

MANAGING DATA PROTECTION IN THE CLOUD COMPUTING WORLD

Patricia Bailey - MAN Truck & Bus (Volkswagen Group)





Bálint Tóásó - Trenkwalder Hungary

Michael Scuvée - Johnson Controls

DATA PROTECTION OVERVIEW

Patricia Bailey, Compliance Manager - MAN Truck & Bus

MAN BUSINESS OVERVIEW

MAN SE			
Commercial Vehicles		Power Engineering	
MAN Truck & Bus <i>Revenue 2014: € 8.4 bn</i>	MAN Latin America <i>Revenue 2014: € 2.3 bn</i>	MAN Diesel & Turbo <i>Revenue 2014: € 3.3 bn</i>	Renk <i>Revenue 2014: € 0.5 bn</i>
			

MAN Facts
<ul style="list-style-type: none"> • Since 16 July 2013: part of the Volkswagen Group • MAN Group: 2014 Revenues: approx. €14.5 bn; approx. 53,000 employees in more than 150 countries • Nearly 40 colleagues in compliance organisation (local and central) • Languages used at compliance organisation: German, English, French, Portuguese, Spanish, Italian, Danish, Russian, Polish, Chinese, Turkish

BASIC DATA PROTECTION CONCEPTS

- **With regard to outsourcing: your company is 'data controller' and outsourcing company is 'data processor'. This means that your company is always responsible for what the outsourcing company does.**
- ***Personal data (specific to one individual)***
 - This data is subject of the EU Directive 95/46/EC of 1995 and the national laws in the EEA countries. Personal data may also protected by national laws in the countries outside the EEA.
 - Penalties resulting from failure to protect this data are generally of an administrative nature (fines by DP authorities), but there may be civil damages from the individual whose data a company failed to protect.
- ***Non-personal data (facts & figures about a company's suppliers, customers & business partners without reference to an identifiable individual)***
 - This data is usually protected by clauses in your company's contracts with these entities.
 - Penalties resulting from failure to protect this data are usually in the form of civil damages from the companies whose data your company failed to protect.
- ***The biggest risk for your company in either case: Loss of Reputation!***

MANAGING DATA PROTECTION

➤ Policies

- Data protection policy
- Information technology policy

➤ Data protection personnel / specialists

- Data protection officer – at highest level
- Data protection coordinators – in each company

➤ Training

- It is not sufficient to train the local specialist: You must train personnel who may work with data from employees, suppliers, & business partners

➤ Interface with IT department

- At top levels: regular contact with the data protection officer
- In subsidiaries: the two departments should work together
- Intervention by the local compliance manager may be needed

WHAT IS THE CLOUD?

- **'The cloud' is space on the Internet (via a server) that is used to store data, operating systems, or programmes.**
- **Typical business uses for storing data in the cloud:**
 - Back-up, disaster recovery, business continuity
 - Data storage: independently or with an operating system (ex: Salesforce.com)
 - Handheld devices (smartphones or tablets)
- **Data protection implications:**
 - The 'data controller' (your company) must assure appropriate security: to prevent both unauthorised access and accidental loss or damage
 - When inside the European Economic Area, the data controller must assure that if any data is being transferred outside the EEA:
 - the jurisdiction it is going to has at least the same protection as the EU Directive; or
 - if it is going to the US, the recipient is signed up to the Safe Harbour; or
 - certain other conditions must be met
 - One key issue may be where the server is located

JURISDICTIONAL ISSUES

- Until recently, the assumption has been that the laws of the country where the server is located govern the protection of the data contained therein.
- **The Microsoft Case (*In re Warrant to Search Certain E-mail Accounts Controlled and Maintained by Microsoft Corporation*)**
 - In 2013, the FBI obtained a warrant under the 1986 Stored Communications Act that sought access to personal data (emails) that were stored on Microsoft's servers in Dublin, Ireland. Microsoft refused to produce the emails and challenged the warrant in US courts.
 - Arguments of the U.S.: the warrant is directed at a company located in the USA; what matters is the location of the company directed to produce the emails, not the location of the data itself.
 - Arguments of Microsoft: the warrant should not have extra-territorial reach; this is not a warrant directed at Microsoft's records, but at data stored by Microsoft; the US government should go through proper channels, using its treaty with Ireland.
 - The status: the local magistrate in New York and the US District Court ruled in favour of the US government. The case is now before the US Court of Appeals. Numerous *amicus curiae* briefs have been filed.

