אם אינך רואה מייל זה לחץ כאן

מגמות גלובליות בתחומי ציות, אכיפה, יצוא בטחוני וסייבר

27 באפריל, 2023

בתקופה האחרונה חלו מספר התפתחויות גלובליות בתחומי הפעילות של מחלקת ציות בינלאומי, אכיפה, יצוא ביטחוני וסייבר. ריכזנו לנוחותכם את עיקרי הדברים, ואנו מגישים לכם את תמצית העדכונים.

1. עדכון נוהל הערכת תכניות הציות של משרד המשפטים האמריקאי
במרץ 2023 עדכן משרד המשפטים האמריקאי (ה-"**DOJ**") את נוהל הערכת תכניות הציות שלו (Evaluation of Corporate Compliance Programs) המשמש כמדריך לפיו בוחן ה-DOJ את תכנית הציות של חברה כחלק מהשיקולים בנקיטת הליך פלילי נגד החברה וגורמים בה. הנוהל, לפיכך, הפך למדריך לחברות בנוגע לבניית תכנית ציות אפקטיבית וכוללת. בעדכון האחרון, עדכן ה-DOJ את הפרק בנוהל הנוגע לשימור ותיוק תקשורת פנימית וחיצונית בחברה. העדכון מראה כי ה-DOJ סבור כי יש לתת דגש משמעותי על נושא זה בעת בחינת תכנית הציות של החברה והתנהלותה בפועל.

ניסיונות ראשונים של ה-DOJ לגעת בסוגיה עלו כבר בשנת 2017, ונתקלו כבר אז בהתנגדות מצד חברות. עיקר הבעיה, כפי שהציגו זאת אותן חברות כבר ב-2017, הוא כי ה-DOJ לא לוקח בחשבון את העובדה כי תקשורת בחברות רבות כבר אינה מתנהלת באמצעים "פורמליים" בלבד (כגון דואר אלקטרוני או פקסים), אלא גם באמצעות תוכנות שליחת מסרים מיידיות, כגון WhatsApp, Signal או Telegram, או על גבי פלטפורמות ורשתות חברתיות כגון Facebook ו-LinkedIn. יצירת תיעוד עקבי של התקשורת בחברה באמצעים אלו הוא קשה עד כדי בלתי אפשרי. החברות התריעו כבר ב-2017 כי אין להן את היכולת האפקטיבית למנוע מהעובדים לתקשר עם לקוחות, ואחד עם השני, באמצעים אלו. כעת, שב ה-DOJ להתייחס לסוגיית תיעוד התקשורת, אך מבלי להתייחס לסוגייה של תוכנות שליחת מסרים מיידיות – וטרם ברור כיצד יילקח בחשבון הפער הקיים בין גישת ה-DOJ לבין המציאות בשטח.

אנו ממליצים ללקוחותינו לשקול את נושא התנהלות התקשורת הפנימית והחיצונית בחברותיהם, ולקבוע בנהלי החברות את אופן התנהלות התקשורת בחברה, שימוש במכשירים אישיים לעומת כאלו המונפקים על ידי החברה, ועוד. אנו ממליצים להגדיר במפורש באילו אמצעים על התנהלות החברה להתבצע, ולשאוף כי אלו יהיו אמצעים אשר ניתן לתעד, כגון דואר אלקטרוני, או תוכנות מסרים המיועדות לסביבת עבודה כגון Teams, Slack, וכדומה. יש לפרוט בפני העובדים בצורה ברורה אילו התקשרויות מותר ואילו אסור לבצע באמצעי תקשורת לא-פורמליים.

אנו זמינים לכל שאלה בנוגע לבניית תכניות ציות, הדרכות לעובדים על תחומי ציות שונים, וחקירות (פנימיות וחיצוניות) בעקבות אירועי הפרה פוטנציאליים.

לקריאה של הנוהל המעודכן ניתן ללחוץ כאן.

