

A PRACTICAL GUIDE TO
INTERNATIONAL DATA PRIVACY
STRATEGY

ISGIG 2008

Pisa 12 March 2008

Christel Cao-Delebarre: Senior Solicitor and Avocat,
Commercial Services, Beachcroft LLP

Fiammetta Amendola: Senior Solicitor and Avvocato,
Commercial Services, Beachcroft LLP

The First Decision You Need to Make: How Compliant Should You Be?

- EU Legislation: The Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data
- 27 local Data Protection Laws
- Legal risk management issue
- Our practical advice: the 80/20 rule

The Minimum You Need to Know: Key EU Definitions (1)

- “PERSONAL DATA”: “(---) any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (Article 2 of the EU Directive)
- “SENSITIVE DATA”: “Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life” (Article 8 of the EU Directive)

The Minimum You Need to Know: Key EU Definitions (2)

- “DATA CONTROLLER”: company, organization or person who alone (or jointly/in common with others) determines the reasons why and the manner in which data are processed
 - Must ensure consent has been obtained from data subjects, that the data is processed in accordance with applicable law and must register with local Data Protection Authority (“DPA”) (if required)
 - Data subjects can exercise their rights against a data controller if the data controller has failed to treat the personal data correctly
 - It is ultimately responsible towards DPAs and data subjects

- “DATA PROCESSOR”: anyone who processes data on behalf of a data controller
 - Usually has contractual obligations to data controller
 - The basis on which the Data Transfer Agreement (“DTA”) is drafted will vary if data is transferred to a controller or a processor

The Minimum You Need to Know: Key EU Principles (3)

- 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
 - not transferred to countries without adequate protection

The Key Things You Need to Do

- Audit/Analyze data processing/data flows/who is who (data subjects/data controller versus data processor)/ purposes
- Notification
- Data Protection policies and notices
- Security Measures
- Data Subject Access Requests Procedures
- Data Retention Policy
- Appointment of a DPO
- Data Transfer Agreement
- Training

The International Data Transfers You Need To Make

- Transfer outside the EEA not allowed except e.g. when data subject's consent has been obtained, processing is necessary for performance of contract, processing is necessary for compliance with legal obligations of the data controller, public interest
- Other Compliance Tools are:
 - Transfer to countries deemed to offer “adequate protection” (so far only Switzerland, Canada, Argentina, Guernsey and the Isle of Man are “adequate”)
 - EU/US Safe Harbor rules
 - EU Standard Clauses
 - Ad-hoc data transfer agreements
 - Binding Corporate Rules (“BCRs”)

EU/US Safe Harbor Rules

- Based on idea of voluntary self-regulation and self-certification of companies with US Department of Commerce
- Key Benefit: Prior approval of data transfers from each DPA normally unnecessary
- Key Negatives:
 - Only covers the transfer of data between the EEA and the US
 - Trades international enforcement of potential violations of transfers to the U.S. (typically private) for FTC enforcement (typically very public) cont'd

EU Standard Clauses

- 3 model form contracts for data transfers to non-EU countries:
 - Controller to Controller (2001/497/EC - Commission decision of 15 June 2001)
 - Controller to Processor (2002/16/EC - Commission decision of 27 December 2001)
 - Controller to Controller (2004/915/EC - Commission decision of 27 December 2004 regarding alternative set of clauses)
- Primary objective: enforcement of EEA citizens' rights against both EEA-based data exporters (controllers) and non-EEA based data importers (controllers/processors)
- These contracts may not mirror the data flows of multinational web-based applications (mainly point-to-point transfers)

cont'd

Ad-hoc Data Transfer Agreements

- May deviate from EU Standard Clauses
- Must adhere to EU Standard Clauses' core principles
- More flexible, but require approval from each DPA

Binding Corporate Rules

- Rules apply to corporate groups transferring data outside the EEA but within their group of companies
- Rules apply irrespective of jurisdiction and nationality of Data Subject
- Rules to be notified to employees
- Must be approved by all relevant DPAs, but submission only to DPA of country where company has main place of business also possible – this DPA will coordinate the authorisation process within EEA
- Actual Trend: today more DPAs seem to promote the use of BCRs for multi-transfers of intra-group data (e.g. in December 2005, the ICO approved the first set of BCRs for the company GE Capital)

Our Practical Recommendations

1. Prioritise management of the compliance project for a successful result
2. Apply the 80/20 rule
3. Understand at a very early stage the types and flows of data and the role of each player (data controller vs. data processor)
4. Develop cost/time effective plan with your lawyers and discuss in detail before implementation
5. Put your house in order and have a data protection internal structure otherwise work will be lost and undertaken again by new people in 5 years time!

Christel Cao-Delebarre
Senior Solicitor and Avocat
Commercial Services
Beachcroft LLP

Mobile: +44 (0) 7801 628 313
E-mail:
ccaodelebarre@beachcroft.co.uk
www.beachcroft.co.uk

Fiammetta Amendola
Senior Solicitor and Avvocatos
Commercial Services
Beachcroft LLP

Mobile: +44 (0)7771 885 396
E-mail:
famendola@beachcroft.co.uk
www.beachcroft.co.uk