The opportunity value of compliance

Multinational companies are increasingly holding local business partners accountable for compliance with the anti-bribery and corruption, sanctions, personal data privacy, and other laws that apply to their business and operations. As a result, many business relationships and transactions cannot start until the required compliance agreements and assurances have been made. For example, signing a supplier code of conduct has become a mandatory requirement for many supplier registration processes. To open a bank account, customers must complete a Know Your Customer questionnaire. To obtain financing, receive sensitive technology, and transfer personal data, customers must agree to special-purpose agreements and compliance terms and conditions. In a global economy, companies with effective compliance programs will be better prepared for the compliance requirements of business partners, giving them greater access to commercial opportunities. This article explains common requirements, obligations, and consequences of the compliance certifications, representations, and agreements required by business partners.

Supplier Codes of Conduct

Supplier Codes of Conduct (SCOC) are commonly used to ensure third-party compliance with anti-bribery and corruption (ABAC) laws by prohibiting bribery, corruption, and unlawful conduct. They can be used to require compliance with specific laws like the US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and other relevant laws and obligations. They can also be used to extend ABAC obligations to a supplier's subsidiaries, affiliates, contractors, agents,

and representatives. SCOCs have also been used to require the establishment of policies, monitoring compliance, and reporting bribery and unlawful conduct.

Companies need to understand what ABAC laws require to avoid the termination of a business relationship or being blocked from future transactions. ABAC laws generally prohibit the offer or acceptance of any form of payment, loans, privileges, benefits, and anything of value to induce behavior or gain an improper advantage. "Anything of value" is broadly defined to include gifts, meals, and entertainment, sponsored travel, and charitable donations. ABAC laws also require integrity due diligence for transactions with government officials and third parties. To effectively comply with ABAC laws and obligations, companies need to establish policies, procedures, and tools designed to prevent bribery and corruption and monitor the giving and receiving of gifts, meals, and entertainment, sponsored travel, and charitable donations. They also need policies, procedures, and tools for conducting integrity due diligence on transactions with government officials and third parties.

KYC Questionnaires and Credit Agreements

Know Your Customer (KYC) policies and procedures support compliance with ABAC obligations as well as sanctions obligations. For ABAC obligations, KYC policies and procedures demonstrate how due diligence is used to confirm that potential customers are not individuals or entities known for corruption, suspected of crimes, at risk of bribery or money laundering, or politically exposed. For sanctions, international financial institutions use KYC questionnaires to collect information required to ensure that potential customers are not restricted parties, owned or controlled by restricted parties, or from restricted countries. Financial institutions also use credit and loan agreements to prohibit borrowers from providing US and EU funds, resources, and assets to restricted individuals or entities or using them for restricted purposes.

Credit and loan agreements facilitate compliance with sanction laws by requiring borrowers to represent that they are not a sanctioned party, owned by a sanctioned party, or from a sanctioned country. These representations can be extended to the borrower's shareholders, directors, officers, and employees, including their subsidiaries, affiliates, contractors, agents, and representatives. Credit and loan agreements can require compliance with specific sanction laws such as those administered by the US Office of Foreign Assets Control (OFAC), under the UN Security Council Resolutions, or the European Union. They can also require representations and warranties that the borrower will not use the funds to breach sanctions. The borrower will not repay the funds from the proceeds of sanctioned activities; there are no pending sanction investigations against the borrower, and the borrower has policies and procedures to comply with sanction laws and obligations. To effectively comply with sanctions obligations and avoid triggering a default, accelerated repayment, and being denied access to financial services, companies will need policies and procedures for identifying and screening relevant individuals and entities against sanctioned party and country lists.

Special purpose agreements

End-Use certifications are used to facilitate compliance with the export control laws that apply to sensitive US and EU origin goods, services, and technology. Sensitive items require a license to export that must be supported by an end-user certification that has been signed by the foreign recipient (i.e., the end-user). The end-use certificate defines who can have access to the sensitive items and how they can be used. To provide a knowing certification, the foreign recipient must have policies and procedures to identify the nationalities of all individuals who might have access to the sensitive items. They will also need procedures for identifying, recording, marking, and monitoring sensitive items and facilities, systems, and procedures for restricting access to sensitive items to authorized persons for authorized uses.

Data transfer agreements are used to ensure that personal data is transferred to personal data recipients with the enforceable data subject rights and legal remedies required by relevant personal data privacy laws and obligations. For example, under the GDPR, standard data protection clauses are a legally authorized methods for transferring personal data from the EU to countries outside the EU.[1] Even the Kingdom of Saudi Arabia now requires public entities to use data sharing agreements[2] to share government-produced data with anyone. Data Sharing agreements set forth the purpose for sharing, the individuals authorized to access data, and the security measures that apply to all parties involved in the Data Sharing. As multinational customers increasingly require business partners to implement "functional privacy programs"[3] in this increasingly data-driven economy, companies will need policies and procedures for collecting and processing personal data, sharing personal data, and responding to breaches involving personal data.

Conclusion

The need to prepare for compliance is growing as multinational companies continue to hold local business partners and customers accountable for the regulatory obligations that apply to their business and operations. Companies with effective compliance programs will be able to maintain existing business relationships and pursue additional regional and international opportunities. Their ability to comply with loan and credit terms and conditions will give them greater access to international financing. They will have less trouble transferring personal data across borders to facilitate the international trade of goods and services. And for companies in need, they will be able to acquire sensitive items and technology from US or EU vendors.

---

[1] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. Chapter 5, Article 46(2)c and d

[2] KSA National Data Governance Regulations, Clause 6.3(8).

[3] Waterman, D, The Rise of Data Protection Compliance as a Risk – What Executives in the Middle East Need to Know, White Label Consultancy, June 3, 2021, from https://whitelabelconsultancy.com/2021/06/the-rise-of-data-protection-compliance-as-a-risk-what-executives-in-the-middle-east-need-to-know/

EMME Advisory Services

EMME Advisory Services (EMME) was established to help companies in the Middle East and emerging markets identify and build the programs necessary to comply with relevant regulatory compliance risks, obligations, and expectations. Before establishing EMME, Granville Collins was responsible for building the Saudi Aramco programs necessary to comply with multinational regulatory compliance obligations, business partner requirements and expectations, and the Kingdom's developing regulatory regime. With the access, observations, and knowledge that comes from twenty years of working for Saudi Aramco in Saudi Arabia, EMME has developed a deep understanding of the operational needs for compliance in the Middle East. For more information contactus@emme-advisory.com or visit www.emme-advisory.com.