

Morgan Lewis



Managing the Global Workforce

Webinar Series 2014



Implementing Workplace Policies Across Multiple Jurisdictions

June 12, 2014

Today's Presenters



Mark Zelek
Miami



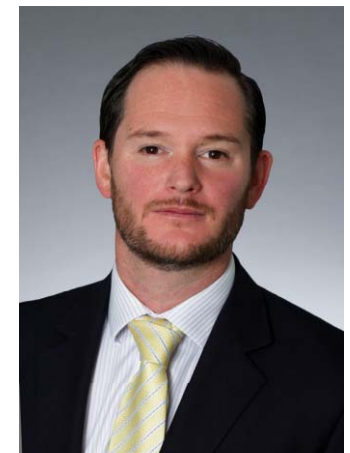
Motoi Fujii
Tokyo



Bela Pelman
Moscow



Melissa Rodriguez
New York



Nick Thomas
London

Overview

- Why have a global policy?
- Challenges of implementing a global policy
- What sort of policies should be “global”?
- Practical tips
- Case study
 - Puerto Rico
 - Japan
 - Russia
 - UK

Why have a global policy?

- Promote and protect an organisation's culture
- Enshrine key values
- Promote and protect an organisation's internal and external brand image
- Regulate employee behaviours across all parts of the business
- Ensure administrative simplicity/efficiency
- Ensure consistency
 - Standards of employee conduct and performance
 - Employee management
 - Appraisals and employee rewards

Challenges of implementing a global policy

- Diverse local custom and practice
 - “That’s not the way we do it here”
 - Entrenched behaviours
- Local laws
 - Minimum rights, e.g. working hours, rest break, holiday
 - Differences in anti-discrimination legislation
 - Data privacy
 - Compulsory procedures
- Employee engagement
 - Works councils
 - Trade unions

Challenges of implementing a global policy (cont.)

- Local culture
 - Workplace
 - Regional/national
 - Differences in “acceptable” behaviour
- Communication
 - Translation
 - Promotion
- Enforcement

What sort of polices should be “global”?

- Aspirational
 - Ethics
 - Equal opportunities/diversity
 - Bullying
 - Corporate responsibility
- Extra-territorial
 - Bribery and corruption
 - Regulatory
 - Data privacy
- International
 - Social media

Practical tips

- Proper planning essential
- Timing
 - Internal soundings
 - Local legal advice
 - Local consultation obligations
 - Translations
- Effective communication
 - Form of communication
 - Timing

Practical tips (cont.)

- Identify senior “responsible” individuals
 - Centrally
 - Locally
- Take local concerns seriously but do not accept “no” without exploring why
- Identify individuals to monitor impact and feedback
- Conduct regular reviews/updates

Case study

- D-BIT Inc. is a large company which manufactures and sells high-tech mining equipment
- From its small beginnings in Texas, D-BIT has expanded significantly and now has operations in the UK, Japan, Russia, and Puerto Rico
- Following a recent piece of unfortunate litigation that did not end well, D-BIT has decided to review some of its employment policies and procedures
- As a consequence of this review, the HR Director, based in Texas, has decided that the company needs to introduce new policies in respect of “Whistleblowing” and people using personal IT equipment on company business (a “Bring Your Own Device”/“BYOD” policy)

Case study (cont.)

- Under the Whistleblowing policy:
 - Any employee who has a concern regarding the conduct of any co-worker, including his or her own management, must report that concern to an internal “Complaints Ombudsman” (CO)
 - The CO, who is based in Texas, will then be responsible for investigating the complaint and concluding what further action, if any, should be taken
 - Only complaints that are made in accordance with the requirements of the policy will be investigated
 - To ensure that the policy is effective, the CO’s findings will be final and not subject to further challenge
 - The CO will also be given unlimited access to any information considered relevant to the investigation

Case study (cont.)

- Under the BYOD policy
 - Employees may use their own devices for company business
 - If requested, employees must immediately deliver up their devices for inspection
 - Employees must also download software onto their devices which allows D-BIT to access and/or monitor various activities
 - D-BIT reserves the right to delete the contents of an employee's device, either on the employee's leaving the company or at any other time "it deems appropriate for business reasons"

Implementing the policies in Puerto Rico

- Whistleblower Issues

- Puerto Rico is a commonwealth of the United States: U.S. federal laws apply in Puerto Rico
- Whistleblower laws
 - *Dodd-Frank Wall Street Reform Act (2010)*
 - *Sarbanes-Oxley Act (SOX) (2002)*
- Anti-retaliation provisions – employment and traditional labor laws
 - *See, e.g., FLSA § 215(a)(3)*
- False Claims Act/qui tam
- Other categories of federal law with whistleblower protections

Implementing the policies in Puerto Rico (cont.)

