Top Compliance Threats in Europe:
Is your company aware and prepared?

Chad A. Fentress – *V.P. and Chief Ethics & Compliance Officer, Nokia Corporation*

Alisia Grenville -*Corporate V.P.and Chief Compliance Officer, ST Microelectronics, NV*

Nick Holland - *Partner, Field Fisher Waterhouse LLP*

Agenda

- Compliance Program
- Cross Border Investigations
- UK Bribery Act
- Trade Controls
- Privacy Compliance
- Training and Awareness

Compliance Program

1. Deciding on the Appropriate Organizational Structure

- Trend towards building or redesigning the compliance organization away from the General Counsel and having a direct and formalized oversight at Board level
- This reporting level of Board oversight is indicative of the growing autonomy and importance of the compliance and ethics function
- But, ultimately, you need to assess your company individually

2. Ask yourself the following questions:

- How do things get done in our company?
- Is the company centralized or decentralized?
- How do we communicate?
- Where are the power bases of the company? Is in product, region, function etc?
- What is the size of the company?
- What will be the budget and resources allotted to compliance & ethics
- How does the company want compliance to be positioned?

3. Model 1: Part of Risk Management

Key Attributes

- Compliance & Ethics reports to the CRO
- Compliance and Ethics is a component of the enterprise risk management function
- Frequent reporting & evaluation of exposure to regulatory risk, less formal focus on business ethics
- Business unit compliance directors directly oversee business unit compliance and ethics programs

Typical companies: companies in heavily regulated industries with considerable compliance requirements (i.e. banks, insurance companies)

Benefits:

- Strengthens C&E officer's ability to identify and quickly respond to emerging risks
- Compliance is integrated into the operational risk management process which allows for a better understanding of interrelationships between compliance risk and other business risks

4. Model 1:

- Direct reporting relationship with CRO facilitates better prevention and detection of compliance risks

Drawbacks:

- Lack of direct access to the CEO eclipses compliance and ethics priorities;
- Channeling compliance through the risk framework may crowd out focus on promoting awareness of business ethics

5. Model 2: Small, within Legal

Key Attributes:

- C&E officer reports to the GC
- C&E office part of the legal department with limited discretionary budget
- Business unit compliance and ethics liaisons provide interface with corporate compliance

Typical companies: companies with low degrees of regulatory intensity and compliance and ethics staff levels are typically low, i.e. technology, retail and manufacturing companies

6. Model 3: Direct reporting to the CEO

Key Attributes:

- CCO reports to the CEO
- Relatively large budget for ethics initiatives
- Business unit compliance directors oversee business unit compliance and ethics program

Typical Adopters: companies in heavily regulated industries, i.e. health care; also companies rebuilding after corporate governance crisis often use this model to create an independent compliance and ethics program with adequate authority and resources

Benefits:

- Elevated and independent position of compliance officer and resultant access to the CEO provides instant authority and stature to the compliance program
- Structure communicates to stakeholders that the company views compliance more than strictly as a minimum legal and regulatory requirement
- Direct relationship with business units facilitates compliance participation in business unit decision making process

Drawbacks: elevated position and large budget increases pressure to measure and communicate the effectiveness of the program

7. Components of Activist Compliance Program

1. Tone at the top
2. Standards and procedures
3. Anonymous reporting line
4. Incentives and discipline
5. Risk assessment
6. adequate resources
7. Board oversight
8. Compliance Training
9. Monitoring and Measurement

8. Components of the Compliance Program

- Tone at the top: senior management must demonstrate corporate commitment to ethical conduct and legal compliance
- Standards and Procedures: Company must have appropriate corporate standards & procedures designed to achieve compliance
- Anonymous reporting line: reasonable steps must be taken to publicize a system for employees to report misconduct without re

8. Components of the Compliance Program

- Incentives and discipline: must provide incentives to perform consistent with program & apply consistent disciplinary measures for misconduct (i.e. carrot & stick)
- Risk assessment: the organization needs to periodically assess the risk of misconduct and take appropriate steps to modify the program to reduce the risk of misconduct identified through the assessment
- Adequate Resources: compliance and ethics programs should be provided with adequate resources to accomplish program goals

8. Components of the Compliance Program

- Board oversight: board needs to be knowledgeable about the content and operation of the compliance program
- Compliance training: the company must take reasonable steps to communicate the program's standards and procedures to the Board. Employees, and agents through effective training programs
- Monitoring and measuring: program needs to be kept effective and regularly evaluated and revised as appropriate

9. An Integrated Program Framework

- And for it to work, you need an integrated program framework, consisting of:
- Enterprise-wide standards
- Consistent, interlinked processes and structures to coordinate activities
- Functional and operational – regional level accountability to ensure consistent implementation of compliance initiatives.

Cross Border Investigations

1. Key Issues

- Document Production/Review
- Privilege
- Local Resources
- Internal or External Investigators
- Disciplinary Action
- Forensic Analysis
- Employee Claims

2. Document Production/Review

- Your ability to gather evidence effectively and efficiency in an internal investigation varies by jurisdiction. Compare the U.S. with Germany.
- You must understand local laws that restrict access to electronic communication eg. *Lex Nokia.*
- Additionally consider:
  - Privacy laws
  - Individual rights
  - Works Councils

3. Cross Border Transfer of Data

- The European Union member states place substantial limits on transmitting personal data outside of Europe.
- These limits profound effects your ability to conduct effective cross-border internal investigations esp. where the information may need to go beyond Europe for consideration eg. US or other Privacy backwards countries.