2. עדכון רשימת וואסנאר

מדינת ישראל מסדירה את הפיקוח על יצוא של ציוד ביטחוני, העברת ידע ביטחוני ועל מתן שירות ביטחוני באמצעות חוק הפיקוח על יצוא ביטחוני, תשס"ז-2007. מתוקף החוק הוצא צו הפיקוח על יצוא ביטחוני (ציוד דו–שימושי מפוקח), התשס"ח – 2008, אשר קובע כי פריטים המנויים ב- Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("**רשימת וואסנאר**"), ואשר נועדו לשימוש ביטחוני, נחשבים כציוד דו-שימושי מפוקח. במקביל לכך, צו היבוא והיצוא (פיקוח על יצוא טובין, שירותים וטכנולוגיה דו-שימושיים), תשס"ו-2006 קובע את אופן הפיקוח על ציוד המופיע ברשימת וואסנאר אך אינו מיועד לשימוש ביטחוני. רשימת וואסנאר מתעדכנת מדי שנה, והעדכון האחרון התפרסם ב-1.12.2022.

העדכון האחרון כלל בעיקר שינויים בקטגוריות 6, 8 ו-9 של הרשימה, הנוגעות לחיישנים ולייזרים, לציוד ימי, ולציוד לתעשיות האוויר והחלל, בהתאמה. כמו כן, נערכו שינויים ברשימת החימושים (Munitions List) הכלולה ברשימת וואסנאר. לבסוף, כדאי לשים לב לכך שההגדרה למה היא "Intrusion Software" שונתה קלות, כך שההגדרה מעט יותר מרחיבה מבעבר. יחד עם זאת, טרם נראה כי יש ביטוי לשינוי הגישה של הממשל האמריקאי כלפי תחום הסייבר ההתקפי (כפי שזו משתקפת מהודעת הנשיא ביידן הנזכרת מטה). עם זאת, ניתן להניח כי בעתיד הקרוב אנחנו עשויים לראות מדינות מערביות נוספות , כגון מדינות האיחוד האירופי, מאמצות גם הן גישה דומה ואולי אף מחמירה יותר. לפיכך, נמליץ ללקוחותינו העוסקים בתחום לבחון האם הם נדרשים לשינוי או עדכון של פעילותם בעקבות דברים אלו. אנו כמובן נשמח לסייע ולענות על כל שאלה.

קישור לרשימת וואסנאר המעודכנות ניתן למצוא כאן. קישור לסיכום השינויים בין הרשימה הנוכחית לזו הקודמת ניתן למצוא כאן.

3. קביעת תהליך ומנגנון לבחינת היבטי ביטחון לאומי בהשקעות זרות

ביום 12.10.2022, ועדת השרים לענייני ביטחון לאומי ("הועדה") פרסמה החלטה שקבעה הליך ומנגנונים לבחינת היבטי ביטחון לאומי של השקעות זרות. כבר באוקטובר 2019, הוועדה הקימה ועדה מייעצת להערכת החששות הפוטנציאליים שהשקעות זרות עלולות לעורר ביחס לאינטרסים של ביטחון לאומי ("**הועדה המייעצת**"). מכוח ההחלטה מ-2019, חברי הועדה המייעצת הם נציגי משרד האוצר, המועצה לביטחון לאומי ומשרד הביטחון. בהחלטה מאוקטובר 2022 נוסף נציג משרד החוץ כחלק מהועדה המייעצת.

ההחלטה מאוקטובר 2019 קבעה כי הרגולטורים – בנק ישראל, רשות ניירות ערך, רשות שוק ההון, ביטוח וחיסכון, משרד האוצר, וכן הגורמים במשרד התחבורה והבטיחות בדרכים, משרד התקשורת ובמשרד האנרגיה המוסמכים על פי דין להעניק אישור להשקעה זרה – היו יכולים לפנות לוועדה המייעצת כדי לקבל את עמדתה בעניין ההשקעה, ובמקרים חריגים בהם הועדה המייעצת סבורה כי קיים חשש כי השקעה זרה עלולה לפגוע באינטרסים של הביטחון הלאומי, רשאית הועדה המייעצת לבקש מהרגולטור למסור את עמדתה בעניין ההשקעה.

