Strafford

Presenting a live 90-minute webinar with interactive Q&A

Impact of EU GDPR and New California Privacy Law on M&A: New Due Diligence and Other Challenges for Buyers and Sellers

Mitigating Risk With Reps and Warranties, Post-Closing Considerations

THURSDAY, JULY 11, 2019

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Avi Gesser, Partner, **Davis Polk & Wardwell**, New York

Scott T. Loughlin, Partner, **Hogan Lovells US**, Washington, D.C.

Nigel Parker, Partner, **Allen & Overy**, London

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-888-450-9970** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

What we will cover today

1	**Introduction** Increasing appreciation of the value of data Greater focus on privacy risk; changes to risk appetite Changes in market practice and enforcement risk Deal types
2	**Early stage activities on a deal** Preparation of a business for sale Populating data rooms Deal structuring NDAs Other agreements (e.g. VDR providers)

What we will cover today

3	**Due diligence phase** How data privacy and cyber security can affect valuation Who should conduct diligence and who should respond Key risks and how to identify them How to quantify and assess identified risks How to address identified risks
4	**Doing the deal** Deal terms: SPA; TSA, etc. Employee communications Works council consultations Pre-closing phase

What we will cover today

5	**After the deal** Updating privacy notices and customer communications Control over use of marketing permissions Data migration; TSA cutover Managing use of data/databases post-deal / on-going controls Post-deal integration activities
6	**Q&A**

Introduction

The value of data

Microsoft Buys LinkedIn for $26.2 Billion, Reasserting Its Muscle

Google buying nest for $3.2 billion..

LinkedIn buys cross-device identity provider Drawbridge

Facebook to buy messaging app WhatsApp for $19bn

Themes

- Data-driven M&A
- Greater appreciation of the value of data
- More data-driven business models

- More focus on data privacy and cyber risk
- Changes to privacy and cyber risk appetite

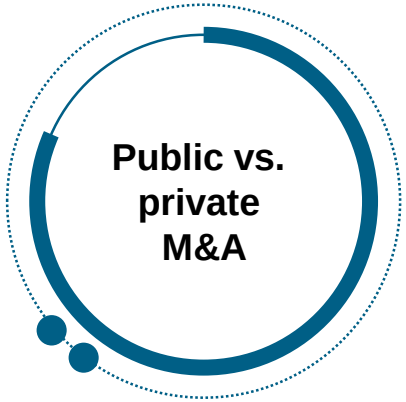
- Evolution of market practice
- Differing approaches across jurisdictions

- More enforcement?
- Intervention of non-privacy regulators (e.g. anti-trust authorities)

Deal types

- Sale/purchase of shares in a privately owned company
- No “transfer” of data on completion
- No change in organization to which permissions/consent to process data may have been given
- Transfer of risk to the buyer (caveat emptor) unless agreed otherwise
- Due diligence process; representations and warranties given by seller

- Sale of “assets” owned by a seller, which could include IP, real estate, receivables, contracts, employees, etc.
- There will be a “transfer” of data on completion from seller to buyer
- There will be a change in the organization to which permissions/consents given
- No transfer of risk to the buyer unless agreed otherwise
- Due diligence process; representations and warranties given by seller



– Sale/purchase of shares in a company, which is listed on a stock exchange
– Due diligence generally limited to publicly available information
– Risks may be disclosed in the company’s annual report or other stock exchange filings

Preparing for the Sale

(sell-side perspective)

Hogan Lovells

Preparation of a business for sale

- Articulating the value of data assets
- Existing notices
- Non-disclosure agreements (NDAs)
  - Incorporate data hygiene principles (need-to-know restrictions, access controls and accountability, data destruction and/or return upon termination)
  - GDPR responsibilities (controller vs. processor)
  - Data transfers
  - CCPA exception to “sale” of data
- Other agreements
  - VDR providers
  - Bankers
  - Advisors
- Document processing and transfers of data
  - From Seller to VDR provider
  - From Seller to potential Buyer