- Whistleblower Issues (cont.)
 - **Law 115: local anti-retaliation law (29 L.P.R.A. § 194a et seq.)**
 - *Employment protections for employees who “offer or attempt to offer, verbally or in writing, any testimony, expression or information before a legislative, administrative or judicial forum in Puerto Rico.” 29 L.P.R.A. § 194a(a).*
 - *Internal complaints?*
 - **Internal threats to offer information to legislative, administrative or judicial forum: “attempt to offer”?**

Implementing the policies in Puerto Rico (cont.)

- Whistleblower Issues (cont.)
 - **Law 80: Unjust Dismissal Act (29 L.P.R.A. § 185a-185m)**
 - *Requires “just cause” for termination*
 - **Law 426: Whistleblower Protection Act (10 L.P.R.A. § 601 et seq.)**
 - *Protects “the rights of public employees and officials who disclose information or testify on alleged improper or illegal acts regarding the use of public property or funds that due to their nature constitute acts of government corruption or fall within the ethical conduct regulated by our legal system.” 10 L.P.R.A. § 601.*

Implementing the policies in Puerto Rico (cont.)

- Whistleblower Issues (cont.)
 - Under Puerto Rico law, whistleblowers have significant incentives to report fraud to the government – but not necessarily to the company.
 - *Encourage* whistleblowers to raise compliance concerns internally.
 - But D-BIT should not limit the employees' right to report concerns externally
 - Investigations should not be limited only to concerns raised through the mechanisms in the D-BIT policy
 - *Ensure* impartial investigations.
 - *Correct* any problems in a timely manner to preserve the integrity of the company.
 - Employees can still go to government forum: D-BIT's CO's findings can be subject to further challenge

Implementing the policies in Puerto Rico (cont.)

- BYOD: Privacy Considerations
 - There is no general statute in Puerto Rico governing or addressing the issue of data protection and privacy.
 - Data protection and privacy matters in Puerto Rico are regulated by:
 - *Several U.S. federal statutes and regulations that apply in Puerto Rico to the same extent as in any state of the United States;*
 - *Provisions of the Constitution of the Commonwealth of Puerto Rico, as interpreted in various decisions of the Puerto Rico Supreme Court; and*
 - *Certain provisions of special laws and regulations.*

Implementing the policies in Puerto Rico (cont.)

- **BYOD: Privacy Considerations (cont.)**
 - **Computer Fraud and Abuse Act (CFAA).**
 - *Permits recovery of civil damages when unauthorized access results in damage exceeding \$5,000.*
 - *Employer could be subject to liability if employee did not provide prior authorization for deletion of personal items.*
 - **Stored Communications Act (SCA) – prohibits unauthorized access to email stored at an email service provider.**
 - *SCA may be implicated if employer views employee's personal email or personal data on employee devices.*
 - *Be careful when relying on verbal consent.*
 - **Employee may later claim he/she did not give consent or it was coerced.**

Implementing the policies in Puerto Rico (cont.)

- BYOD: Privacy Considerations: Case Law Under the SCA
 - *Issue:* Should D-BIT reserve the right to delete the contents of an employee's device, either on the employee leaving the company or at any other time "it deems appropriate for business reasons"?
 - *Require consent of employee to wipe data upon separation from company*
 - *Clearly define "appropriate for business reasons"*

Implementing the policies in Puerto Rico (cont.)

- **Data Privacy: Constitutional Protections**
 - The Puerto Rico Constitution protects the right to privacy.
 - Under the Puerto Rico Constitution, the right to privacy must be protected by state actors and also observed by private parties, including private employers.
 - The Puerto Rico Supreme Court has described the right to privacy as a “fundamental right” of the “highest hierarchy” and has stated on numerous occasions that, while the U.S. Constitution sets the minimum safeguards of fundamental rights that apply in Puerto Rico, the breadth of the Bill of Rights under the Puerto Rico Constitution is broader in scope than the Bill of Rights under the U.S. Constitution.

Implementing the policies in Puerto Rico (cont.)

- Data Privacy: Constitutional Protections (cont.)
 - Vega v. Telefónica, 156 D.P.R. 584, 600 (2002): Analyzes multiple factors to determine whether the employer's workplace video surveillance violated the employees' right to privacy
 - *Employer's reasons for the surveillance: (1) security; (2) avoiding sabotage or theft; (3) evaluating employee productivity; (4) evaluating customer service.*
 - *Evaluate: (1) how intrusive the surveillance method is vis-à-vis the employer's needs; (2) workplace characteristics (e.g., open space?); (3) duties of the employees at issue; (4) function of the facilities subject to surveillance; (5) surveillance equipment's capabilities; and (6) notice and use of the system.*

Implementing the policies in Puerto Rico (cont.)