ההחלטה מאוקטובר 2022 מחזקת את עמדתה של הוועדה, ומעניקה לה סמכויות

נוספות המאפשרות לה לפנות מיוזמתה לרגולטורים שונים ולבקש מהם למסור לה מידע על השקעות זרות קיימות וצפויות ועל מאפייני הענף הרלוונטי, לצורך גיבוש עמדותיה ומסקנותיה.

לפי ההחלטה מאוקטובר 2022, "גורם זר" הוא מי שאינו אזרח או תושב ישראלי (לגבי יחיד), ולגבי "חבר בני אדם" (כלומר חברה או ישות אחרת) גורם זר הוא מי ששליטה בלפחות 20% מאמצעי השליטה בו היא בידי מי שאינו אזרח או תושב ישראלי. במקרים חריגים בהם סבורה הועדה המייעצת כי קיים חשש לפגיעה משמעותית באינטרסים בהיבטי ביטחון לאומי, חבר בני אדם שאדם שאינו תושב או אזרח ישראלי הוא "בעל עניין בו" ייחשב גם כן כגורם זר.

להרחבה ניתן לקרוא את ההחלטה המלאה של ועדת השרים לענייני ביטחון לאומי מיום 12.10.2022 כאן.

4. עדכון סנקציות והגבלות יצוא עקב הפלישה הרוסית לאוקראינה
ב-24 בפברואר ציינו שנה לתחילת הפלישה הרוסית לאוקראינה וללחימה שלצערנו נמשכת עד היום. לקראת מועד זה, ממשלות וגופים בינ"ל שונים עדכנו את משטרי הסנקציות הנרחבים שהוטלו עד כה על רוסיה, בלארוס ומדינות נוספות. לאור ציון דרך זה והמשך הלחימה באזור, משטרי הסנקציות המרכזיים השיתו סנקציות נוספות על חברות ואישיים רוסיים:

<u>האיחוד האירופי</u>
ב-13.4.2023 עדכן האיחוד האירופי את משטר הסנקציות שלו על רוסיה בעקבות פעולותיה באוקראינה. בעדכון האחרון התווספו לרשימת הסנקציות האירופאית גם קבוצת 'וואגנר' כולה (לאחר שבעדכון הקודם התווספו לרשימה מספר ממפקדיה), וכן חברת תקשורת אשר בראש חבר הנאמנים שלה עומד יבגני פריגוז'ין, העומד גם בראש קבוצת 'וואגנר'. נכון להיום, האיחוד האירופי מטיל הגבלות על 1473 אינדיבידואלים ו-207 גופים בעקבות הלחימה בין רוסיה ואוקראינה. נזכיר, כי ביום 25.2.2023 אישר האיחוד האירופי את חבילת הסנקציות העשירית נגד רוסיה. סנקציות אלו כללו הגבלות על ייצוא טכנולוגיות רגישות לרוסיה, הגבלות על ייבוא של אספלט וגומי סינטטי, אספקת שירותי אחסון גז לרוסיה, והגבלות על העברה דרך רוסיה של טכנולוגיות דו-שימושיות שיוצאו מאירופה. בנוסף, האיחוד האירופי השעה את רשיונות השידור של ערוצי הטלוויזיה RT Arabic ו-Sputnik Arabic, הטיל הגבלות על אזרחים רוסים המונעות מהם לשאת תפקידים בגופים של האיחוד האירופי הנוגעים לתשתיות קריטיות, וכן הטיל סנקציות נוספות על 87 יחידים ו-34 חברות, ובכללם גורמי צבא בכירים, מפקדים בכירים של 'קבוצת וואגנר' כאמור, ויצרני מל"טים.