PRIVACY ASPECTS OF OVERSEAS INTERNAL INVESTIGATIONS

BALINT TOASO DR. MSC

**Senior Legal Counsel and Compliance
Manager - Trenkwalder**

AGENDA

1. AGE OF CLOUD COMPUTING
2. INTERNAL INVESTIGATIONS
3. PRIVACY VS. DATA PROTECTION
4. SAFE HARBOUR



#CWEurope

COMPLIANCE WEEK EUROPE
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

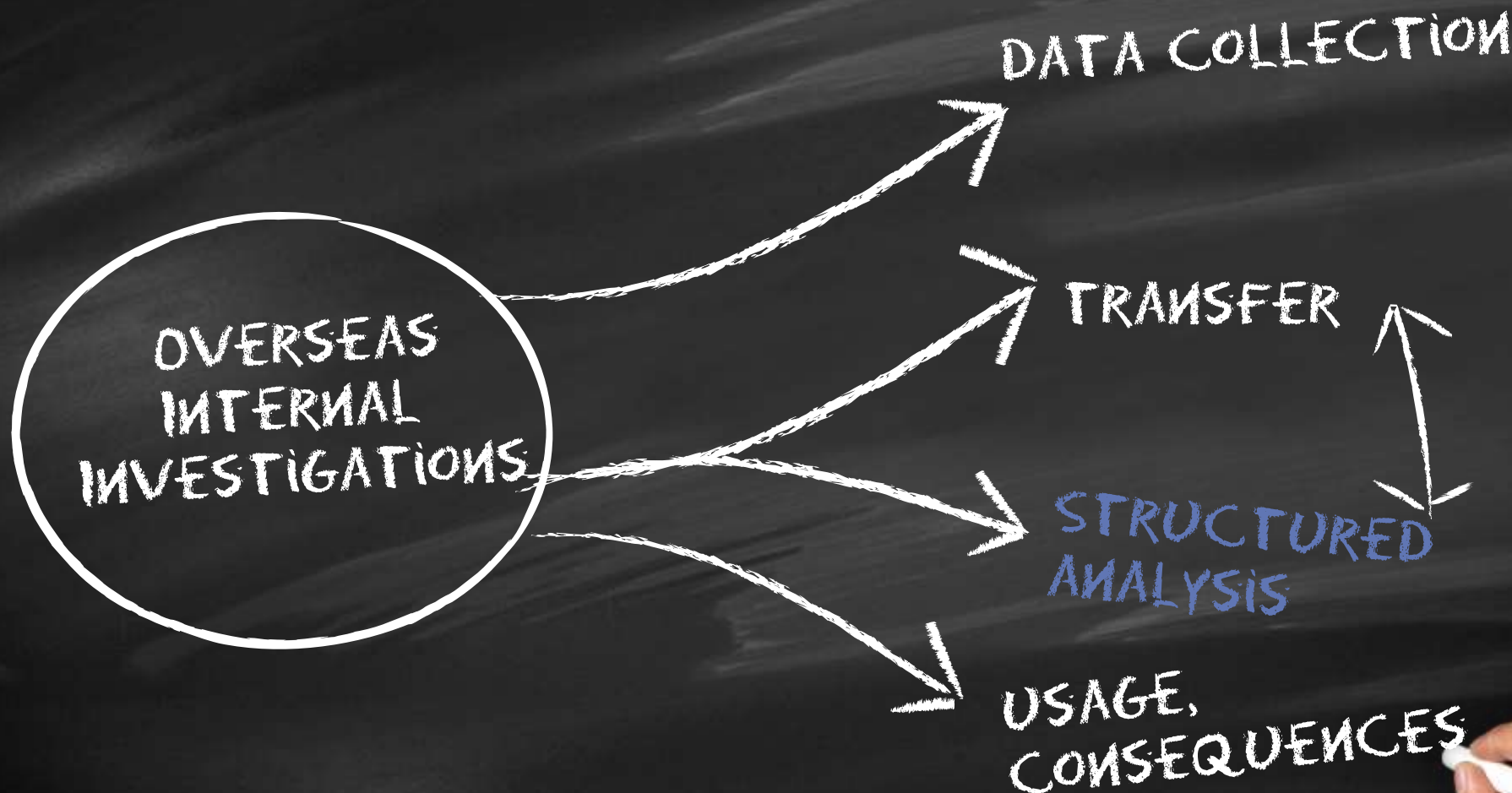
1. PODCASTS WIKIS NETWORK
WEBLOGS INTERNET FORUMS
BLOGGING COMMUNITY
RSS FEEDS
BLOGS E-MAIL SURVEILLANCE
VIDEOS SOCIAL MEDIA
PICTURES CLOUD
ASHLEY MADISON
HACK LIST INTERNET
CC TV
BIG DATA