- Keep in mind EU's restrictions apply to *intra-company data* transfers.

- There are exceptions, The EU's laws provide exceptions for when personal data may be transmitted outside of Europe to the U.S. or any other non-qualified country (consent, safe harbour, binding corporate rules etc.)

4. Blocking Statutes

- Mainly a US issue, some countries have enacted criminal prohibitions preventing export of certain documents.
- Even though aware of these criminal laws, some U.S. courts have required the production of such documents.
- Example: French law:

  Subject to treaties or international agreements and the laws and regulations in force, it is prohibited for any person to request, seek or disclose, in writing, orally or otherwise, economic, commercial, industrial, financial or technical documents or information leading to the constitution of evidence with a view to foreign judicial or administrative proceedings or in connection therewith.

5. Privilege

- Outside of the U.S. and a few other common law jurisdictions, generally unavailable to in-house counsel
- Consider
  - Use of local external counsel
  - Think through waiver in US or elsewhere as part of cooperation, how will that affect privilege analysis in the local country?
  - Local governments can gain access to confidential material provided to the US authorities through Mutual Legal Assistance Treaties.

6. Local Resources

- Can local internal resources effectively investigate the allegation i.e. too close to the target to be independent?
- Even if independent (legal or finance) should internal resources be put in the situation of investigating peers or key business i.e. Can the relationships survive an investigation?

7. Interviewing Local Witnesses

- The labor and employment laws may allow employees to refuse cooperate.
- Privacy laws may also excuse employees from submitting to questioning by counsel.
- Internal or local counsel can provide guidance on the jurisdiction's privacy, labor and employment laws.

8. Disciplinary Action

- Local law matters
- Disciplinary systems and procedures used “globally” may not be lawful in the local country or require employee representational agreement (works councils/unions/labour awards).
- Get local expert advice from your internal counsel or local experts.

9. Forensic Analysis

- Back to the data: where is it and what can you do legally or in accordance with employee agreements/rights?
- Internal or external resources?
- Example: 6 laptops, limited financial data 120K Euros.
- Keep in mind while the content of emails is important, relationship mapping can tell another story: *who and when and how often were people communicating?*

10. Employee Claims

- Employees terminated for misconduct often bring claims against the company for termination.
- Prepare in advance:
  - Ensure evidence is collected in a way that will allow use in subsequent litigation whether criminal or civil (fruits from a poison tree issues)
  - Prepare reports and memos anticipating that third parties, including the subjects, may have access to and use those reports.
- Don't let employee claims prevent appropriate action: sometimes its simply worth the cost to remove a bad actor from your workforce and pay the statutory damages.

UK Bribery Act

1. Overview

- Provisions of the Act
  - Section 1 – Giving or offering a bribe
  - Section 2 – Receiving or requesting a bribe
  - Section 6 – Bribery of a foreign public official
  - Section 7 – Corporate offence of failing to prevent bribery
- Government “adequate procedures” guidance
- Scope of the Act
- Enforcement trends

2. Section 1 - Bribing another person

- Where a person (P)
  - Offers, promises or gives a *financial or other advantage* to another person; and
- P intends the advantage
  - To induce a person to perform improperly a function or activity; or
  - To reward a person for the *improper performance of a function or activity*

3. Section 2 - Requesting or receiving a bribe

- Generally mirrors the 'Active Bribery' offence in section 1
- Where a person requests, agrees to receive or accepts a *financial or other advantage*…
- Linked to *improper performance* of a function or activity

Sections 1 and 2

- Financial or other advantage – question of fact
- "Function or activity"
  - Does not need to have a connection to the UK or be carried out in the UK
  - Includes activities of a public nature, connected with a business or performed on behalf of a body of persons
- What does "improper"/ "improperly" mean?
  - Person performing the function or activity is in breach of an expectation of good faith, impartiality or trust
  - Based on UK standards of expectation of performance

4. Section 6: Bribery of foreign public official

- A person is guilty of an offence if he offers promises or gives a financial advantage to a foreign public official with the *intention to influence* the official in his capacity as a foreign public official
- P must intend to obtain or retain business or an advantage in the conduct of business
- It is not an offence if the applicable law permits or requires the foreign official to be influenced by the payment or gift
- No carve out for facilitation payments

5. Section 7: the Corporate Offence

- A commercial organisation commits an offence if
  - Any person *performing services* for the commercial organisation pays a bribe, and
  - Intends that bribe to obtain/retain business advantage for that commercial organisation
- No corporate liability for receiving bribes
- Strict liability
- Jurisdiction
  - Extends to commercial organisations carrying on business in the UK
  - It does not matter where in the world the bribe took place
- Defence
  - To show that "adequate procedures" have been implemented to prevent bribery

6. Adequate procedures defence

- Government guidance identifies 6 principles:
  - Risk Assessment
  - Top level commitment
  - Due diligence
  - Policies & Procedures
  - Communication
  - Monitoring & review

6. Adequate procedures defence

"Adequate Procedures" Guidance: scope

- Connection with the UK

"Carries on a business, or part of a business in the UK"

- Degree of connection
- Stock exchange listing only
- No "carve out": Court will determine
- Subsidiaries and parents

6. Adequate procedures defence

"Adequate Procedures" Guidance: third parties "performing services"

- Employees, subsidiaries, agents
- Determined by "all the relevant circumstances"
- Employee presumption
- Degree of control
- Joint ventures
  - Contract
  - Ownership
- Distributors

