Top 10 Data Protection Do’s & Don’ts in M&A

Strategic Data Protection & Compliance
8th Annual Summit
October 23, 2013

Presented By Alja Poler De Zwart
Overview

Identification of key data protection issues and how to resolve them:

- Why does it matter?
- Privacy in a nutshell
- Pre-deal preparation
- Due diligence for buyers
- Top 10 Do’s and Don’ts
- Deal breakers
Why does it matter?

- Almost all M&A transactions require the parties to exchange personal data
  - Seller’s employee (HR) and customer (CRM) information
  - Information on the nature of the services, such as e-commerce activities
- Addressing data protection compliance at an early stage allows sufficient time for any necessary remedial steps
- Privacy laws exist in 90+ countries worldwide
- Enforcement has increased
- Sanctions for non-compliance can bring business to a halt
- In Europe, Draft Data Protection Regulation will replace the current Directive
  - Will apply not only to companies established in EU/EEA but also to companies that collect and process EU/EEA residents’ personal data
  - Fines for non-compliance of up to 2% of annual worldwide turnover
Data protection in a nutshell

• **Personal data** are any information relating to an identified or identifiable individual

• **Sensitive personal data** are information about health, sex life, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and in many jurisdictions criminal conduct and records

• **Processing of sensitive data** is usually prohibited unless there is opt-in consent from individuals or if narrow exceptions apply

• **Processing** is any operation involving personal data, such as collection, use, modification, storage, access, disclosure, transfer, and deletion
  
  ➢ Personal data may be processed only where there is an applicable legal basis, unless narrow exceptions apply

• **Transfer** of personal data outside the EEA requires an adequate transfer mechanism
General guidelines

- Designate person responsible for data protection issues
- Limit collection/disclosure of personal data to a minimum
- Limit internal and external distribution of personal data on a “need to know” basis
- Use secure methods to share personal data
- Be particularly careful with use of sensitive personal data
- When required, give notice and provide choice to individuals
- Comply with individuals’ access and correction rights
- Ensure personal data are deleted when no longer needed
M&A process

- Privacy issues need to be addressed by all parties (buyer and seller) at every stage of a transaction

Initial Contact (MoU)  Contract Negotiation  Implementation/Transition
Preparation for sellers

- Check that business is in good enough “data protection shape” to ensure a smooth transaction
  - Notice to individuals to cover the intended processing
  - Access, correction, and rectification policies
  - Appropriate technical and organizational security measures
    - Prevent unauthorized or unlawful processing, accidental loss, destruction, or damage
  - Cross-border data transfer safeguards
  - Registrations with data protection authorities
  - Seller may need to retain certain data for business continuity and regulatory compliance
Preparation for buyers

• Identify potential data protection issues or areas of concern
  ➢ What information is required to carry on the business post-acquisition?
  ➢ How might the buyer’s proposed use of the information post-acquisition differ from the seller’s current use?
  ➢ Is the business being acquired “information heavy”?
  ➢ What is the significance of the information (personal data) in the transaction?

• By addressing these issues at an early stage, the buyer will be in a better position to –
  ➢ Ensure compliance in the deal due diligence process
  ➢ Negotiate the sale and purchase agreement
  ➢ Identify steps it may need to take post-completion to achieve an appropriate level of compliance
  ➢ Determine price offer
Due diligence for buyers

- Treat information received in a manner that allows for easy return if the deal does not go ahead

- Request details –
  - Local registrations with data protection authorities or reasons for not registering
  - All enquiries, notices, complaints, proceedings, and claims brought by individuals or authorities within a limited period
  - All outstanding access and correction requests and complaints
  - All privacy and data protection audit results/reports from the past 3-5 years
  - Any privacy penalties, fines, undertakings, or orders
  - Any data security breaches in the past 3-5 years and remedial action taken
  - Any data protection or associated policies
  - Notices given to individuals
  - Sources of personal data and how they were obtained, used, and retained both internally and externally
  - Copies of all material data processing agreements
  - Seller’s approach to (cross-border) compliance, i.e., the basis/transfer mechanism or exemption on which the seller relies when processing and transferring personal data
Do

1. Appoint a person or a team responsible for privacy-related issues
2. Educate and collaborate with your team to achieve business goals
3. Have a standard deal playbook (diligence questionnaires and document request forms) in place that is appropriate for data protection issues
4. Seek and retain external legal advice
5. Put in place appropriate data processing agreements with third-party due diligence providers and check registrations, notifications to individuals, etc.
6. Identify information to be retained and information to be transferred
7. Implement appropriate technical and organizational security measures in respect of the transaction process
   - Disclosure of personal data only as needed for due diligence purposes; make sure information is protected and returned if the deal doesn’t go through
8. Assess company’s data protection compliance
9. Confirm the ability to lawfully sell personal information
10. Try to reduce/allocate identified risks
    - Closing conditions, indemnities, purchase price adjustments, holdbacks
Don’t

1. Start the transaction process unprepared – get to know the other party
2. Assume business compliance – perform extensive due diligence
3. Wait till the very last moment – start preparation and due diligence on time
4. Ignore the benefits of good legal advice – retain legal counsel
5. Forget to or choose not to implement security measures in respect of the transaction process
6. Assume that the other party will provide all necessary information – be diligent, check, and double check as much as possible, keep asking questions
7. Underestimate or ignore privacy and data protection issues identified during due diligence – take immediate action
8. Hesitate to reduce/allocate identified risks
9. Retain or process more information than strictly necessary
10. Underestimate or ignore post-acquisition steps required to achieve an appropriate level of data protection compliance (e.g., update notices and registrations)
Deal breakers

• Due diligence reveals major privacy and data protection issues
  ➢ Company’s overall data protection non-compliance
  ➢ Lack of or non-compliant or risky agreements with service providers
  ➢ Recent or frequent data security incidents
  ➢ Pending legal claims and procedures
  ➢ Data protection sanctions and PR exposure – or high risk of
  ➢ Company lacks ability to lawfully transfer/sell personal information
  ➢ Dubious privacy commitments
    ▪ “We never share your information with ANYONE”

• Company is unwilling to reduce/allocate risks
  ➢ Closing conditions, indemnities, purchase price adjustments, or holdbacks

• Company made false representations and warranties about the status of data protection compliance
References


- Draft Data Protection Regulation