

DE BRAUW
BLACKSTONE
WESTBROEK

Privacy and Security

The Balancing Act

Lokke Moerel
Partner ICT
De Brauw Blackstone Westbroek
lokke.moerel@debrauw.com
+31 88 888 1648

Security and Privacy – The Balancing Act

Biometric Authentication

- **Highest security standards to protect society (and individuals forming part thereof)**
- **Biggest impact on privacy of individuals**
- **The Privacy Paradox: if used for protection of personal data: strongest protection of privacy and biggest impact on privacy**
- **The Security Paradox: strongest security and biggest security risks**

Security and Privacy – The Balancing Act

- Security requirements amount to import control
- Privacy requirements amount to export control

Long arm reach data protection legislation

- EU data protection transfer requirements
- long arm reach Data Protection Directive

Long arm reach of security laws

- US Patriot Act: access to PNR from EU air passengers / SWIFT data

Public-to-Private Outsourcing

What is New?

- **Private Actors have been streamlining their IT for quite some time:**
 - centralisation of IT
 - outsourcing and off-shoring (follow the sun principle)
- **“dynamic routing”**: routing of data is not foreseeable
- **more and more cross-border exchange of personal data both within groups of companies and between different groups of companies**

What is New?

- **Outsourcing by Private Actors involves sensitive data**
- **Biometrics for access control well used by Private Actors**
- **Numerous security incidents have caught headline attention for quite some time**
- **Mostly security incidents in EU itself**
- **Issue of conflicting laws (foreign governments to access the data) known for some time**

Conflicting laws

- **Different data protection regimes:**
 - **EU:**
 - **rights of individuals prevailed**
 - **data protection is fundamental human right,**
 - **protection through public law requirements and public control by Data Protection Agencies.**
 - **US:**
 - **focus on sensitive sectors (Telcom, Health, Government)**
 - **trade oriented approach (selfregulation)**
 - **no public law protection**
- **Economic debate transferred into security debate: information requirements of war on terrorism**

Conflicting laws

- **Long arm reach data protection laws**
- **Overlapping and outright conflicting requirements**
- **Data transfer requirements**

- **Centralisation of IT and outsourcing attracts a multitude of applicable laws**
- **100% compliance is not possible**
- **Present EU data transfer regime is outdated and leads to non-compliance**

EU Data Protection Directive

- **dates from time international data transfers were incidental transfers**
 - **expats**
 - **sale of a company**
 - **incidental contracting with US consultants, travel agencies**

EU Model Clauses inadequate for data transfers

- numerous contracts, numerous permits
- require description data transfers:
 - categories data subjects
 - data transferred
 - recipients of data
 - purposes of transfer

- **significant changes require:**
 - **entering into new Model Contracts**
 - **new permits**
 - **new notifications**
- **false sense of compliance:**
 - **compliance on paper**
 - **no material compliance**

Off-shoring

- **Often both customer and supplier are a group of companies**
- **EU model clauses do not facilitate sub-processing (no processor-to-processor model agreement)**
- **For every new client new Controller – Processor Agreements**
- **no solution for “back office” of supplier**

Again - What is New?

- **Does public-to-private outsourcing pose “the most significant ethical questions”?** (p. 11 paper)
- **Use of different biometrics?**
- **Use of different techniques?**
- **Larger scale?**
- **Other or larger security risks?**
- **Other conflicts of law?**
- **Other data transfer issues?**
- **What about “raises legitimate national security concerns”** (p. 12 paper)

Real Issues

- **Underlying processing itself**
- **After 9/11 more focus on security to detriment of data protection**
- **Not so much: whether use biometrics meets data protection requirements**
- **Real issue: should we process these data for security purposes in first place?**
- **Real issue: do our security laws pass the data protection test?**
- **Real issue is not the outsourcing of these data processing**
- **Does not mean outsourcing does not raise data transfer issues**

Data protection issues off-shoring

- **Rely on contractual regime**
- **Paper compliance**
- **No harmonised EU data security laws**
- **Development solutions for “back office” of the processor other than EU model contracts**
- **Alternative: BCR for Controllers (private actors, governments)**
- **Alternative: BCR for Processors**

Next step: BCR

- Use global privacy policy also as tool for compliance EU data transfer rules (alternative for Model Clauses)
- Applying art. 26(2) EU Data Protection Directive (permit based on “adequate safeguards”)
- art. 29 Working Party:
 - WP 74 dated 3 June 2003 material requirements
 - WP107 co-operation procedure for DPAs
 - WP108 model checklist for application for approval of BCR
 - WP 133 model application form
- BCR: mainstream alternative, even preferred option

- **BCR for Processors:**
 - **uniform adequate security level**
 - **check of actual security policy by DPAs**
 - **auditing requirements**
 - **EU headquarters liable**

Co-ordinated procedure

- Request permit from “lead EU DPA”
- Mutual recognition countries
- Lead DPA coordinates approval remaining DPAs concerned
- Central approval BCR

Privacy Wish-list

- **Full harmonisation EU Security Requirements**
- **Guidance WP 29 on BCR for processors**
- **Further guidance WP 29 on use of biometrics especially for governments**
- **EU Model Clause Processor-to-Processor**
- **EU data breach notification requirements**
- **List countries with unacceptable state control powers**