6. Adequate procedures defence

"Adequate Procedures" Guidance: third parties intending to confer business advantage

- requires intention by third party to confer business advantage for the company
- Indirect insufficient: dividend, loan payments
- Direct benefit required: eg. linked to sales
- Unclear if benefit has to arise directly from the bribe

6. Adequate procedures defence

"Adequate Procedures" Guidance: Facilitation payments

- Small bribes paid to facilitate routine government action
  - eg. Customs clearance
- Not exempted (contrast US legislation)
- Duress
  - Life, limb or liberty
- Public interest
  - Joint guidance of SFO and DPP indicates that where self report, or procedures followed, prosecution less likely

6. Adequate procedures defence

"Adequate Procedures" Guidance: Gifts and Hospitality

- Hospitality unlikely to breach Act if it is:
  - Reasonable or proportionate
  - Has bona fide business purposes
  - Is not intended to influence performance of function
- Unduly lavish hospitality could give rise to inference of impropriety
  - Consider timing
  - Consider internal codes of conduct

6. Comparison of FCPA and UK Bribery Act

	FCPA	**UK Bribery Act**
Prohibits commercial bribery	No	Yes
Prohibits receipt of bribe	No	Yes
Prohibits facilitation payments	No	Yes
Imposes strict liability for failure to prevent bribery	No	Yes
Prison sentence per violation	5 Years	10 Years

7. Enforcement

Enforcement Trends

- Managed outcomes – quasi deferred prosecution agreements
- Finality elusive – multiple actions in multiple jurisdictions
- Exposure of shareholders – using Proceeds of Crime legislation
- Dawn raids – upheld by the courts

7. Enforcement

- Managed outcomes:
  - UK SFO encourages "self reporting", offering civil rather than criminal resolution
- Civil Recovery Order (CRO)
  - eg. *Balfour Beatty* and *Macmillan publishers* cases
- Quasi Deferred Prosecution Agreements
  - eg. penalty "agreed" with SFO in *Innospec* case
- Whistle-blowing:
  - UK SFO has launched confidential whistle-blowing hotline. Expectation that competitors will use.

7. Enforcement

Closure elusive

- *Innospec* case
  - Multiple regulators/prosecutors: quasi DPA with UK SFO, and DPA with US Department of Justice
  - Corporate then agent/directors:
    - Corporate plea agreement March 2010
    - Agent prosecuted in US December 2011
    - Directors being prosecuted in UK 2012
- *Johnson & Johnson* case
  - Director then corporate:
    - Director of subsidiary (dePuy) prosecuted April 2010
    - Company civil settlement with UK SFO, and fines paid to US SEC and the US Department of Justice

7. Enforcement

Shareholders

- Proceeds of Crime Act (part 5)
  - Power to pursue “criminal property”
- *Mabey & Johnson* case
  - 2009 criminal prosecution of company
  - 2011 former directors and sales managers convicted of corruption
  - 2012 parent company ordered to pay over part of dividends that arose from subsidiary securing contract by corruption

7. Enforcement

Dawn Raids

- *Alstom* case
  - March 2010 SFO dawn raids on business and residential addresses
  - 3 board members arrested
  - SFO press release resulting in wide reporting in the national and international press
- Judicial review
  - *Burgin v Commissioner of Police for the Metropolis*
  - SFO action upheld July 2011

8. Conclusions

- Bribery Act is far-reaching: includes liability for those "performing services" outside UK
- Enforcement is growing
- Implementation of "Adequate procedures" avoids potential liability for companies

Trade Controls

1. Dealing with Trade Controls

- Be proactive rather than reactive
  - Recently a board member asked me if the company has controls or a monitoring process to understand where our products ultimately end up?
  - Think about your organization's needs and how products and goods are moved from site to site or distributor to end customer
  - No that trade compliance is probably not part of the corporate ethics and compliance function

2. Import/Export Compliance Function

- What does it do?
  - Monitor changing regulations (10+2, CTPAT, AEO) and communicate necessary activities to internal stakeholders
  - Ensure processes and documentation are in place for import controls, export controls, DEA requirements, etc.
  - Monitor compliance through internal audits of internal business and external audits with key suppliers such as freight forwarders
  - Conduct/coordinate supply chain risk assessments and communicate mitigation strategies to relevant stakeholders
  - Maintain positive relationships with the government agencies such as Census, DEA, Customs, BIS
  - Interface with key suppliers such as freight forwarders and brokers
  - Work closely with internal functional expertise such as regional experts, HTS classifications, technology organization, legal, finance, corporate tax, business organizations to address trade and compliance issues

3. Building an Effective Export Compliance Program: The components

- Understand the (US) export regulatory framework
- Conduct an Export Compliance Risk Assessment
- Create an Export Compliance Policy and/or Manual
- Structure and Organize The Export Compliance Function
- Develop Export Compliance Operating Procedures
- Mitigate Third-Party Risk
- Automate Processes and Controls
- Create Training Awareness, and Assessment Programs
- Manage Documentation and Recordkeeping