עוד נזכיר שבמסגרת חבילת הסנקציות הקודמת, אשר אושרה בספטמבר 2022, האיחוד האירופי אסר אספקת שירותי פרסום, מחקר שוק וסקרי דעת קהל, ושירותים נוספים לרוסיה (ובכלל זה הן לממשלת רוסיה והן לחברות וגופים שהוקמו ברוסיה). בנוסף, האיחוד האירופי גם הוסיף פריטים חדשים לרשימת הפריטים האסורים לייצוא לרוסיה, ובכללם מזל"טים שמיועדים לשמש כצעצועים/לתחביבים (ושאינם לשימוש מקצועי), גנרטורים, מחשבים ניידים ורכיבי מחשוב, מערכות ניווט רדיו, מנועי מטוסים וחלקי מנועים, מצלמות ועדשות, ועוד.

<u>בריטניה</u>
גם בריטניה הודיעה ב-24/02/2023 כי היא מעדכנת את משטר הסנקציות שלה, ומוסיפה איסורי מסחר וייצוא לרוסיה על "כל פריט אשר התגלה כי רוסיה משתמשת בו בשדה הקרב", ופריטים רבים נוספים; הוספה של עשרות יחידים וחברות לרשימת הסנקציות הבריטית, וביניהם שרים בממשל הרוסי ובכירים בחברות ממשלתיות או הקשורות לממשל כגון GAZPROM ו- Aeroflot. כמו כן, נוספו מספר בנקים רוסיים לרשימת הסנקציות.

בריטניה גם מחריפה את הסנקציות וההגבלות על המסחר עם חצי-האי קרים, ועל האזורים האוקראיניים שבשליטת רוסיה – Donetsk, Luhansk, Kherson ו- Zaporizhzhia.

<u>ארה"ב</u>
ב-24.02.2023 הוציא ה-Office of Foreign Assets Control (OFAC) אשר פועל תחת

משרד החוץ האמריקאי עדכון של הסנקציות האמריקאיות כלפי רוסיה. בין העדכונים ניתן למנות סנקציות בתחומי הכרייה של מתכות ואבנים יקרות וכן על מספר חברות רוסיות מרכזיות בתחום; הוספה של 11 בנקים רוסיים נוספים לרשימת הסנקציות של OFAC; הוספה של עשרות חברות ויחידים לרשימות הסנקציות של OFAC, בדגש על כאלו הנוגעים לניהול הון ואשר מסייעים ליחידים וחברות ברוסיה לחמוק מהסנקציות הקיימות.

מאידך, ב-08.3.2023 הודיע OFAC כי הוא מסיר מספר בנקים הקשורים לתאגיד הבנקאות SBERBANK מרשימת הסנקציות שלו. יחד עם זאת, נדגיש כי מניסיוננו תאגידים בנקאיים רבים מסרבים להעביר או לקבל כספים מתאגידים בנקאיים הנמצאים ברוסיה או בלארוס, אף כאשר אין אינדיקציה ישירה או משמעותית לקיומן של סנקציות עליהם. לפיכך, אנו עדיין ממליצים, ככל והדבר מתאפשר, לבחון קבלת והעברת תשלומים דרך תאגידים בנקאיים שאינם ממוקמים ברוסיה או בלארוס.

עוד נעדכן כי OFAC הכריז כי יינקטו 'סנקציות משניות' כנגד יחידים או חברות אשר מסייעים לממשל הרוסי, בין אם באופן ישיר בקשר ללחימה באוקראינה או בניסיון לחמוק מהסנקציות האמריקאיות או באופן עקיף דרך סיוע כלכלי. פירושן של הסנקציות המשניות הוא שיחידים או חברות שייקבעו כמסייעים לרוסיה כאמור יתווספו בעצמם לרשימת הסנקציות האמריקאית, וזו בלי קשר לשאלה אם החוק האמריקאי כלל חל עליהם או לא – מה שהופך את הסנקציות המשניות לנרחבות הרבה יותר.

