

## DATA PRIVACY AND SECURITY PRE-DILIGENCE ANALYSIS

The following lists some of the key areas of analysis we can perform in preparing for future acquisition or investor diligence.

Data Map	<ul style="list-style-type: none"><li>• Evaluate target company's information collection, use and disclosure practices</li><li>• Identify data privacy and security laws applicable to target company and gaps in their compliance</li><li>• Evaluate risks based on types of personal data collected (e.g., health data, children's data, sensitive data)</li><li>• Review whether target company transfers data across borders and if they comply with applicable data localization laws</li></ul>
Privacy Policy	<ul style="list-style-type: none"><li>• Review whether target company's public-facing privacy policy accurately describes its information collection, use and disclosure practices</li><li>• Review whether target company is providing appropriate privacy notices to its job applicants, employees and contractors</li><li>• Evaluate risk of liability based on target company's public and internal privacy policies</li></ul>
Vendors	<ul style="list-style-type: none"><li>• Identify all vendors used by target company</li><li>• Evaluate whether target company properly vetted vendors for data privacy and security issues</li><li>• Review vendor contracts to ensure appropriate data privacy and security terms included</li><li>• Assess whether target company has entered into appropriate contracts with vendors if there is a cross-border data transfer</li></ul>
Privacy Requests	<ul style="list-style-type: none"><li>• Evaluate target company's procedures and protocols for responding to data subject privacy requests (e.g., request to delete, access or correct personal data and opt-out of sale)</li><li>• Assess whether target company has failed to properly authenticate the identity of data subjects and/or not responded to prior requests</li></ul>
Cybersecurity	<ul style="list-style-type: none"><li>• Assess whether target company has implemented appropriate security measures to safeguard data</li><li>• Review whether target company has adequate cybersecurity insurance for data breach coverage</li><li>• Evaluate if the target company has experienced data breaches in the past, how they responded to the data breaches, and whether they provided appropriate notices to data subjects and/or enforcement authorities regarding the data breaches</li></ul>

If you have any questions, please feel free to contact Susan M. Natland, Jessica C. Sganga or Arsen Kourinian at Knobbe Martens.