4. Structure of Import/Export Compliance Function

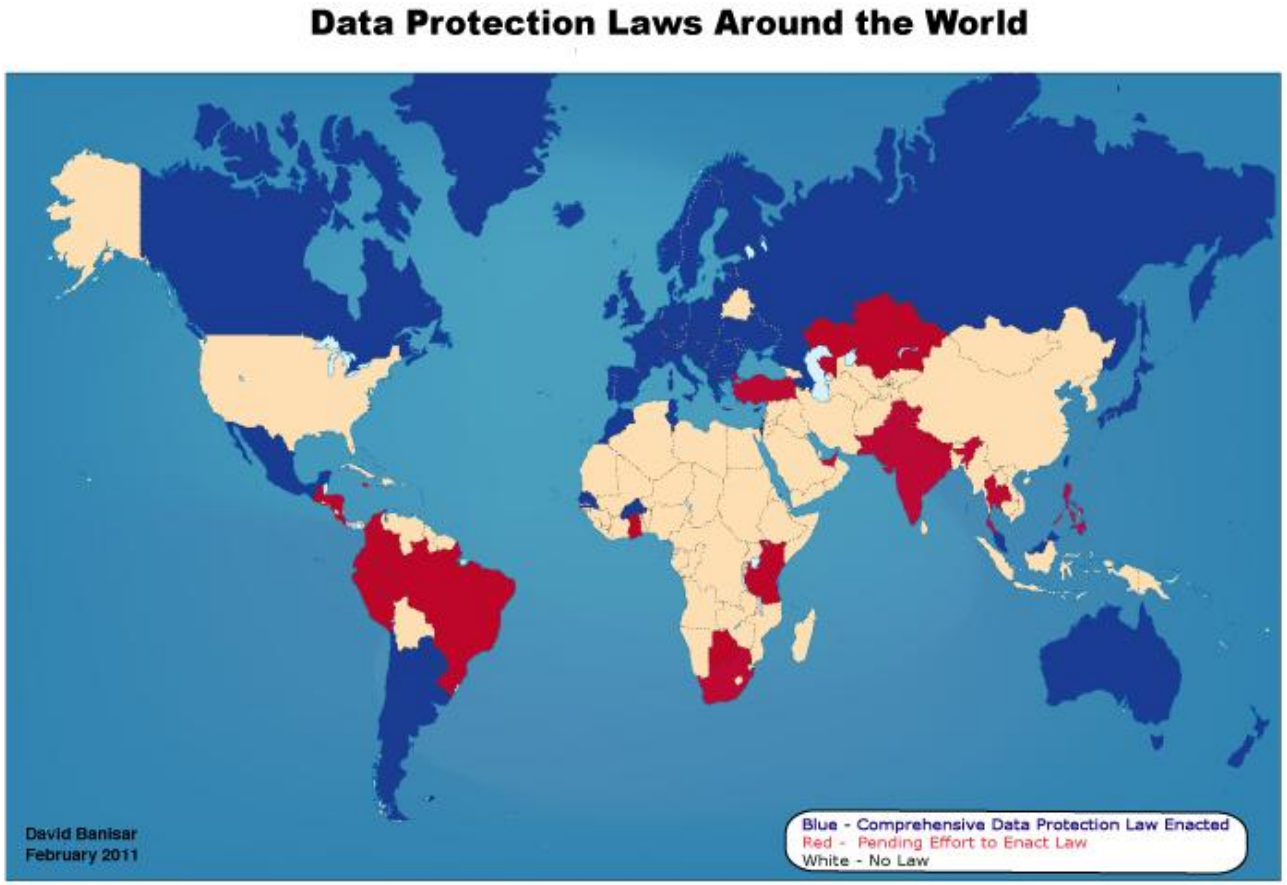
- Centralized import/export compliance functions improve strategic alignment, standardization of processes and lower total costs.
  - However, this structure can also diminish local relationships and expertise
- Decentralized import/export compliance functions improve focus on regional and national requirements
  - Decentralized structures can benefit from centralized governance for common import/export activities such as product coding
  - Decentralized organizations often face slower policy implementation, lack of clear accountabilities and uncoordinated communication channels

Privacy Compliance

1. Data Privacy – A Significant Concern Globally

- Privacy laws in many countries and regions give individuals rights designed to protect their personal data
- The EU and its members states have the most comprehensive privacy regimes and set the global standard but other countries and regions (in particular Asia Pac) are catching up and this is a global issue as a result.