- Data Privacy: Employment Law: Privacy Protections
 - Act No. 207 of September 27, 2006: Social Security numbers cannot be displayed on ID cards or any other document of general or routine circulation or be displayed in documents distributed to people without a legitimate need to access said numbers, except in certain limited circumstances.
 - Act No. 59 of August 8, 1997: requires that written notice of any drug-testing program and of any positive results be delivered personally to each employee. The information collected as a result of drug tests carried out pursuant to the program may not be disclosed by the employer to any third party.
 - Other employment law privacy protections.

Implementing the policies in Puerto Rico (cont.)

- Data Privacy: *Issues*
 - What is the purpose of D-BIT's BYOD policy?
 - Which employees would be covered?
 - What is subject to review and when?
 - Who has access?

Implementing the policies in Puerto Rico (cont.)

- BYOD
 - Ensure that BYOD policy provides clear notice as to purpose, scope, methodology, and use
 - *But limit ability to monitor, collect, or share personal data on devices*
 - *Provide training for IT and other employees with access to employees' personal devices*

Implementing the policies in Puerto Rico (cont.)

- BYOD (cont.)
 - Require each employee to provide affirmative consent to the BYOD policy, including consent to:
 - *Wipe data upon an employee's separation from D-BIT.*
 - *Collect data from any devices if that employee is subject to a legal hold.*
 - Maintain a record of that consent.

Implementing the policies in Japan

- Whistleblowing
 - The Whistleblower Protection Act came into effect in Japan in 2007.
 - This law protects whistleblowers by preventing dismissal and any unfavorable treatment.
 - Workers who are protected by this law must not have ulterior motives, such as obtaining financial gain or causing damages to others.
 - Reportable facts to be protected shall be those regarding any crime or violation of disposition by the government, provided in the acts listed in the appendix of the law.

Implementing the policies in Japan (cont.)

- Whistleblowing
 - A worker will be protected if he or she reports to
 1. **The compliance counter of the company** since the worker deems that reportable events have occurred.
 2. **The administrative organization** with the authority to impose some disposition or recommendation, since the worker has reasonable grounds to believe that the reportable events have occurred.
 3. **A third party to be considered necessary to prevent the occurrence of the reportable events** since, in addition to the reasonable grounds of the previous item,
 - The whistleblower will be dismissed,
 - The evidence will be concealed, or
 - The employer believes there is no justifiable reason for the whistleblowing, etc.

Implementing the policies in Japan (cont.)

- Policy regarding whistleblowers:
 - Each employer should have a whistleblower policy to make its employees understand the basic framework of the law.
 - The whistleblower policy must make clear the outline of operation of the compliance officer.
 - It is very important to have a compliance officer.
 - If there is no whistleblower report made to the compliance officer does not mean that the employer is “clean.”
 - Employers should make every effort to increase reports from employees, since an employer can find something critical that can/will have a huge negative impact on the company’s management.

Implementing the policies in Japan (cont.)

- Policy regarding BYOD
 - Many companies have an IT policy, including a BYOD policy.
 - Regarding data privacy, Japan has the Private Information Protection Act.
 - The law basically states that it is the employer's obligation
 - *to specify the purpose of the utilization of personal information;*
 - *not to handle the personal information beyond the scope necessary for the achievement of the purpose;*
 - *to specify the purpose of the utilization of personal information when acquiring the information; and*
 - *not to provide the personal information to a third party without obtaining the prior consent of the person.*

Implementing the policies in Japan (cont.)

- Policy regarding BYOD
 - Many companies have prohibited employees from having personal information on their computer because if an employee has his or her computer stolen and personal information becomes divulged, it will be treated as a serious social issue in the media.
 - Other points of the IT policy are:
 - *the company has a right to scrutinize any computer, including an employee's computer, to be used for the business of the company, without obtaining the employee's consent about the scrutiny;*
 - *to prohibit the taking of classified company secrets and any other relevant information regarding the company's business.*

Implementing the policies in Japan (cont.)

- **General**

- The policy (work rules, the rules of employment, employee handbook) is very important.
- If the work rules provide more favorable terms for employees than an employment agreement, then the terms of the employment agreement will be raised to the level of the work rules.
- The employer must obtain an opinion from the employee representative regarding the contents of the work rules and submit the opinion with the work rules to the Labor Standard Inspection Office.
- Even though the policy is not submitted to the office, the policy has legal binding effects if an employer makes it known to its employees — for example, by posting it on the intranet.

Implementing the policies in Japan (cont.)

