The General Data Protection Regulation's Impact on M&A

PRACTICAL ADVICE ON HOW TO CONTINUE A SMOOTH M&A PROCESS

Presented by
Avi Gesser, Davis Polk partner, Litigation/Cybersecurity
Pritesh P. Shah, Davis Polk partner, IP and Technology Transactions
Steven Silberstein, COO, BlueVoyant

May 24, 2018

Davis Polk

Davis Polk & Wardwell LLP

CLE CREDIT AVAILABLE

WWW.CYBERBREACHCENTER.COM

Agenda

The GDPR – Important Implications for M&A Transactions

Legal Diligence – Target Characteristics and What to Ask

Technical Due Diligence

Transaction Agreement Considerations

Conclusion & Takeaways

The GDPR – Important Implications for M&A Transactions: When, for Whom and Why?

Effective tomorrow, **May 25, 2018**

Extraterritoriality	Scope	Fines
Governs the processing of E.U. personal data by companies both within and outside of the E.U. ▪ **Processing** is defined broadly as any kind of use, including storage and destruction ▪ **Personal Data** includes online identifiers and location data ▪ **Processing in the U.S.** related to offering goods or services or monitoring behavior in the E.U. is covered	GDPR governs the processing of personal data by data *controllers* (determining the purpose and means of the processing) and data *processors* (processing on behalf of the controller)	GDPR violations can result in fines up to the greater of **EUR 20 million or 4% of total worldwide annual turnover** of the preceding financial year

How do Data Privacy and Cybersecurity Obligations affect M&A Transactions?

- Regulators are requesting Cybersecurity Due Diligence (e.g., NYDFS)
- Recent enforcement actions highlight the importance of Cybersecurity DD in M&A transactions
  (e.g., Yahoo! Resolution)
- Effects that cybersecurity obligations can have on M&A transactions:
  - Civil and regulatory liability resulting from an undisclosed breach
  - Loss in value of stolen intellectual property
  - Loss of customer and/or employee goodwill as a result of an undisclosed breach
  - Costly regulatory compliance obligations for the acquirer (e.g., GDPR, HIPPA)
  - Significant expenditures to remediate poor cybersecurity

The GDPR – Important Implications for M&A Transactions: What are Main Risks of Non-Compliance?

Adequate Security	Breach Notification – Low Thresholds and Short Deadlines	Data Subject Rights	Data Transfers from the E.U.	Vendor Management
Controllers are required to implement "appropriate technical and organizational measures" for data protection	▪ Controller must **inform the Supervisory Authorities within 72hrs** after becoming aware of the breach and risk to rights and freedoms of individuals likely ▪ Controller must inform individuals in case of **high risks** for their rights and freedoms	Controllers must be able to locate, delete, hand over and correct the data of a specific individual to comply with data subject rights (e.g., "right to be forgotten", "right of access", "right to data portability")	Additional requirements to transfer data outside of the E.U. to ensure appropriate protection	Controllers may only use processors who provide "sufficient guarantees" to implement appropriate technical and organizational measures and contracts must have enumerated provisions

Legal Diligence:
Target Characteristics and Team

Target Characteristics

- Importance of the data (personal or otherwise) to the target's business
- Type of data (PCI, SSNs, highly sensitive information)
- Consumer focused vs. business to business
- Geographic footprint (extent of operations in the E.U. / transfers abroad)
- Heavily regulated component of target business (healthcare, financial services, etc.)

Team Composition

- More than just the lawyers
- Business team users of data
- Chief Information Security Officer
- Chief Information Technology Officer
- Chief Privacy Officer / Data Protection Officer

Legal Diligence: Questions to Ask

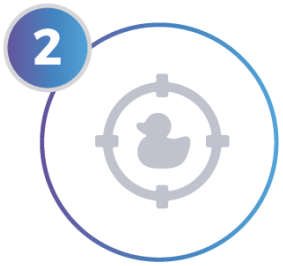
- Do you operate in the EU or otherwise process EU data?
- What kind of data do you have?
- How and for what purpose is your data used?
- With whom is it shared and why?
- Is data transferred across borders?
- What security safeguards are used to protect the information?
- Who is responsible for privacy and cybersecurity?
- What are your cyber/privacy policies, procedures and training?
- Have there been any past breaches and how have they been resolved?
- Have there been cyber/privacy regulatory actions or civil litigation?
- Do you have cyber insurance? What is covered? In what amount?
- Do you have a law firm and cyber firm on retainer? An FBI contact?

Technical Cyber Due Diligence

Cyber M&A Due Diligence provides a detailed perspective of a company's network and technology risk profile before a merger and can be leveraged to increase preparedness for IT integration after a merger.

DISCOVERY

What infrastructure am I buying?



VULNERABILITY

Is that infrastructure exposed and vulnerable?

TARGETED

Has or Is the infrastructure been or being targeted?

COMPROMISE

Is there evidence of breach?

Cyber M&A Due Diligence – The External View is Key…

WHAT INFRASTRUCTURE AM I BUYING?

