - Australia, Switzerland, Canada, Argentina, Guernsey, Isle of Man, Andorra, Jersey, New Zealand, Uruguay, Faroe Islands, and Israel (more limited)
- Safe harbor agreement for U.S. companies
- Data transfer agreement incorporating European standard contractual clauses
- Binding corporate rules
- Exceptions

Proposal to Overhaul European Data Protection Law

- January 2012: Proposal for new General Data Protection Regulation
- Harmonize European data protection law
- New law will address issues from new technology
  - Cloud computing
- Draft regulation must be approved
- Further two years to implement new law

Proposals

- New definition of consent
  - Explicit consent
- Right to be forgotten
- High fines for noncompliance
  - Up to €1 million or 2% of annual worldwide turnover
- Designated data protection officers
- Concerns with lack of uniformity on employee issues
- EPP amendments – exclusion of all employee data???

Russian Data Privacy Laws – General Overview

- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (28 January 1981)
- Federal Law on Personal Data (Personal Data Law)
- Chapter 14 of the Labour Code
- Resolutions of Russian Government
- Decrees of Roskomnadzor (Data Protection Authority), Federal Service for Export and Technological Control (FSTEK), and Federal Security Service (FSS)

Processing – Key Rules

- No employer can process any personal data of any employee
  - Other than upon consent from the employee; or
  - If one of the exemptions set out in the Personal Data Law applies (e.g., to protect life and health)
- No employer can transfer any personal data of any employee to any third party
  - Other than upon consent from the employee; or
  - If a federal law stipulates otherwise

General – Liability

- Civil
  - Compensation for losses and damages (including moral damage)
- Administrative
  - Currently, fines up to 10K rubles per breach
  - In the future, possibly, fines up to 500K rubles per breach and turnover fines of 0.5% – 2% of the total income
- Criminal
  - Fines up to 300K rubles per breach
  - Corrective services/work
  - Imprisonment up to four years

Personal Data Types

- General
  - Name, passport details, profession, education, etc.
  - Any data other than sensitive, criminal record, or biometrical
- Sensitive
  - Health, religious and philosophical beliefs, political opinions, sexual orientation, race and nationality, and criminal record
- Criminal record (“super” sensitive)
- Biometrical
  - Fingerprints, iris images
  - Arguably, certain types of photographic images (photos)

Types of Processing

- Depending upon the type of personal data, different rules apply to
  - "General" processing (i.e., by the employer itself)
  - Transfers to third parties (including parent company, lawyers, forensic auditors, IT providers)
  - Cross-border transfers
    - *Safe countries: 64 countries including Canada, Germany, Poland, and the UK*
    - *Non-safe countries: all other including the United States, China, and Japan*

Types of Consent

- Depending upon the type of data and processing, different consents apply
  - Consent
    - *No prescribed content/form*
    - *Could be in electronic form*
  - Special written consent
    - *Must refer to goals, ways, and conditions of data processing*
    - *Must list names and addresses of all third parties*
    - *Must be "blue ink" or equivalent*

Different Categories of Personal Data – Different Consents

- General Personal Data
  - Consent for general processing, transfer to third party, transfer to safe country
  - Special consent for transfer to non-safe country
  - Certain exemptions apply
- Sensitive Personal Data/Biometrical Personal Data
  - Special consent for general processing, transfer to third party, any cross-border transfer
  - Specific or limited exemptions apply

Practical Solutions – Be Prepared!

- General obligation to keep personal data confidential and secure
- Obtaining consents at the time of employment
  - Employment agreement
  - Policies (make sure that the polices are made formal in Russia)
  - Stand-alone document
- Establishment of information technology (IT) system for protection (including use of Russian IT services certified by FSTEK and/or FSS)
- Notification of Roskomnadzor for personal data processing (unless processing is subject to an exception)

Mexican Data Privacy Law – General Overview

- Personal Data Protection Law (the “Federal Law”)
  - Enacted on July 5, 2010 and entered into force on July 6, 2010
- Personal Data Protection Rules
  - ARCO Rights:
    - *Access*
    - *Rectification*
    - *Cancellation*
    - *Opposition*

Mexico – Federal Law Highlights

- Scope of Federal Law
- Data Protection Authority – Institute for Access to Information and Data Protection
- Penalties for Violation
  - Warning
  - Fine (up to ~$736,300)
  - Additional Fine (up to ~$1.4 Million)
  - Fines in Double

Mexico – General Issues

- Notice and Consent
  - Types of Consent
  - Instances Where Consent Is Not Required
- Security and Breach Notices
- Transfers of Data
- Impact on U.S. Companies

Colombian Data Privacy Laws – General Overview

- Colombian Constitution
  - Constitutional Writ of Protection
- Law 1266/2008
  - Prior Consent Requirement for Transfer
  - Exceptions
- Law 1581/2012
  - Implementation of Constitutional Right to Know
- Law 527/1999
  - Electronic Marketing

Colombia – Data Privacy Issues

- Data Protection Authority
- Notice and Consent
- Data Retention
- Data Security
- Access to Personal Data
- Cross-Border Transfer of Data
- Penalties

Brazilian Data Privacy Laws – General Overview

- No Comprehensive Data Privacy Law
- Data Privacy Rights Scattered in Different Laws
  - Article 5 of Brazilian 1988 Federal Constitution
  - Rights of Minors
  - Wiretapping
  - Telecommunications
  - Habeas Data
  - Financial Data
  - Brazilian Civil Code

Peruvian Data Privacy Laws – General Overview

- Personal Data Protection Law
  - Data Protection Authority
    - *National Authority for Protection of Personal Data*
  - Rights
  - Penalties
  - National Register of Personal Data Protection
  - Cross-Border Transfer of Data

Peru – Data Privacy Issues

- Notice and Consent
- Data Retention
- Data Security
- Access to Personal Data
- Correction Rights

Questions?