#CWEurope

COMPLIANCE WEEK EUROPE
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

2.



#CWEurope

COMPLIANCE WEEK **EUROPE**
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

2. TYPICAL ISSUES:

- CONSENT, OR?
- NOTIFICATION
- SCOPE
- USAGE OF EVIDENCES



#CWEurope

COMPLIANCE WEEK **EUROPE**
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

2. FURTHER ASPECTS:



ULTIMATE
GOAL?



EXTRA-TERRITORIAL?



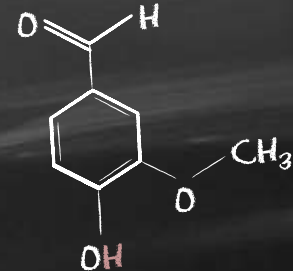
PENALTIES



SENSIBLE PERSONAL DATA



THIRD PARTIES



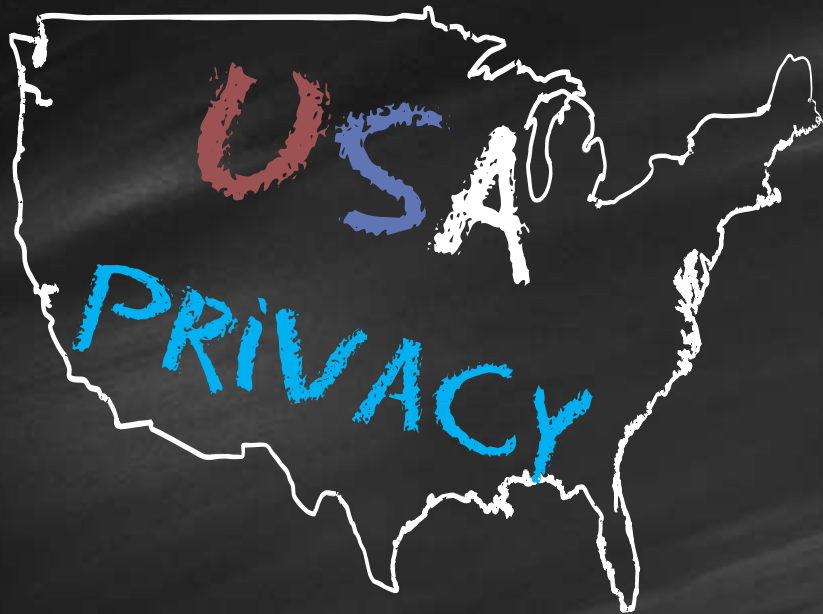
NEW EU FORMULAS?



#CWEurope

COMPLIANCE WEEK **EUROPE**
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

3.



#CWEurope

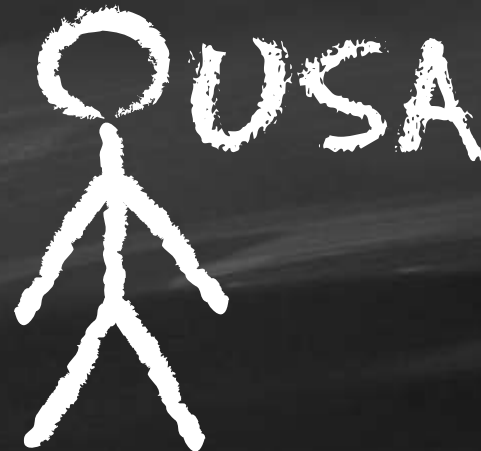
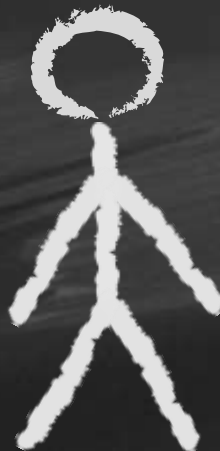
COMPLIANCE WEEK **EUROPE**
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

4.

