imaa
Institute for Mergers, Acquisitions & Alliances

M&A Due Diligence

Data Privacy Checklist

1. INVENTORY ALL DATA ASSETS:

- [ ] Identify all data assets held by both the acquiring and target companies.
- [ ] Categorize data based on sensitivity, such as personally identifiable information (PII), financial data, health information, etc.

2. ENSURE REGULATORY COMPLIANCE:

- [ ] Determine the applicable data privacy regulations (e.g., GDPR, CCPA, HIPAA) and ensure both companies are compliant.
- [ ] Review the target company's privacy policies, consent management practices, and data breach response procedures.

3. REVIEW DATA GOVERNANCE FRAMEWORK:

- [ ] Assess the target company's data governance framework, including data ownership, access controls, and data retention policies.
- [ ] Evaluate data classification practices and the implementation of appropriate security measures (encryption, access controls, etc.).

4. SCRUTINIZE DATA PROCESSING ACTIVITIES:

- [ ] Understand the purpose and legal basis for collecting and processing personal data.
- [ ] Review data processing agreements with third parties and ensure compliance with contractual obligations.

5. ASSESS DATA PROTECTION MEASURES:

- [ ] Evaluate the target company's data protection measures, including security policies, employee training, and incident response plans.
- [ ] Assess the effectiveness of technical safeguards, such as encryption, pseudonymization, access controls, and data backup procedures.

6. VERIFY DATA TRANSFER COMPLIANCE:

- [ ] Determine if the target company transfers data internationally and assess compliance with cross-border data transfer regulations.
- [ ] Review the existence and validity of Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) for data transfers, if applicable.

7. REVIEW DATA SUBJECT RIGHTS PROTOCOLS:

- [ ] Review how the target company handles data subject rights requests (e.g., access, rectification, erasure) and ensure compliance with applicable regulations.
- [ ] Assess the processes for obtaining and managing consent for data processing activities.

8. INVESTIGATE DATA BREACHES AND NOTIFICATIONS:

- [ ] Evaluate the target company's history of data breaches and incident response procedures.
- [ ] Assess the effectiveness of breach notification practices, including timely reporting to relevant authorities and affected individuals.

9. PERFORM VENDOR DUE DILIGENCE:

- [ ] Review third-party vendor relationships, including data processors and cloud service providers.
- [ ] Assess the target company's due diligence process for selecting and monitoring vendors for data privacy compliance.

10. EVALUATE DATA PRIVACY CULTURE:

- [ ] Evaluate the target company's privacy awareness programs, employee training, and privacy governance structure.
- [ ] Assess the integration of privacy-by-design principles in product development and business processes.

11. CONFIRM DOCUMENTATION AND RECORD-KEEPING:

- [ ] Ensure the target company maintains proper documentation, including privacy policies, consent forms, data processing agreements, and records of data processing activities.
- [ ] Evaluate data classification practices and the implementation of appropriate security measures (encryption, access controls, etc.).

12. DEVELOP A REMEDIATION PLAN:

- [ ] Identify any deficiencies or non-compliance areas and develop a remediation plan to address them post-merger/acquisition.
- [ ] Assign responsibility for implementing necessary changes and ensure a timeline for resolution.