- General
 - Basically, the employer can change the policy without its employees' consent.
 - But if the change has an adverse impact on employees, then the change must be reasonable in light of:
 - *the extent of the disadvantage for the employees;*
 - *the need for changing the working conditions;*
 - *the appropriateness of the contents of the changed policies;*
 - *the status of negotiations with a labor union or the employees; or*
 - *any other relevant circumstances.*

Implementing the policies in Russia: Whistleblowing

- No law in Russia directly addressing whistleblowing
- Effective as of January 1, 2013:
 - All Russian companies must develop and implement measures aimed at combating corruption
- The Ministry of Labor and Social Protection Guidelines of November 8, 2013
 - All employees must adhere to anti-bribery rules
 - Special focus on international conventions
 - Clear recognition of FCPA and UK Bribery Act

Implementing the policies in Russia: Whistleblowing (cont.)

- In order to make the policies of the parent company mandatory for the Russian company:
 - Must be made “internal policies” by the appropriate corporate action;
 - Have to be available in Russian and communicated to individuals (as evidenced by signed receipt of the relevant policies); and
 - Compliance with the policies must be made part of individual employment agreements.

Implementing the policies in Russia: Whistleblowing (cont.)

- Personal data issues
- Depend 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 others including the United States, China, and Japan*

Implementing the policies in Russia: Whistleblowing (cont.)

- Has the personal data been processed in compliance with the Russian law?
 - Purpose of the processing of the personal data
 - Only the employee may provide her/his personal data
 - Transfer of the personal data of an employee to a third party
- On what basis has the data been transferred to the US?
 - Employment agreement
 - Personal data policy
 - Consent (stand-alone document)

Implementing the policies in Russia: BYOD

- The Russian Constitution protects the right to privacy
- Privacy issues
 - Employer may have access only to business-related data or to personal data that employee granted its consent for processing
 - IT and other employees with access to employees' personal devices should obtain employees' consents
- Remote deletion of the contents of device
 - Employee's consent
 - Elaborate on grounds for remote deletion
- Compensation for employees for the use of personal equipment?

Implementing the policies in Russia

- General
 - Russian Labour Code
 - Federal Law on Personal Data (Personal Data Law)
 - Employer's own policies and regulations
- Policies should be in compliance with Russian labor laws
- Should not contain any provision that can be viewed as less favorable than the provisions set forth by labor laws

Implementing the policies in Russia (cont.)

- General – types of internal policies and regulations
 - “Staff schedule” (personnel chart)
 - Internal labor regulations
 - Regulations on payment of salaries and remuneration
 - Personal data protection policy
 - Vacation schedule
 - List of employees on flexible working hours
 - Log on training and education of the authorized persons
 - Regulation on labor safety service
 - Others

Implementing the policies in Russia (cont.)

- Recommendations
 - Make sure that all mandatory HR policies are in place
 - Global HR policies must be made “internal policies”
 - Appoint local HR manager
 - Monitor compliance

Implementing the policies in the UK

- Whistleblowing
 - Local whistleblowing legislation that differs from that in the United States
 - Complaints could amount to “grievances” under UK law, which trigger a two-stage process under the ACAS Code of Practice on Disciplinary and Grievances
 - Failure to follow code could create legal risk
 - How will investigation be managed?
 - *Potential transfer of personal data, including sensitive personal data, to the United States*
 - *Will policy permit delegation to local investigators?*
 - *How will confidentiality be preserved?*
 - 8-hour time difference – will UK employee ever be able to speak with Texas-based CO?

Implementing the policies in the UK (cont.)

- BYOD
 - Data privacy issues
 - *Access to personal non-business-related data*
 - *Monitoring of activities*
 - *Proportionality*
 - Deletion of memory – criminal damage?
 - UK more permissive than other EU countries
 - Express agreement required

Implementing the policies in the UK (cont.)

- General
 - Consultation requirements?
 - *EWC*
 - *Trade union*
 - Communication of policy
 - Training for local management/HR

Questions?

Mark Zelek

Morgan Lewis | Miami
mzelek@morganlewis.com
+1.305.415.3303

Motoi Fujii

TMI Associates | Tokyo
motoi_fujii@tmi.gr.jp
+81 03 6438 5511

Bela Pelman

Morgan Lewis | Moscow
bpelman@morganlewis.com
+7 495 212 2528

Melissa Rodriguez

Morgan Lewis | New York
mcrodriguez@morganlewis.com
+1.212.309.6394

Nick Thomas

Morgan Lewis | London
nthomas@morganlewis.com
+44 (0)20 3201 5561

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

© 2014 Morgan, Lewis & Bockius LLP. All Rights Reserved.



international presence

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