YOU ARE NOT
PROVIDING
SUFFICIENT
LEVEL OF
PROTECTION!

KHAM, KHAM

EU



#CWEurope

COMPLIANCE WEEK EUROPE
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

4.

IDEA: SAFE HARBOUR



#CWEurope

COMPLIANCE WEEK EUROPE
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

4.

PROS

CONS

EASY

FAST

SELF-MADE

CHEAP

WEAK

UNCLEAR

WHICH

ENFORCEMENT?

FUTURE?



#CWEurope

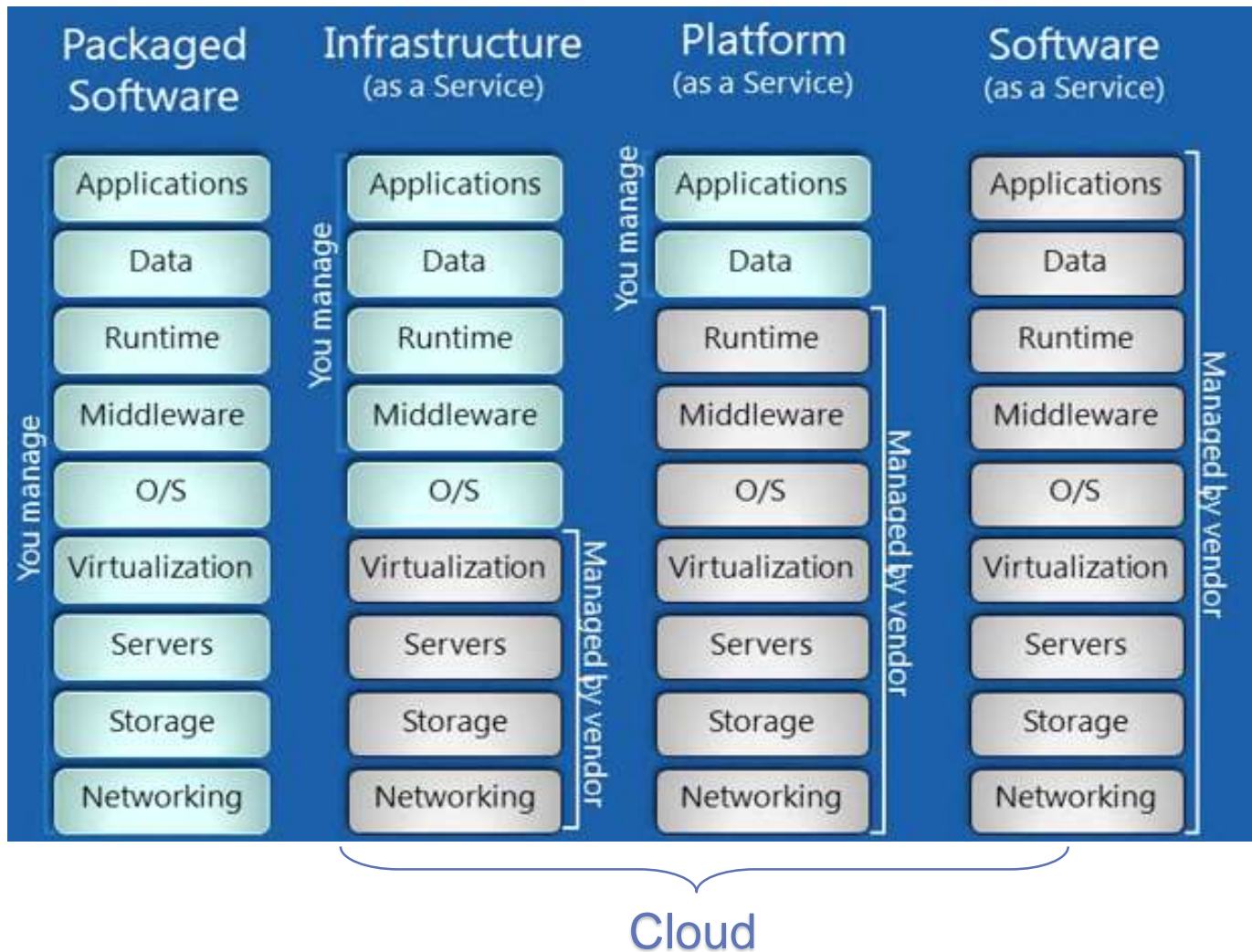
COMPLIANCE WEEK EUROPE
POWERFUL INSIGHTS. PRACTICAL IDEAS. REAL SOLUTIONS

CLOUD & DATA PRIVACY

Michael Scuvée, Director, Global Data Privacy - Johnson Controls

CLOUD MODELS

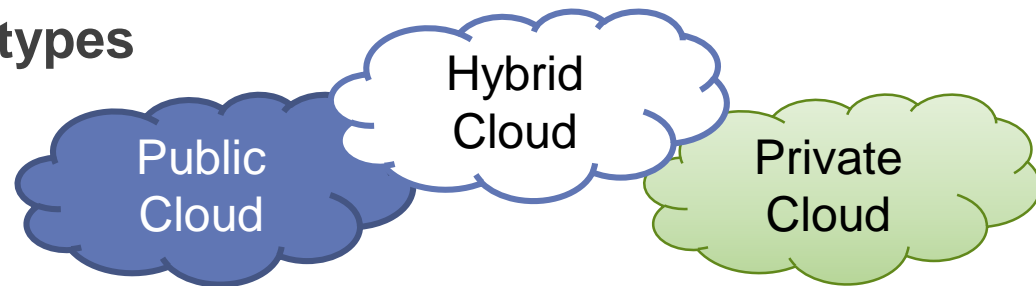
Distinguishing Cloud Deployment models



@CWEurope

CLOUD MODELS

Distinguishing Cloud types



Scalability	High	High
Data segregation	Multiple tenants infrastructure	Single client environment
Infrastructure	Shared infrastructure	Dedicated infrastructure
Storage Location	Little to no control	Visibility / Contractual guarantees
Cost	Low	Medium / High
Security	Generic	Adapted to company risks – contractually guaranteed
Management burden	Low	Medium / High
Application control	Low: automatic updates	End-to-end control: customization



TRAINING & COMMS

43%

of C-level executives say
negligent insiders are the greatest
threat to sensitive data

Teaching employees about data privacy

- Recognize personal data
 - Any information
 - Relating to
 - Identified or identifiable
 - Natural person
- Recognize sensitive personal data
- General awareness and function specific trainings (HR, IT, finance, legal, procurement...)

WORKING WITH IT

Engaging with IT

- Privacy baked into IT project management processes
- Privacy impact assessments – keep it simple