Hogan Lovells

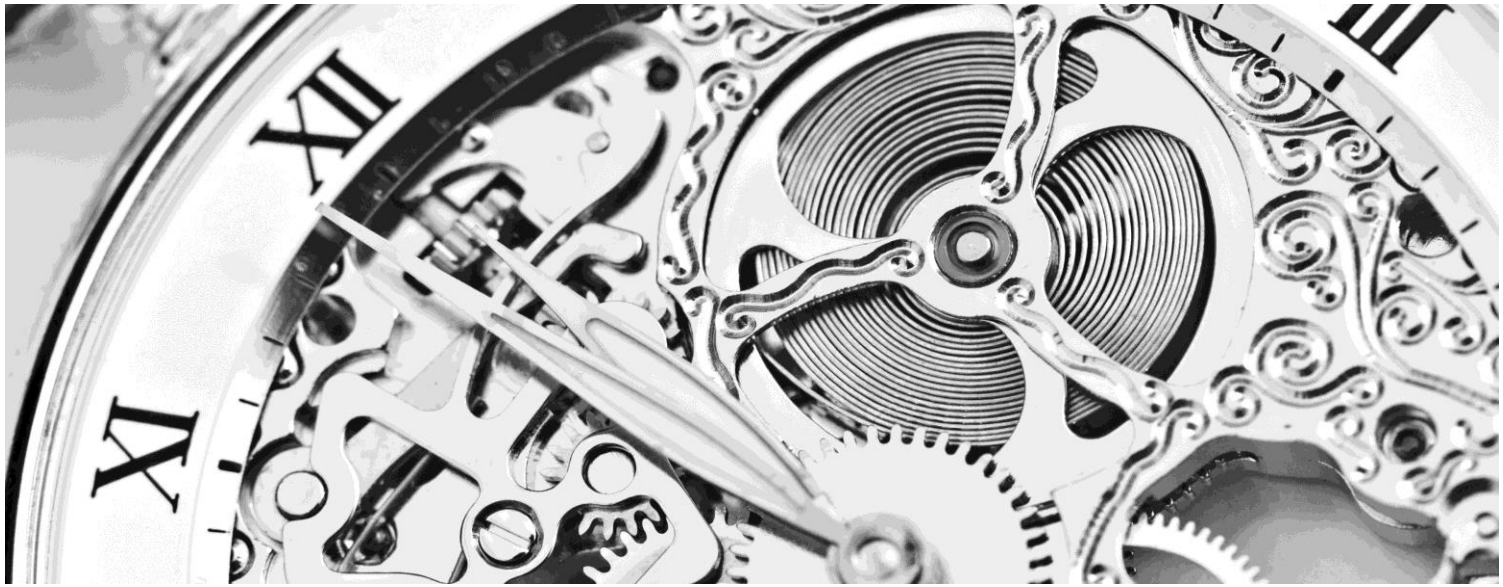
Preparing for diligence

- Populating data rooms
  - Minimize personal information in the data room
  - Limited access “clean rooms”
  - Sharing HR or consumer data, anonymized or aggregated basis only if possible
  - Due diligence request governance process
- Getting ready to respond to diligence questions

Hogan Lovells

Deal structuring

- Type of transaction
  - Stock sales vs. asset deals
  - GDPR data “controller”
  - CCPA “sale” of data
- Limits on legal authority to transfer data
  - Pre-deal data transfers
  - Setting up the transaction in a way that allows for data transfers



Hogan Lovells

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

- Regulators are requesting Cybersecurity Due Diligence (e.g., NYDFS)
- Recent disclosures and enforcement actions highlight the importance of Cybersecurity DD in M&A transactions (e.g., Marriott and 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. the GDPR, HIPAA)
  - Significant expenditures to remediate poor cybersecurity

CCPA and GDPR –Implications for M&A Transactions
What are the main compliance obligations?

Adequate Security	Breach Notification – Low Thresholds and Short Deadlines for GDPR	Data Subject Rights	Data Transfers from the E.U. for GDPR	Vendor Management
Data controllers are required to implement reasonable or appropriate technical and organizational measures for data protection	▪ Controller must **inform the Supervisory Authorities within 72 hours** after becoming aware of the breach and risk to rights and freedoms of individuals likely ▪ Controller must inform individuals in case of **high risks** to 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 Ca or 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

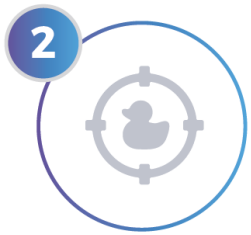
- Do you operate in Ca or E.U. or process Ca or E.U. data?
- What kind of data do you have?
- How and for what purposes is your data used?
- With whom is the data shared and why?
- Is data transferred across borders?
- What security safeguards are used to protect the information?
- Who is responsible 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 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?