אז מה יש לעשות?
ככל שחברה שוקלת לייצא לרוסיה או לייבא ממנה, ליצור קשרים כלכליים עם לקוחות/ספקים רוסיים או לקיים כל קשר עסקי אחר עם גורמים רוסיים עליה לפעול באופן הבא:

1. לבדוק האם הלקוח/הספק/הקשר העסקי מופיע באחת מרשימות הסנקציות;
2. לבדוק האם קיים קשר אירופאי/אנגלי/אמריקאי לעסקה (אם באמצעות עובדים בעלי אזרחות כפולה או חברות בנות באזור הרלוונטי);
3. אם קיים קשר אירופאי, אנגלי או אמריקאי, לבדוק האם המוצר/שירות נופל לתוך אחד ממגבלות הייצוא לפי הדין הספציפי החל.

אנו במחלקת האכיפה והציות של מיתר נשמח לסייע בניתוח השלבים האמורים, ובמידת הצורך להפנות את לקוחותינו למשרדים זרים שאנו עובדים איתם בצמידות בנושאים אלו לצורך קבלת חוות דעת מותאמות לדין המקומי הרלוונטי.

בנוסף, לשם ציות עם משטרי הסנקציות הגלובליים, אנו במחלקת האכיפה והציות מציעים סינון ובדיקה של לקוחות ושותפים עסקיים בטרם ההתקשרות באמצעות תוכנות מתקדמות המאפשרות סינון וניתוח לפי רשימות סנקציות בינלאומיות, מאגרי תקשורת ומידע עסקי. כמו כן, נשמח לסייע בגיבוש נהלי סנקציות המותאמים לצרכי החברה.

5. אבטחת סייבר

5.1. דיווח ל-FBI על אירועי סייבר

בחודש פברואר [פורסם בעיתון ה-Wall Street Journal] כי סוכני ה-Federal Bureau of Investigation (FBI) הצליחו להסתנן בחודשים האחרונים לקבוצת הכופרה (Ransomware) הידועה Hive, לאסוף מודיעין אודות אופן פעילותה ולשבש אותו. במסגרת איסוף המודיעין, גילו ב-FBI כי בכ-20% בלבד מאירועי הכופרה בהם הייתה מעורבת הקבוצה, פנו הקורבנות לרשויות האכיפה. ה-FBI מנסה כעת לשנות מגמה זאת, וקורא לחברות הנפגעות מהתקפות כופרה להודיע לו על כך, תוך שהוא מבטיח לסייע לנפגעים להתמודד עם המתקפה עצמה, התקשורת ואף רגולטורים. באותה נשימה, עם זאת, נזכיר כי ה-FBI התבטא בעבר וציין כי "לא ישמש כפרוקסי בין חברות לבין הרגולטורים המפקחים עליהן" בכל הנוגע לאירועי סייבר, כך שהיקף ההבטחות הנוגעות לרגולטורים לא ברור דיו. שאלת הדיווח לרשויות אכיפה אודות אירועי סייבר נמצאת כיום בבחינה של מחוקקים במדינות השונות, ועל אף שברוב המדינות לא קיימת חובה כזאת נכון להיום, זוהי סוגיה שחשוב לשקול ולתת עליה את הדעת במהלך מתקפת סייבר.

5.2. ממצאי ביקורת רוחב של הרשות לניירות ערך בנושא סיכוני סייבר

בתחילת שנת 2023 פרסמה הרשות לניירות ערך דוח ריכוז ממצאי ביקורת רוחב בנושא סיכוני סייבר בתאגיד מדווח שהופק לאחר ביקורת רוחב שערכה הרשות במהלך שנת 2022 כולה. הדוח מתמקד בתאגידים מדווחים שאינם כפופים לרגולטורים חיצוניים בתחום הסייבר (ובכלל) ולכן אינו מתייחס לגופים כגון בנקים, חברות ביטוח, חברות תקשורת וכדומה. הביקורת – והדוח שהופק בעקבותיה – מהווים המשך לגילוי הדעת המשפטי שפרסמה הרשות באוקטובר 2018 אשר נגע לחובות הגילוי בנושא סייבר. הרשות ציינה כי מסקנותיה, כפי שעולות מהדוח, ישולבו בגילוי דעת משפטי נוסף בנושא אשר צפוי להתפרסם בקרוב. נציג כמה ממסקנות אלו להלן.