 - Light to low risk projects (typically personal data used for authentication purpose only)
 - Full to medium / high risk projects
- Information classification / hosting / data sensitivity
- Third-party security reviews



You don't know what
you don't know !



@CWEurope

LABOR RELATIONS

Communicating your 'cloud' projects

- 'Cloud' may have negative connotations: Unknown data location? Government access? Data transferred to the US?
- But cloud often means better security – break the myths
- Describe your security and privacy screening processes
- Document and explain the change
- Communicate promptly
- Respect co-determination



LEGAL AND PRIVACY CHALLENGES

Article 29 Working Party opinion WP196:

- Controller – processor roles
- The cloud client is responsible as a controller
- Subcontracting contractual safeguards
- International transfers
 - Contractual guarantees about storage location
 - Safe Harbor not addressing cloud-specific security aspects exhaustively

“...complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.” article 29 Working Party opinion WP196 – adopted July 1st 2012

CLOUD & DATA PRIVACY

Practical Lessons

- Engage with IT to identify relevant projects
- Run privacy impact assessments
- Carefully select and screen your providers
- Consider WP196 when negotiating contracts with providers
 - Storage location
 - Use of subcontractors
 - Security
 - Choice of legal instruments – complement SH with EC Standard contractual clauses or clauses meeting DPA requirements
- Communicate pro-actively and engage with employee reps

THANK YOU!

We want your feedback! Use the conference app or visit the Registration desk.

Be sure to join the Twitter conversation: @CWEurope