Davis Polk

Transaction Agreement Considerations: Representations and Warranties

- "Personal Data" must be broad enough to cover the CCPA and 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 contractual 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 made
- 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

Doing the deal

Hogan Lovells

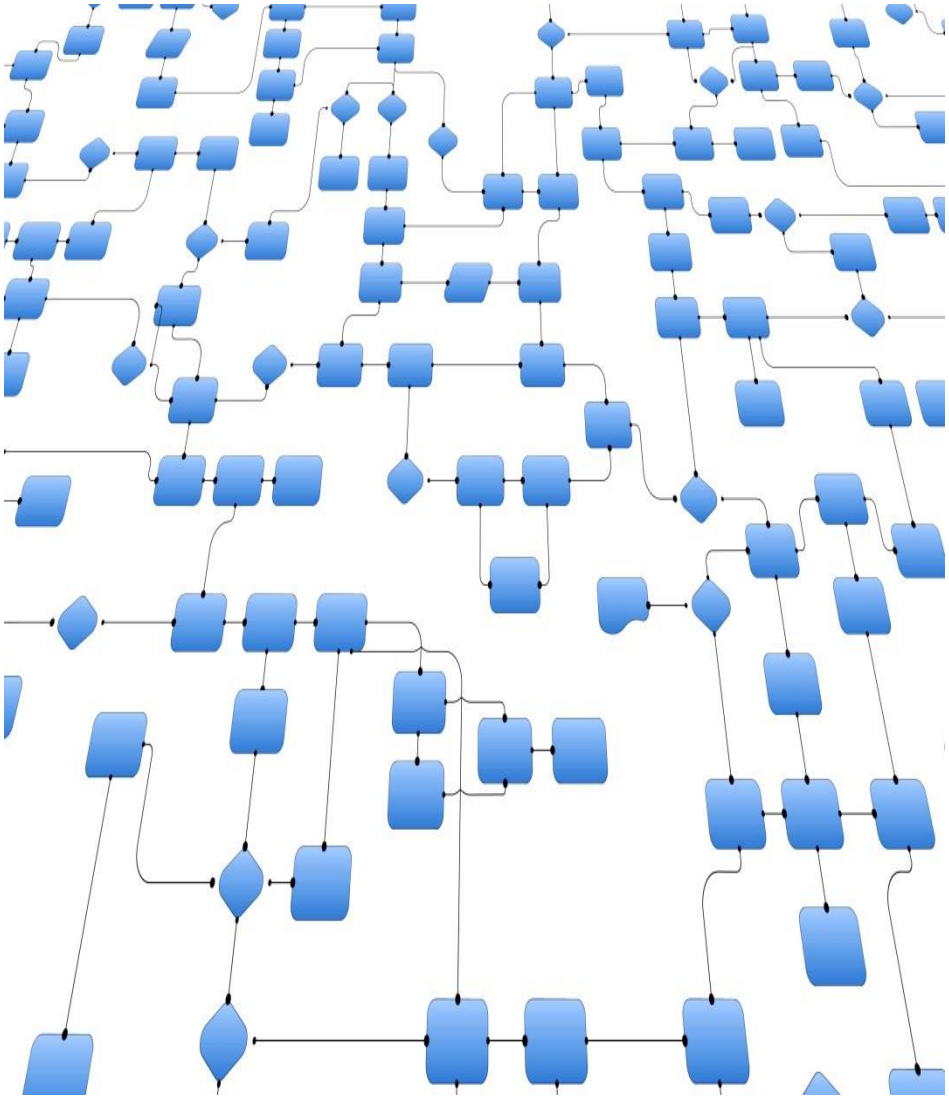
Agreements & Contractual Terms

- Reps and warranties
  - Support of due diligence
  - Longer and more comprehensive terms for privacy and data security, fundamental reps
  - Disclosure schedules
  - R&W insurance
- Covenants and Conditions
- Indemnities
  - Aggressive asks regarding breach
- Parties' roles with respect to personal data
  - Controller/Processor terms
  - Business/Service Provider terms
- Other data privacy provisions