INFRASTRUCTURE OVERVIEW

PUBLIC FACING INFRASTRUCTURE ATTACK SURFACE:

NOTE: HOST SCANNING OPTION NOT SELECTED BY CLIENT

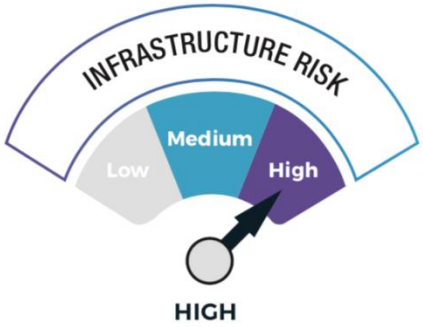
TOPOLOGY BREAKDOWN

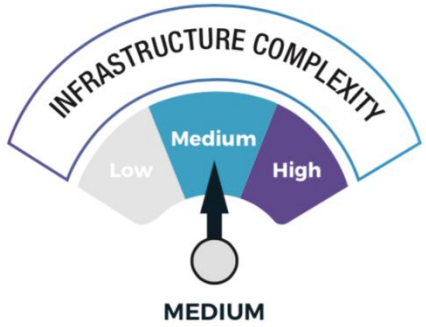
36%
OF THE NETWORK IS HOSTED INTERNALLY

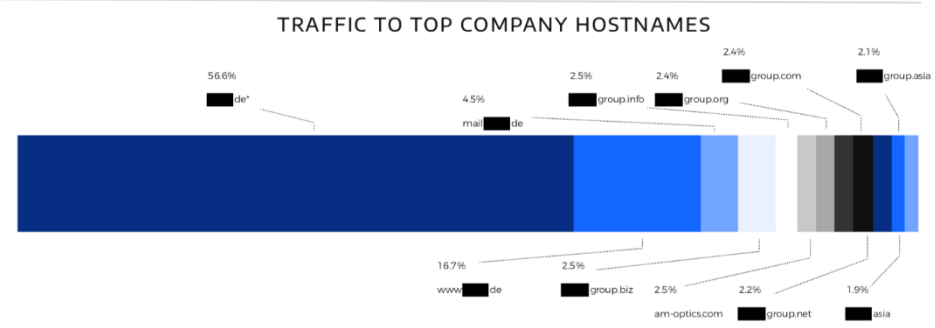
64%
OF THE NETWORK IS OUTSOURCED TO THIRD PARTY CLOUD PROVIDERS

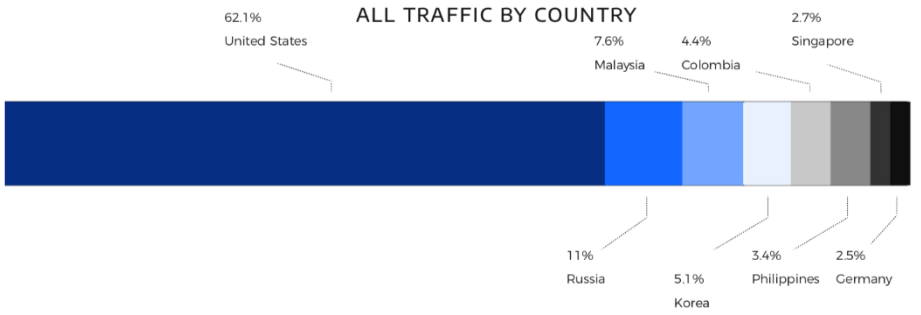
THE TOP THREE CLOUD PROVIDERS ARE

amazon web services
Google
linode









Transaction Agreement Considerations: Representations and Warranties

- "Personal Data" must be broad enough to cover GDPR's expanded breadth
- More than compliance with law; also:
  - Current and prior external and internal privacy policies
  - Cross-border transfers subject to appropriate bases
  - Applicable industry standards (e.g., PCI-DSS)
  - Data-privacy-related contract obligations (e.g., processor-controller obligations)
  - Relevant guidance (Art. 29 WP/FTC best practices)
- Appropriate information security program
- No breach, exfiltration or unauthorized use of personal data
- No breach notification obligations or notifications
- No claims, investigations or complaints
- No restriction on transfer

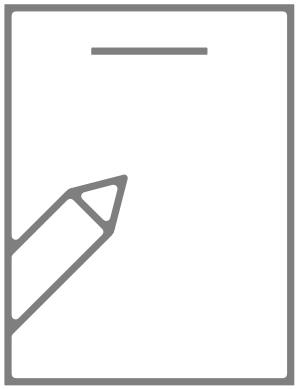
Transaction Agreement Considerations: Risk Allocation

- Consider adequacy of representation and warranty indemnity survival periods and limitations on liability
- Consider special indemnities for any known issues
- Make personal data and cybersecurity issues an excluded liability
- If utilizing representation and warranty insurance, check if data privacy is excluded
  - Consider the scope of data privacy diligence to be conducted: while known liabilities are typically excluded from coverage, doing meaningful diligence will help with obtaining coverage
  - Consider adequacy of insurance limits

Transaction Agreement Considerations: Post-Closing Implications

- Transition Services Agreements involving personal data must meet processor-controller requirements
- Buyer's planned use of data may not be permitted without updated, affirmative consents from relevant data subjects
- Transfer of target data outside of the E.U. requires appropriate basis
- New or expanded regulatory compliance function

Conclusion & Takeaways



GDPR is effective tomorrow

M&A buyers, investors and sellers should evaluate whether the GDPR will apply and consider the materiality of personal data to the target's business

GDPR is lengthy and dense – important to understand and prioritize review

Enforcement actions will help provide guidance

Questions?

Visit: **www.cyberbreachcenter.com**