Nick Thomas
Partner
London
+44 (0) 20 3201 5561
nthomas@morganlewis.com

Bela Pelman
Of Counsel
Moscow
+7 495 212 2528
bpelman@morganlewis.com

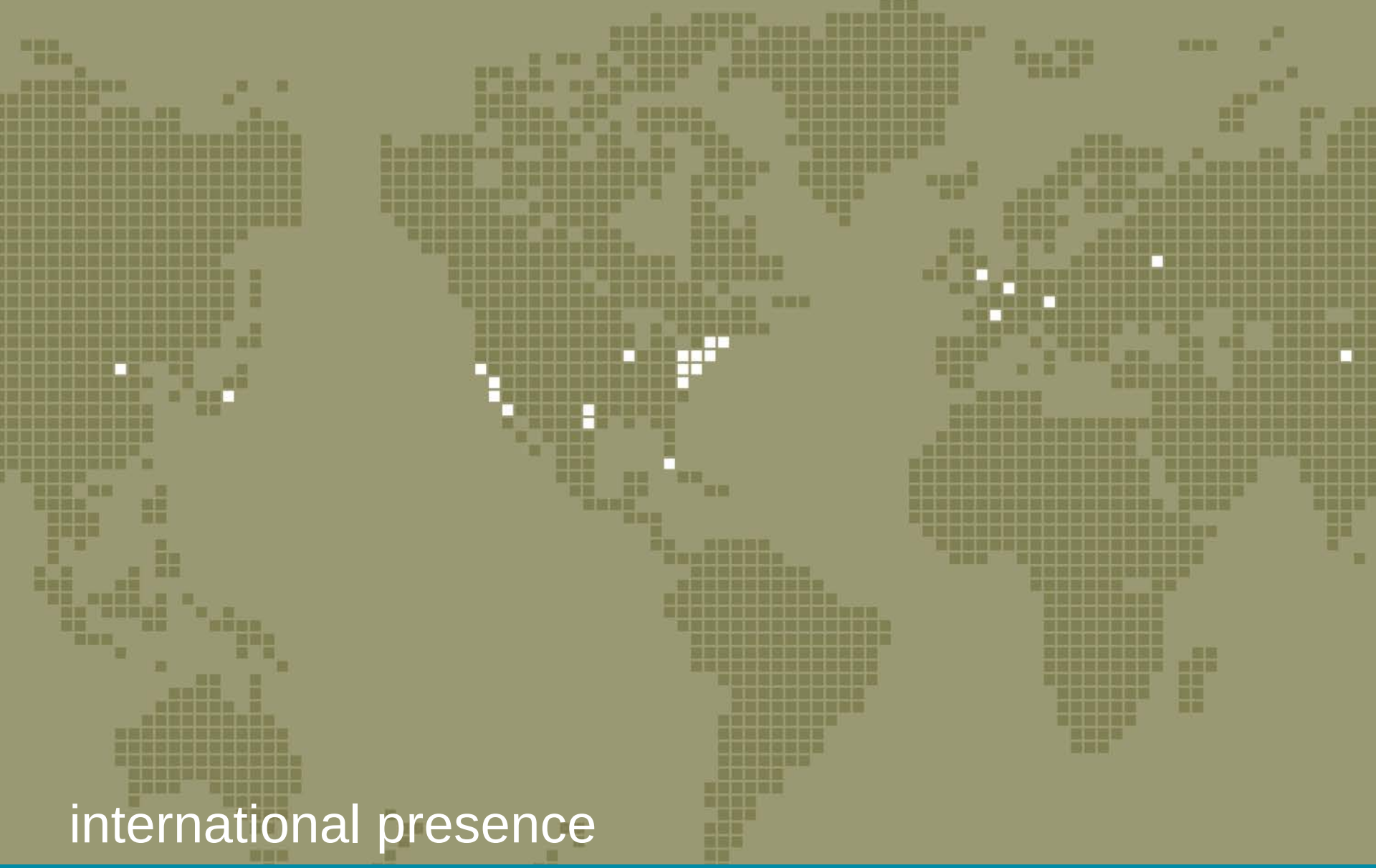
Felipe Alice
Associate
Houston
713.890.5763
falice@morganlewis.com

Morgan Lewis

DISCLAIMER

- This material is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered Attorney Advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change.

- **IRS Circular 230 Disclosure**
  To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein. For information about why we are required to include this legend, please see http://www.morganlewis.com/circular230.



international presence

Almaty Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston Irvine London Los Angeles Miami Moscow New York Palo Alto Paris Philadelphia Pittsburgh Princeton San Francisco Tokyo Washington Wilmington