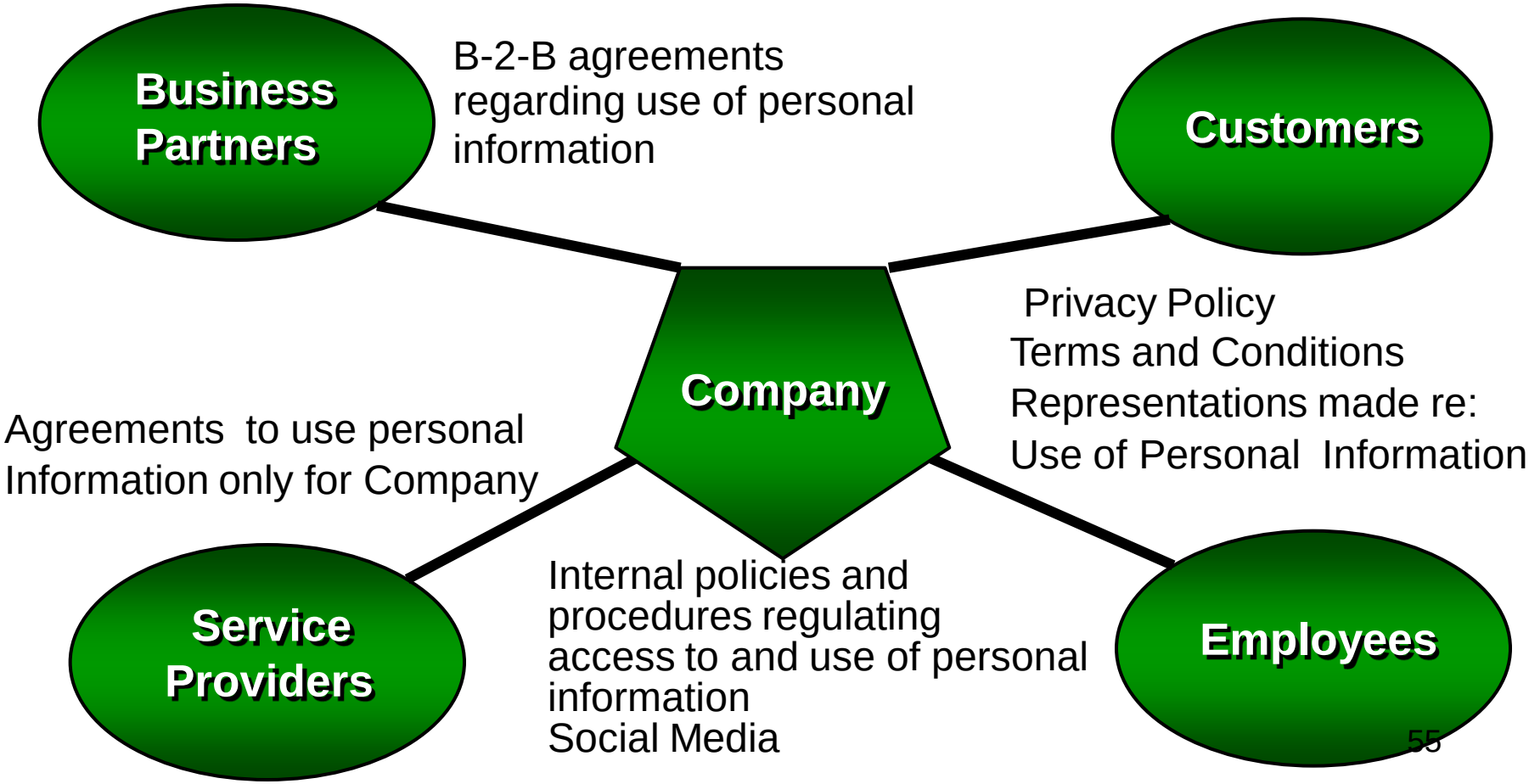
1. Data Privacy – A Significant Concern Globally



1. Data Privacy – A Significant Concern Globally

- US (takes a more sector-specific approach)
  - HIPAA – Health data
  - Gramm – Leach – Bliley – Financial Services data
  - Dodd-Frank Whistleblowing Rules
  - Various state-level data breach notification laws
  - US Privacy Act 1974
- Canada: PIPEDA – Federal law
- India – new law of April 13, 2011 – The Information Technology Rules 2011
- New Laws also in India, Peru and Korea in 2011
- Even China and Malaysia are considering more comprehensive data privacy laws
- New European Regulation

2. A Global Privacy Ecosystem



3. Key EU Privacy Principles

Personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure; and
- not transferred to countries without adequate protection

4. Key EU Privacy Compliance Requirements

- Registration of personal data/databases/systems with local Data Protection Authorities (DPAs) –
- Data Privacy Policies –
- Web Privacy Statements -
- Data Subject Access Request Policy –
- Data transfer agreements –
- Training for employees –
- Germany: Data Protection Officer –
- Third Party provider Contracts –
- Employee Notification –
- Data Retention Policy –
- Audit –
- Privacy Organisation Structure –
- Cloud offering –
- Marketing issues : cookies, social media etc –
- Data security / data breach –

4. Key EU Privacy Compliance Requirements

- 1995 EU Data Privacy Directive based on 1980s technology, although new proposed Regulation likely to come into force in 2014.
- Therefore have to take a “flexible” and practical approach in complying with the law.
- This only works if you have relationships with DPAs.
- Consequences of non-compliance include serious negative publicity (damage to Company brand and loss of business), fines, criminal penalties in certain countries, and general disruption to business.
- Data Privacy processes and associated policies & teams have become best practice for large multinational corporations.

5. Spotlight: Requirements for Cross-Border Data Transfers

- EU prohibits data transfers to non-EEA countries without "adequate level of protection"
- Need to enter into data transfer arrangement to ensure unrestricted data flows
- A combination of Binding corporate rules (BCR) (for transfers between Company group companies) and Data Transfer Agreements (for transfers outside of the group) could be the most appropriate compliance mechanism, although other tools may be used
  - Exceptions under the EU Data Privacy Directive
  - EU/US Safe Harbor rules
  - EU Model Clauses
  - Alternative Business Clauses
  - Ad-hoc data transfer agreements
  - BCR

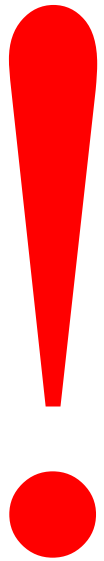
6. Benefits of a compliant data processing system

- Reduced risk exposure.
- Competitive advantage.
- Cost saving – tackling data protection and security at the outset is cheaper and more efficient than fire fighting.
- Streamlined processes and operations.
- Contributes to the efficient management and exploitation of a key business asset.
- Easier to acquire companies as part of the due diligence process.