ראשית, מבדיקת הרשות עולה כי קיימת מעורבות נמוכה של הדירקטוריון בחברות השונות בנושאי סייבר ואבטחת מידע – ב-90% מהחברות שנדגמו הדירקטוריון כלל לא אישר את נוהל אבטחת המידע, וב-70% מהחברות שנדגמו חברי הדירקטוריון כלל אינם מקבלים דיווחים עיתיים אודות הגנת הסייבר ואבטחת המידע בחברה, ואינם מקיימים דיונים רלוונטיים על כך. עוד עולה מהדוח כי ככלל, קיים קשר מועט בין מערך אבטחת המידע של החברות לבין ההנהלה – מה שהתבטא בחוסר בתוכניות עבודה סדורות ומיעוט בבקרה על ביצועיו של המערך על ידי גורמי ההנהלה הבכירים. הקשר המועט אף משפיע על הערכת הסיכון בקרב חברות אלו – כ-40% מהחברות שנדגמו כלל לא ביצעו הערכת סיכוני סייבר בשנים האחרונות, ולכ-80% מהחברות כלל אין תכנית סדורה לעריכת סקרי סיכונים.

לבסוף, מהדוח עולה כי רובן המוחלט של החברות אינן ערוכות – בפן הניהולי-משפטי – לקראת אירוע סייבר. ל-76% מהחברות אין כלל נהלים מתאימים להתמודדות עם אירועי סייבר (ובכלל זאת על דיווח אודות אירועי סייבר), לכמעט מחצית מהחברות אין צוות תגובה מגובש לניהול אירועי סייבר, וגם בחברות אשר מינו צוותים כאלו לא נערכים כלל תרגולים או הדרכות לצוותים אלו.

מהאמור בשתי הנקודות המפורטות לעיל, ניתן לראות כי חברות נוטות לנסות ולשמור את סוגיית אבטחת הסייבר וההתמודדות עם אירועי סייבר כעניין "פנימי" – אך זהו ניסיון שנועד לכישלון, שכן לחברות אין את הכלים והיכולת להכיל ולהתמודד עם אירועים כאלו לבד. רמת מוכנות נמוכה, יחד עם אי-דיווח על אירועים בעת האירוע, עשויים לגרום לנזק רב יותר מאירוע סייבר מאשר הנזק שהייתה החברה מתמודדת איתו מלכתחילה.

צוות הסייבר שלנו במיתר ישמח לסייע בהכנה לקראת אירועי סייבר על ידי גיבוש נהלים מותאמים לחברה ועריכת הדרכות ותרגולים לצוותי התגובה לאירועי סייבר; במתן סיוע משפטי צמוד ומקיף במהלך אירועי סייבר; במתן סיוע שוטף כחלק משיקום החברה, וכן ליווי צמוד במהלך הדיאלוגים עם הרגולטורים הרלוונטיים לאחר אירוע הסייבר.

6. פרסום מדיניות הממשל האמריקאי בעניין רכישה ושימוש ברוגלות מסחריות (Commercial Spyware) ופרסום ה-ECHRI's Code of Conduct

הממשל האמריקאי פרסם ב-27 למרץ, 2023 הודעה בעניין החלטתו של הנשיא ג'וזף ביידן על איסור רכישה ושימוש של הממשל האמריקאי ברוגלות מסחריות (Commercial spyware) המהוות סכנה לביטחון הלאומי האמריקאי. בהחלטה מציין הנשיא ביידן כי האיסור כולל רוגלות מסחריות אשר שימשו או משמשות לצורך מעקב אחר מחשבים או עובדים של הממשל האמריקאי; רוגלות מסחריות אשר שימשו לחשיפת מידע סודי של הממשל האמריקאי; רוגלות מסחריות הנמצאות בשליטת ממשלות זרות הפועלות נגד ארה"ב; רוגלות מסחריות אשר שימשו או משמשות ממשלות זרות לצורך מעקב אחר אקדמאים, עיתונאים, אקטיביסטים, ומתנגדי שלטון; וכן רוגלות מסחריות אשר נמכרות בידי חברות אשר מוכרות רוגלות מסחריות זהות או אחרות לממשלות אשר משתמשות בהן לצורך דיכוי פוליטי והפרות זכויות אדם משמעותיות אחרות.

