View this email in your browser

Compliance Updates

May 19, 2020

This update identifies recent developments in the field of compliance, including the transition to "working from home" policy implemented in many places on account of the COVID-19 pandemic and its ongoing effects; the amendments to US regulations applying to the export of items for military applications in China, Russia and Venezuela; and the evolving zero tolerance stance of the Department of Justice ("**DOJ**") towards financial institutions facilitating corruption, money laundering or any other criminal activities.

Cyber

The COVID-19 pandemic has had an unprecedented impact on businesses all around the world. The first wave of COVID-19 may be nearly behind us, however the possibilities it created for companies to work from home and use videoconferencing tools in an effective manner are vast. The option of effectively working from home will become useful if another quarantine is warranted, however, if it proves itself, working from home may become a viable possibility regardless of the current pandemic.

With all the positive aspects of working from home, it comes with many cyber risks. According to Check Point Software Technologies ("**Check Point**"), there are approximately 2,600 cyberthreats and around 200 fraudulent sites that appear to be connected to the COVID-19 pandemic every day. The shift to work-from-home technologies included large-scale use of videoconferencing services, collaboration platforms and other digital tools. Check Point reports that approximately 1,700 fraudulent sites offered videoconferencing services. Cyber-attackers are constantly searching for vulnerabilities, resulting in exploitation of weak websites and the sending of malware and phishing both in emails and via WhatsApp. Many of these

attacks use COVID-19 related issues.

The shift to working from home needs to be accompanied by cyber security teams and chief information security officers ("CISOs") understanding the extent of the exposure to these new cyberthreats and the need to protect their companies while enabling the business to work smoothly and without interruptions. In light of the COVID-19 pandemic, the Israel National Cyber Directorate (INCD) has issued guidelines for minimizing the risks associated with remote work for organizations and businesses, and CISOs should review and familiarize themselves with them. Additionally, CISOs will have to adapt themselves to the changes and this could be done efficiently if they focus on the technology, services and security features that are critical to the activities of the company; adopt cybersecurity risk policies (such as incident response plans, disaster recovery and specific guidance to the employees) and test their efficiency. Once these policies are set up, it is also necessary to ensure constant monitoring of the Company's compliance with them. If these practices are adopted, companies can adjust to the transition to working from home while remaining effective and alert to the existing cyberthreats. Our compliance team would be pleased to assist in strengthening your company's cybersecurity resilience.
To read the INCD's guidelines (in Hebrew) click here.

Export

BIS expands export controls applying to items intended for military applications in China, Russia and Venezuela

On April 20, 2020, the US Department of Commerce, Bureau of Industry and Security ("BIS") expanded Section 744.21 of the Export to the Administration Regulations ("EAR"), imposing the same licensing requirements for export for "military use" "and military end users" applying to Russia and Venezuela, on China as well. The definition of "military end use" now includes "supporting" or "contributing" to the operations, and "maintenance", "repair", "overhaul", "refurbishing", "development" or "production" of military items for all three countries. If any of these elements apply to the export in question, that would be sufficient to violate the new regulations. In addition, new items were added to the categories of materials processing, electronics, telecommunications, information security, sensors and lasers and propulsion that are subject to licensing requirements under Part 744, Supplement No 2. There was also an expansion of the EEI filing requirement. Lastly, BIS annulled License Exception CIV. License Exception CIV permitted exports, reexports and in-country transfers of items on the Commerce Control List (CCL) requiring a license in relation to Country Group D:1 for national security reasons only, provided that the items were intended for civilian end users and civil uses only.[1]

In light of these amendments, it is most probable that BIS will not grant export licenses for these items, and companies will be required to determine whether their dual-use goods are listed in Part 744, Supplement No 2. If they are, the companies will be required to conduct enhanced due diligence in the evaluation of who is the end user (ensuring that no Chinese military entity is an end user, including national armed services, national guard, national police or government intelligence). Additionally, it will not be sufficient to know the immediate use of their product or technologies. Companies will need to evaluate whether there is a possibility that their product or technology could support or contribute to any military use when exporting to China, Russia and Venezuela. This enhanced due diligence may be required for items that were not subject to any export license requirements prior to the amendments.

Money Laundering and Corruption

On April 30, 2020, Bank Hapoalim B.M ("**BHBM**") and Bank Hapoalim (Switzerland) Ltd ("**BHS**"), reached an agreement with the Department of Justice of the Eastern District of New York (the "**DOJ-ENY**") for their role in a money laundering conspiracy. The agreement includes a three-year non-prosecution agreement and an undertaking to forfeit $20,733,322 and pay a fine of $9,329,995 to resolve an investigation into the banks' involvement in a money laundering conspiracy that enabled international soccer bribery. The agreement was reached based on the banks' complete cooperation, and BHBM's undertaking to update its AML program and to close branches in Miami and Latin America, amongst others.

In this case, the DOJ-ENY's stance was made clear and it declared that it is committed to holding financial institutions accountable, when they knowingly facilitate corruption or other criminal activities. The banks admitted to conspiring to commit money laundering in an amount of over $20 million, involving bribes and kickbacks to soccer officials to steer broadcasting rights for soccer matches and tournaments to the sport marketing executives. Said kickbacks and bribes were given to officers in the Fédération Internationale de Football Association ("FIFA") and other soccer organizations. BHBM admitted to allowing illicit activities to continue, after employees had discovered and reported them. This new shift toward accountability of financial institutions and the heavy penalties attached thereto, set a potential new standard of enhanced due diligence of financial institutions clients' accounts to verify that they are not facilitating criminal activities.
To read the DOJ-ENY's announcement click here.

In addition, in the federal arena, BHBM and BHS entered into a Deferred Prosecution Agreement for Criminal Misconduct ("**DPA**") with the DOJ. BHS pleaded guilty and charges were filed against BHBM for conspiring with US taxpayers and others to hide more than $7.6 billion in more than 5,500 secret Swiss and Israeli bank accounts. According to the DPA, the BHBM and BHS are required to fully cooperate with ongoing investigations and disclose information it may later uncover regarding US-related accounts. BHBM will pay a total of $214 million ($77,877,099 in restitution to the IRS, $35,696,929 forfeit to the US and $100,811,585 as penalty). BHS will pay $402.53 million ($138,908,073 in restitution to the IRS, $124,628,449 forfeit to the US and $139,998,399 as penalty). Since 2008, this DPA is the second-largest recovery by the DOJ in connection with its investigations of tax evasions by foreign banks.
To read the DOJ's announcement click here.

If you have any questions or would like to receive any assistance regarding the matters discussed in this update, please call Meitar's compliance team.

---

[1] To date, Country Group D:1 consists of Armenia, Azerbaijan, Belarus, Cambodia, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Mongolia, Moldova, North Korea [also subject to U.S. embargo] Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Venezuela, Vietnam, and Yemen.

Contact Information

Yuval Z. Sasson, Partner
+972-3-6103190
ysasson@meitar.com

Dr. Shimrit Itay-Horev, Associate
+972-3-6103100
shimriti@meitar.com

Rotem Raybee, Associate
+972-3-6103100
rotemr@meitar.com

For additional information about our firm's Cross Border Compliance group, click here.

To join our newsletter click here

Meitar | Law offices
16 Abba Hillel Silver Road, Ramat Gan, 5250608, Israel | +972-3-6103100