7. Data Privacy: The Consequences of Non-Compliance

May include:

- Fines (in the UK these can now be up to £500,000) plus EU considering fines of 2% global turnover
- Imprisonment
- Disruption or suspension of business critical data processing
- Audit and investigation
- Undertakings to regulators
- Complaints and actions from customers, employees, suppliers etc.
- Damage and distress to individuals or groups of people



…or worse:

- Damage to the Company brand and loss of business

7. Consequences of Non-Compliance: TJX

LETTER FROM TJX'S PRESIDENT AND CEO

September 21, 2007

To Our Valued Customers:

At TJX, our first priority always has been and continues to be, our customers. I want each of you to know how much I personally and, on behalf of the Company, regret any difficulties you may have experienced as a result of the criminal attacks on our computer systems announced earlier this year. Importantly, we truly appreciate that you have continued to place your trust in us with your loyalty and patronage.

We remain committed to providing our customers a safe shopping environment as you shop for great values, fashion and brands. TJX has been working diligently with some of the world's best computer security firms to further enhance our computer security. We have also continued to work with law enforcement and government agencies and very much want to see that the sophisticated cyber criminals who attacked our computer systems are brought to justice.

We have worked diligently to reach a settlement, which is subject to Court approval and other conditions, that offers a good resolution for our customers. This settlement agreement addresses the different ways customers have told us they have been impacted by the intrusion(s), and we believe that the terms of this settlement are beneficial to our customers. (However, due to the approvals required in connection with class action settlements, customers cannot yet seek benefits under our proposed settlement.) We have provided separate links, below, to the press release and to additional information regarding the proposed settlement and customer benefits. Customers may also call our special customer helplines for additional information, listed below.

Additionally, I encourage you to access the information we are providing on this website to learn more about steps you can take to protect your credit and debit card information, or to contact our special customer helplines.

Once again, we sincerely regret any inconvenience you may have experienced as a result of the attacks on our computer system. We are deeply grateful for your continued trust and patronage.

Respectfully,

Carol Meyrowitz
President and Chief Executive Officer

- TJX suffered a data breach in 2007 which compromised the personal data of thousands of customers.
- In August 2009 TJX reached a settlement with the Massachusetts Attorney General under which it agreed to pay **$9.75 million** to 41 US States affected by the breach and **implement and maintain a comprehensive Information Security Program**.
- Under the settlement TJX must **regularly report to the 41 Attorneys General** on the efficacy of its Information Security Program.

7. The Consequences of Non-Compliance: further examples

- German bank **Deutsche Postbank AG** has been fined a total of **€120,000** by the data protection authority of North Rhine Westphalia for the illegal disclosure of customers' bank account transaction data. The bank **allowed another company to access the data for sales purposes**.
- In August 2010, **Zurich Insurance** was fined **£2.27 million** for the loss of **unencrypted computer back-up tapes containing the details of 46,000 policy holders.** Zurich failed to implement appropriate controls to prevent the loss of confidential information from clients including bank and credit card details.
- The Spanish Supreme Court has upheld a **€300,506** fine received by insurance company **AXA Aurora Iberica** (the Spanish arm of global insurance company AXA). The fine was imposed by the Spanish Data Protection Authority after AXA **disclosed the personal data of its customers to a third party without the consent of the individuals**.
- **Sony in April 2011** went thought a very public global data security breach of its Playstation 3 network with damages and brand loss still to be estimated.

7. The Consequences of Non-Compliance: further examples

- **In April 2011**, Spanish Courts confirmed the decision of Spanish Data Protection Agency to fine the shopping centres company, **El Corte Inglés €60,101** for surveillance video recording outside the facilities the company owns in the city centre in Málaga and capturing the image of pedestrians and the cars parked in the surroundings, disregarding the Spanish video recording regulation.
- **In June 2011**, **Surrey County Council** was fined **£120,000** by the ICO after three incidents of misdirected emails containing sensitive data. The ICO said the penalty recognises the council's failure to ensure that it had appropriate security measures in place to handle sensitive information.
- **In March 2011, Google** received its first ever fine for improperly gathering and storing data for its Street View application. The **€100,000** penalty is the largest ever by French body CNIL. **In August 2011**, Google has received an extra-judicial settlement proposal from the Belgian federal prosecutor for **€150,000** regarding the same issue. Dutch Data Protection Agency has also confirmed that it will fine Google with **€150,000** if the company doesn't comply with its demands.

8. Conclusions

- Project must be supported by top management
- Data protection compliance is no longer a dirty word as part of the corporate governance tag
- 80/20 rule applies – 100% compliance is not truly attainable
- Have a data protection internal structure otherwise work will be lost undertaken again by new people in 5 years time
- Proactiveness and relationships with DPAs are key - if they know you are a “good guy” enforcement is less likely
- Understand the types and flow of data

Training and Awareness

1. Training & Awareness

- Why?
  - Common sense,
  - USSG 7 standards,
  - OECD Good Practice Guidance, &
  - UK Bribery Act Guidance
- All require that organizations train and communicate on the importance of ethics and compliance