ההגדרה של "רוגלה מסחרית" כוללת כל חבילת תוכנה שסופקה למטרות מסחריות, במישרין או בעקיפין באמצעות צד שלישי או חברת-בת, המספקת למשתמש בחבילת התוכנה את היכולת לקבל גישה מרחוק למחשב, ללא הסכמת בעליו או המשתמש בו, וזאת על מנת לגשת, לאסוף, לנצל, לחלץ, ליירט, לאחזר או להעביר תוכן, לרבות מידע המאוחסן או משודר באמצעות מחשב המחובר לאינטרנט, וכן על מנת

להשתמש במחשב לצורך הקלטת צליל או תמונה או איתור מיקומו של המחשב.

בבואם של גופי ממשל אמריקאיים לבחון האם רוגלה מסחרית מהווה סכנה לביטחון הלאומי האמריקאי, לפי הקריטריונים האמורים מעלה, עליהם יהיה לבחון האם החברה שמספקת את הרוגלה הייתה מודעת לקיומם של הקריטריונים האמורים, והאם היא נקטה צעדים כדי להסיר את הסיכון לביטחון הלאומי האמריקאי, או שיתפה פעולה עם הממשל האמריקאי בניסיונותיו למנוע שימוש לא ראוי ברוגלה. חשוב לציין כי ההחלטה מחריגה מספר שימושים מוצרים ברוגלות – ובעיקרם שימוש ברוגלות לצורכי ניסוי, מחקר, ניתוח, ופיתוח אמצעי הגנה מפני אותן רוגלות, וכן לצורכי חקירות פליליות הנובעות משימוש או מכירה לא-חוקיים ברוגלות.

לצורך הטמעת החלטה זו, יפיץ ראש המודיעין הלאומי האמריקאי (Director of National Intelligence) דו"ח פנימי המתבסס על חומרי מודיעין, מידע גלוי, מידע פיננסי, וכל מידע רלוונטי נוסף, ובו יפורטו מדינות, חברות ורוגלות מסחריות אשר עונות לקריטריונים המנויים מעלה. במידת הצורך, מספר מצומצם של בכירים בממשל האמריקאי (ביניהם ראש המודיעין הלאומי, ראש ה-CIA, וראש ה-NSA) רשאים להעניק רישיון זמני שתוקפו שנה אחת לשימוש ברוגלה מסחרית העונה לקריטריונים האמורים מעלה, אם הוא סבור שיש בכך "יוצא דופן". כמו כן, ההחלטה כוללת דרישות דיווח שונות: סוכנויות וגופי ביצוע של הממשל האמריקאי שמשתמשים כיום ברוגלות מסחריות ידרשו לערוך תוך 90 ימי מיום פרסום הדו"ח בדיקה פנימית של אותן רוגלות ושל השימוש בהן, ולפרט מדוע הן לא מהוות איום על הביטחון הלאומי האמריקאי, ומדוע הם סבורים שיש לאפשר להם להמשיך ולהשתמש ברוגלות מסחריות אלו – או להפסיק את השימוש בהן. לאחר מכן על הסוכנויות יהיה לערוך בדיקה זו באופן שנתי. הסוכנויות ידרשו גם לדווח תוך 45 ימים מרכישתה של רוגלה חדשה לעוזר לנשיא לענייני ביטחון לאומי (APNSA) על הרכישה, ולכלול בדיווח פירוט על מטרת הרכישה ועל השימושים המותרים ברוגלה.

לקריאת נוסח ההחלטה המלא אנא לחצו כאן.