Hogan Lovells

Ancillary Agreements

- Transition services Agreements
  - Processing activities
  - CCPA service providers
  - GDPR processor
  - Other jurisdictions
  - Governance process
- Cross-border transfers
  - Model Clauses
  - BCRs
  - Shield
- Data transfer agreement
  - C2C considerations



Hogan Lovells

Works Council Consultations

- Coordination and collaboration with works councils for employee data transfers
- Where the deal is sensitive from an HR standpoint, works councils will be the front-line enforcers
  - Under applicable national laws, works councils may have consultation or co-determination rights
  - As a best practice, assume that works councils will be vigilant regarding data protection in connection with employee data
- Transfers of HR data to the US or Asia are highly sensitive because of Snowden effect
  - Some German "shop agreements" may prohibit transfers without works council approval
- For sensitive deals, Seller needs an "accountability package" ready to show works councils to demonstrate Seller's compliance

Hogan Lovells

Communications to Employees

- Depending on the jurisdiction, there may be restrictions on transfers of employee data
- Update employee notices to include disclosure of HR data in the context of a corporate transaction, such as merger or sale of assets
  - Personal data may be shared with parties to a transaction, may be transferred outside of the jurisdiction
  - Existing references to potential disclosure in the context of corporate transaction may be sufficient
  - Employees may have a right to object
- Timing of notice
  - Before personal data is shared in the context of the merger
  - Considerations for later notice (e.g. insider trading)
- Consent requirements for transfers of sensitive data
  - EU regulators have determined that consent in the employment context should not be relied on, as it may not be deemed to be "freely given" due to hierarchic relationship in the employment context
  - Without consent, transfer and/or disclosure of sensitive personal data may be a violation of the GDPR
  - Redact or anonymize any sensitive HR data, avoid disclosing if not possible
  - After closing, sensitive data could potentially be transferred under other GDPR provisions, e.g. Article 9 (2)(b)
- Status of employee data under the CCPA

After the deal

Communications

- On a business sale, transfer of personal data on completion will lead to change of “controller”
- The new controller needs to identify itself to impacted individuals within a reasonable time.
- Separate notice may also be given by the seller.
- The seller may wish to agree the content of the updated privacy notice with the buyer, to manage the risk of complaints

– There is no mechanism under EU anti-spam laws (the e-Privacy Directive) for transferring marketing consents on a business/asset sale.
– The seller may restrict under the deal terms the buyer’s use of marketing consents collected by the seller.
– Restrictions imposed by the seller (e.g. branding; frequency of marketing; subject-matter of marketing) may reduce risk of complaints.

– The seller and buyer may share a common consumer-base post-deal.
– Parties may agree a process for dealing with Q&A from consumers, which reflects allocation of responsibility for dealing with issues: “your watch” vs “my watch”.

Separation activities

Data migration

- How to identify data to transfer from seller to buyer…
- Dedicated vs. shared systems
- Un-structured vs. structured datasets
- Data protection risks associated with retaining or disclosing excess data
- Risk-mitigation through on-going controls (e.g. monitoring; audit; training)
- Risk mitigation vs. cost
- “Wrong-pockets” clauses, e.g. on-going information sharing arrangement

TSA cutover

- Transferring vs. non-transferring systems
- Ensuring compliance with data privacy principles, e.g. under GDPR on security, data minimisation and purpose limitation
- Seller obligation to delete, restrict use of or secure business data held on retained systems; buyer obligation to delete, restrict use of or secure retained business data held on transferred systems

Integration activities

Integrating programs

- Integrating a target business into the buyer's privacy program…
  - Privacy notices
  - Governance
  - Policies and procedures
  - Training
  - Intra-group agreements
- Pros and cons of integration versus keeping a target business at arm's length
- Managing information security risks (e.g. risk of data breaches) across combined buyer and target IT estate

Risks

- Combining datasets (e.g. pooling consumers) across business…
- Business potential to realise value from combined datasets, e.g. to access additional consumers, to derive additional insights about consumers or to exploit commercial relationships
- Tension with data privacy principles: e.g. under GDPR, transparency, purpose limitation and legal basis (consent/legitimate business purpose)

Thank You

Avi Gesser
Davis Polk & Wardwell
avi.gesser@davispolk.com

Scott T. Loughlin
Hogan Lovells US
scott.loughlin@hoganlovells.com

Nigel Parker
Allen & Overy
nigel.parker@allenovery.com