2. What, Who and How to Train

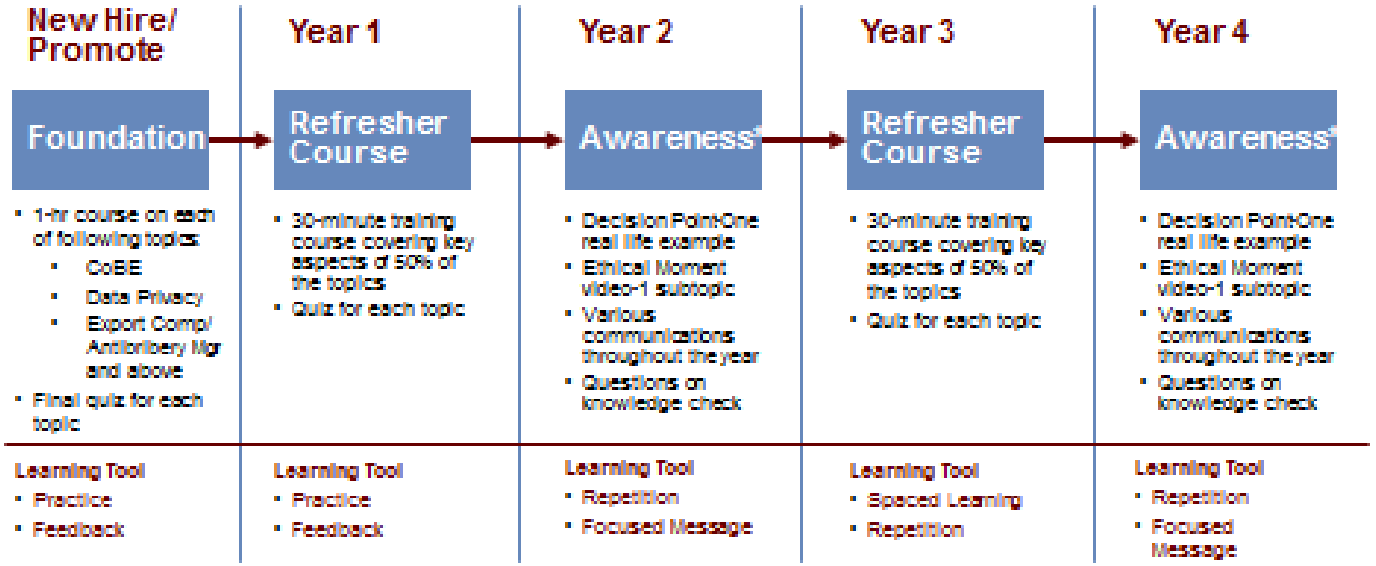
- Every employee should take a one hour training course on the FCPA, UK Bribery Act and EU Data Privacy Law.

3. What, Who and How to Train

- Nonsense!
- Training should be targeted to those employees that need it to “safely” perform their jobs
- Prioritize your risks
- Target employees who face that risk
- Provide training that is relevant to where they live and what they do
  - CBT
  - Live
- What works in your company’s culture?

Sample Path of a Topic in our Cyclical Training Approach

New Joiners will take Foundation courses during their first 60 days. In subsequent years, they will fall into the company program.



NOTE: This does not apply to other required training (e.g., Finance, Local or other)

*Awareness activities and/or Vehicles may change as Technology advances. Test answers will be analyzed to provide topics for awareness activities

9

Source: Accenture Presentation to ECOA 2008

4. How Do You Ensure Training is Effective?

- Did you change observed behaviour (violations/reports)?
- Employee perceptions (survey data changes)?
- Measure knowledge retention:
  - Pre-test for baseline knowledge
  - Post-test 30 days after training to test retention
  - Post-test 90 days after training for long term retention

5. Legal and Practical Considerations

- Required Ethics & Compliance training?
- What does “required” mean—sanctions for failure to complete?
  - Reduce performance ratings and bonus
  - Bock access to internal systems
- Works Councils will need to be involved
  - Local Language requirements
  - Potentially country or workforce based exceptions to global programs