במקביל, בסוף חודש מרץ 2023 נערך זו הפעם השנייה כנס ה-Summit for Democracy בהובלת ארה"ב, דרום קוריאה, קוסטה ריקה, הולנד וזמביה. בכנס הראשון, אשר התרחש בדצמבר 2021, הושקה יוזמת ה-Export Control and Human Rights Initiative ("**ECHRI**") אשר שמה לה למטרה להיאבק בניצול לרעה של טכנולוגיות וציוד דו-שימושיים על ידי מדינות ושחקנים שאינם מדינתיים הגורמים להפרות של זכויות אדם. כעת, לאחר מעט יותר משנה של עבודה, הושק בכנס השני ה-Code of Conduct של ה-ECHRI, המציג מסגרת של התחייבויות עבור מדינות אשר יבחרו לאמצו, שמטרתן קידום של פיקוח אפקטיבי על ייצוא של ציוד דו שימושי, מוצרי תוכנה וטכנולוגיה אשר עשויים לגרום לפגיעה בזכויות אדם.

בין ההתחייבויות המנויות ב-Code of Conduct ניתן למנות התחייבות לשקול שיקולים של שמירה על זכויות אדם בעת חקיקה, התקנת תקנות, ויצירת כלי אכיפה רגולטוריים בתחומי הפיקוח על הייצוא; להתייעץ עם גורמים מקצועיים מהמגזר הפרטי, האקדמיה, אנשי וארגוני טכנולוגיה וגורמים מטעם קבוצות מיעוט וקבוצות סיכון להפרה של זכויות אדם בעת עיצוב מדיניות פיקוח על ייצוא; לשתף מידע אודות סיכונים ולשתף פעולה בפיתוח והטמעת אמצעי אכיפה ופיקוח אפקטיביים בכל הנוגע לפיקוח על הייצוא; ולעודד מדינות נוספות לאמץ את הקוד.

נכון לעכשיו, המדינות אשר אימצו את ה-Code of Conduct כוללות את אלבניה, אוסטרליה, בולגריה, קנדה, קוסטה ריקה, קרואטיה, צ'כיה, דנמרק, אקוודור, אסטוניה, פינלנד, צרפת, גרמניה, יפן, קוסובו, לטביה, הולנד, ניו זילנד, צפון מקדוניה, נורבגיה, הרפובליקה של קוריאה, סלובקיה, ספרד, ובריטניה.

בעוד של-Code of Conduct אין משמעות 'אופרטיבית' בשלב זה, ניתן לראות כי הוא ממשיך את המגמה ההולכת ומתחזקת של מתן דגש על שיקולים הנוגעים להפרה ופגיעה בזכויות אדם בגיבוש מדיניות של פיקוח על ייצוא. לפיכך, אנו ממליצים ללקוחותינו העוסקים בתחומים רלוונטיים לוודא כי הם נותנים דגש דומה בעת ביצוע שיקולים עסקיים, ובעת עריכת בדיקות נאותות ללקוחות פוטנציאליים ולקוחות קיימים.

ה-Code of Conduct המלא זמין לקריאה כאן.

צוות הציות הבינלאומי במיתר ישמח לעמוד לשירותכם בנוגע לכל אחד מהנושאים המפורטים מעלה ובנושאים רבים נוספים, ולסייע בכל שאלה.

פרטי קשר

יובל ששון, שותף
03-6103190
ysasson@meitar.com

ד"ר שמרית איתי-חורב, שותפה
03-6103190
shimriti@meitar.com

נועם חורהאוס, עו"ד
03-6144041
noamg@meitar.com

למידע נוסף אודות מחלקת ציות בינלאומי לחצו כאן

מובהר, כי האמור לעיל הינו מידע כללי, אין בו התייחסות לנסיבות ועובדות ספציפיות ואין לראות בו משום חוות דעת ו/או ייעוץ משפטי לעניין קונקרטי.

להצטרפות לעדכוני לקוחות לחץ כאן

דרך אבא הילל סילבר 16, רמת גן, 5250608, ישראל | 03-6103100

הסר | דווח כספאם