

Ensuring DLP: impact of the Belgian law on companies' obligations

L-SEC & Agoria ICT
16 December 2008
Peter Van de Velde
Bird & Bird
peter.van.de.velde@twobirds.com

BIRD & BIRD



Ensuring DLP: regulatory requirements

INTRODUCTION

- ▼ Electronic data management
 - ▼ increasing reliance on electronic data
 - ▼ data are everywhere
 - ▼ proliferation of emails, blogs, social media
 - ▼ legal status of electronic documents
 - ▼ data security becomes a regulatory issue
- ▼ The impact of regulatory requirements
 - ▼ global – local
 - ▼ EU – sector

BIRD & BIRD



Ensuring DLP: regulatory requirements

- ▼ Regulatory requirements – some international examples:
 - ▼ EU Data Protection Directive
 - ▼ EU e-Privacy Directive
 - ▼ EU Data Retention Directive
 - ▼ Basel II (CRD)
 - ▼ MiFID
 - ▼ Sarbanes – Oxley (SoX)

BIRD & BIRD

3



Ensuring DLP: regulatory requirements

- ▼ Regulatory requirements – some Belgian examples:
 - ▼ Wet Bescherming Persoonsgegevens / Loi Vie Privée (1992)
 - ▼ Wet Elektronische Communicatie / Loi Communications Electroniques (2005)
 - ▼ Wetgeving Elektronische Facturatie / Loi Facturation Electronique

BIRD & BIRD

4



Ensuring DLP: regulatory requirements

- ▼ Regulatory requirements – other:
 - ▼ general obligation of carefulness (Art. 1382 BW/CC)
 - ▼ general business law requirements
 - ▼ corporate codes of conduct
 - ▼ sectoral requirements/professional secrecy rules
 - ▼ CAO/CCT n° 68 and n° 81
 - ▼ cybercrime laws

BIRD & BIRD

5



Ensuring DLP: regulatory requirements

- ▼ Regulatory Compliance – Example 1:
 - ▼ Wet Bescherming Persoonsgegevens / Loi Vie Privée (WBP/LVP)
 - ▼ “personal data”
 - any information relating to an identified or identifiable natural person
 - ▼ “processing”
 - any operation performed on personal data
 - ▼ “data controller”
 - natural or legal person that determines the purposes and means of processing
 - ▼ “data processor”
 - natural or legal person that processes personal data on behalf of the controller (but not the employees)

BIRD & BIRD

6



Ensuring DLP: regulatory requirements

- ▼ Wet Bescherming Persoonsgegevens / Loi Vie Privée (WBP/LVP)
 - ▼ business information may contain personal data
 - ▼ general rules of thumb:
 - data may not be held longer than necessary for the purpose of the processing
 - access rights for individuals
 - notification to the Privacy Commission
 - ***obligation to secure personal data!***
 - no transfers of data outside the EEA unless adequate protection
 - ▼ privacy law = criminal law!

BIRD & BIRD

7



Ensuring DLP: regulatory requirements

- ▼ WBP/LVP: Confidentiality and security of processing
 - ▼ The security obligation (Art. 16 WBP/LVP):

"(...) take the appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing of personal data"
 - ▼ organisations need to ensure an appropriate level of security taking into account
 - ▼ the state of the art in security
 - ▼ the cost
 - ▼ the nature of the data to be protected
 - ▼ the nature of the risks
 - ▼ choice of a third party data processor (outsourcing!): sufficient guarantees in respect of security - a written agreement is required

BIRD & BIRD

8



Ensuring DLP: regulatory requirements

- ▼ WBP/LVP: Confidentiality and security of processing
 - ▼ The security obligation – what does the law say?
 - ▼ keep the data updated
 - ▼ restrict access to / processing of data to authorised persons
 - ▼ inform authorised persons
 - ▼ ensure compliance of programmes with notifications
 - ▼ Obligation of means
 - ▼ The “ten commandments” of the Privacy Commission (www.privacycommission.be)



Ensuring DLP: regulatory requirements

- ▼ WBP/LVP: Confidentiality and security of processing
 - ▼ The security obligation – what does it mean for organisations?
 - ▼ written security policy / strategy
 - ▼ data security officer
 - ▼ organisational measures
 - ▼ measures to protect physical security of data
 - ▼ measures to protect network security
 - ▼ classification of data / restricted access
 - ▼ tracking / monitoring schemes
 - ▼ follow-up / control
 - ▼ incident response / business continuity
 - ▼ record-keeping



Ensuring DLP: regulatory requirements

- ▼ WBP/LVP: Enforcement
 - ▼ Privacy Commission
 - ▼ Criminal Courts
 - ▼ President of the Court of First Instance
 - ▼ special procedure for data subjects
 - ▼ Court of First Instance
 - ▼ Chairman of the Privacy Commission (action right)
 - ▼ Damage claims
 - ▼ Art 15bis
 - ▼ Use of WBP/LVP in commercial cases?