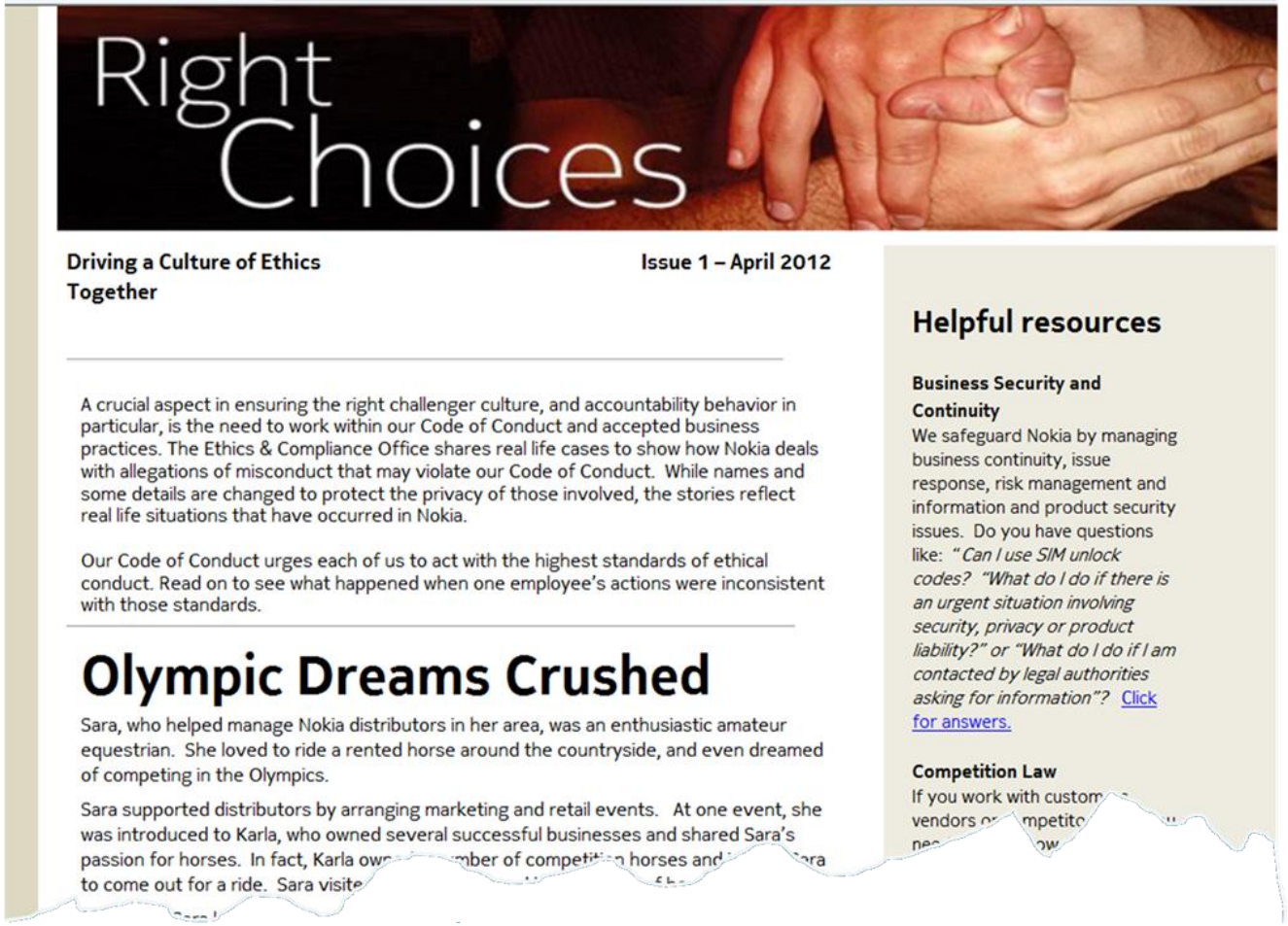
6. What's More Important Than Training?

- Talking about what's the organization standards and expectations for ethical conduct
- Effective messaging can make a huge difference in employees' perceptions of ethical standards and their obligations to meet them
- Don't focus solely on "tone from the top", but perhaps even more importantly
  - Muddle at the middle
  - Buzz at the bottom
- Consider an annual plan across key risk sectors using various channels, methods and media

7. Awareness Messaging

- Can take many forms
  - Social Media
  - Emails
  - Newsletters
  - Intranet articles
  - Flash based games
  - Short “ethical dilemma” videos or even serials
- Key
  - Focused on relevant subjects
  - Compliment and support training programs

8. Case Based Newsletter



Right Choices

Driving a Culture of Ethics Together

Issue 1 – April 2012

A crucial aspect in ensuring the right challenger culture, and accountability behavior in particular, is the need to work within our Code of Conduct and accepted business practices. The Ethics & Compliance Office shares real life cases to show how Nokia deals with allegations of misconduct that may violate our Code of Conduct. While names and some details are changed to protect the privacy of those involved, the stories reflect real life situations that have occurred in Nokia.

Our Code of Conduct urges each of us to act with the highest standards of ethical conduct. Read on to see what happened when one employee's actions were inconsistent with those standards.

Olympic Dreams Crushed

Sara, who helped manage Nokia distributors in her area, was an enthusiastic amateur equestrian. She loved to ride a rented horse around the countryside, and even dreamed of competing in the Olympics.

Sara supported distributors by arranging marketing and retail events. At one event, she was introduced to Karla, who owned several successful businesses and shared Sara's passion for horses. In fact, Karla ow… …mber of competit…n horses and … …ara to come out for a ride. Sara visite…

Helpful resources

Business Security and Continuity
We safeguard Nokia by managing business continuity, issue response, risk management and information and product security issues. Do you have questions like: *"Can I use SIM unlock codes? "What do I do if there is an urgent situation involving security, privacy or product liability?" or "What do I do if I am contacted by legal authorities asking for information"?* Click for answers.

Competition Law
If you work with custom… vendors o… mpetito… …ow…

9. Appendix

- United States Sentencing Guidelines
- OECD Good Practice Guidance on internal Controls, Ethics and Compliance
- UK Bribery Act 2010 Guidance

10. Source Documents

OECD Good Practice Guidance on internal Controls, Ethics and Compliance A(2)(8):

Companies should consider, inter alia, the following good practices for ensuring effective internal controls, ethics, and compliance programmes or measures for the purpose of preventing and detecting foreign bribery: … measures designed to ensure periodic communication, and documented training for all levels of the company, on the company's ethics and compliance programme or measures regarding foreign bribery, as well as, where appropriate, for subsidiaries; (emphasis added).

www.oecd.org/dataoecd/5/51/44884389.pdf

10. Source Documents

United States Sentencing Guidelines. Effective Compliance and Ethics Program

§ 8B2.1(b)(4)(A) *The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program, to the individuals referred to in subparagraph (B) by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities.*

www.ussc.gov/Guidelines/2011_Guidelines/index.cfm

10. Source Documents

UK Bribery Act 2010 *Guidance*

Principle 5

The commercial organisation seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training, that is proportionate to the risks it faces.(Emphasis added)

twww.justice.gov.uk/guidance/bribery.htm