Ensuring DLP: regulatory requirements

- ▼ Privacy Commission – powers:
 - ▼ notification/public register
 - ▼ advisory opinions
 - ▼ recommendations
 - ▼ investigation of complaints
 - ▼ substantive investigation powers (audit/inspection)
 - ▼ inform public prosecutor of infringements
 - ▼ no administrative fines



Ensuring DLP: regulatory requirements

- ▼ Judicial enforcement of the WBP/LVP
 - ▼ What is sanctioned?
 - ▼ infringements listed in Art. 38-39
 - ▼ Who is liable?
 - ▼ data controller and his employees/directors
 - ▼ What are the sanctions?
 - ▼ criminal fines
 - ▼ publication of court order
 - ▼ confiscation of carriers of personal data
 - ▼ interdiction to manage any processing of personal data for up to 2 years
 - ▼ recidivism can lead to imprisonment
 - ▼ civil liability of data controller for fines incurred by employees/directors



Ensuring DLP: regulatory requirements

- ▼ Enforcement of data protection law – other countries:
 - ▼ Nederland
 - ▼ France
 - ▼ United Kingdom
 - ▼ Deutschland
 - ▼ España



Ensuring DLP: regulatory requirements

▼ Regulatory Compliance – Example 2:

- ▼ Wet Elektronische Communicatie / Loi Communications Electroniques (2005)
 - ▼ data retention: 12 to 36 months
 - ▼ unrestricted access to data from Belgium
 - ⇒ *implementation of EU Data Retention Directive!*
 - ▼ telecommunication secret
 - ▼ encryption
 - ▼ archiving of commercial email / transactions
 - ▼ security obligations for network and service providers



Ensuring DLP: regulatory requirements

▼ Regulatory Compliance – Example 3:

- ▼ CAO/CCT n° 81 on the monitoring of e-mail and internet use at work
 - ▼ transparency (information obligations)
 - ▼ control requires specific objective
 - ▼ phased approach
- ▼ But what do the courts say?
 - ▼ legal uncertainty
 - ▼ a good policy can save a lot of trouble



Ensuring DLP: regulatory requirements

▼ DLP and Cybercrime

- ▼ Wet Informatiecriminaliteit / Loi Criminalité Informatique (2000)
 - ▼ offences against the confidentiality, the integrity and the availability of IT-systems and data
 - data manipulation (viruses, ...)
 - hacking
 - external hacking
 - internal hacking
 - ▼ liability issues (cf. DoS attacks, ...)
 - ▼ case law: pragmatic! (offenders not liable for security costs)



Ensuring DLP: regulatory requirements

De Rechtbank acht deze schade niet het gevolg van het misdrijf. Om reden dat het internetbankieren niet voldoende beveiligd was, niettegenstaande de bank hiervan uitging, kan dit uiteraard beklagde niet in de schoenen geschoven worden. Integendeel, beklagde heeft door zijn handelen meer misbruiken kunnen voorkomen. De vordering is dan ook ongegrond.

(...)



Ensuring DLP: regulatory requirements

▼ What's next?

Towards a law on
security breach
notifications?



Ensuring DLP: regulatory requirements

▼ Why is good data security important?

- ▼ evidence in legal disputes
- ▼ control by regulatory / supervisory authorities
 - ▼ Privacy Commission
 - ▼ Competition Authorities
 - ▼ Tax Administration
 - ▼ other
- ▼ protection of interests vis-à-vis third parties
 - ▼ good housekeeping



Ensuring DLP: regulatory requirements

▼ Conclusions

- ▼ Data security
 - ▼ understand the patchwork of legal requirements
 - ▼ ensuring the confidentiality, integrity, authenticity and availability of information
 - ▼ establish a data security policy that ensures regulatory compliance (e.g. personal data) and that is commercially workable
- ▼ Action points
 - ▼ risk analysis
 - ▼ solutions, policies and practices
 - ▼ assessment and follow-up

BIRD & BIRD

21



THANK YOU FOR YOUR ATTENTION

Peter Van de Velde
Advocaat
BIRD & BIRD
Oudergemselaan 22-28 bus 9
1040 Brussel

peter.van.de.velde@twobirds.com

+32 2 282 60 59

BIRD & BIRD

22

