

27 בינואר 2016

יז' בשבט התשע"ו

אסדרת פעילות הסייבר בישראל - הקמת מרשם לאומי של העוסקים בתחום ופרסום טיוטת צו הפיקוח על

מוצרי סייבר

ברצוננו להביא לידיעתכם שתי התפתחויות באשר לאסדרת פעילות הסייבר בישראל: האחת נוגעת למקצועות הגנת הסייבר והשנייה לפיקוח על יצוא בטחוני בתחום הסייבר.

א. אסדרת מקצועות הגנת הסייבר

1. ביום 31 בדצמבר 2015 פרסם לראשונה מטה הסייבר הלאומי מדיניות אסדרה של מקצועות הגנת הסייבר, לפיה יוענקו תעודות הסמכה ויוקם מרשם לאומי פומבי של הפרטים הכשירים לעסוק במקצועות הגנת הסייבר, וזאת בהתאם לעמידתם בתנאי סף ובמבחנים תיאורטיים ומעשיים ("מסמך המדיניות").
2. לאור השונות הגבוהה הקיימת בין העוסקים בתחום כיום, ובהתאם להחלטת ממשלה מס' 2443 מיום 15.2.2015 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", נמצא כי יש צורך לוודא את עמידת העוסקים בהגנת הסייבר בסטנדרטים מקצועיים, וזאת כדי להבטיח רמה מקצועית הולמת, וכדי להתמודד כהלכה עם איומי ביטחון, בטיחות הציבור וכלכלת ישראל בתחום הסייבר.
3. ככלל, הסמכת פרט והכללתו במרשם לא תהווה תנאי לעיסוק במקצועות הגנת הסייבר, אולם, רגולטורים בענפי המשק השונים יעשו שימוש במרשם כדי לחייב העסקת בעלי מקצוע מוסמכים. לצד זאת, המרשם יהווה סטנדרט מחייב לעוסקים בתחום במשרדי הממשלה ובגופים "רגישים", כמוסבר בהמשך.
4. דרישות ההסמכה יכללו תנאי סף בדבר גיל, אזרחות ישראלית והיעדר עבר פלילי; עמידה בבחינות תיאורטיות ומעשיות לקבלת הסמכה בסיסית ולהסמכה לרמת המומחיות המתקדמת (הרמה המתקדמת תכלול גם דרישת ותק מינימאלי של ארבע שנות ותק מקצועי), ועמידה תקופתית, מדי שלוש שנים, בדרישות לשמירת כשירות מקצועית.
5. רשימת המקצועות שיוסדרו, כמפורט במסמך המדיניות, תוך חלוקה לרמת מומחיות בסיסית ולרמה מתקדמת, הם כדלקמן:
 - 5.1 מיישם הגנת סייבר - בעל ידע תיאורטי בסיסי ויכולת יישומית (Hands-on) האחראי על יישום הגנת סייבר בארגון;
 - 5.2 מוסמך מבדקי חדירה - בעל ידע עדכני ויכולת מעשית גבוהה בנושאי איתור חולשות במערכי הגנת סייבר ובדיקת חדירות (Penetration Testing);
 - 5.3 מוסמך תחקור סייבר - בעל ידע עדכני ויכולת מעשית גבוהה בנושאי תחקור אירועים (Forensic);
 - 5.4 מוסמך מתודולוגיות הגנת סייבר - בעל ידע תיאורטי מקיף ומעמיק במכלול נושאי מתודולוגיות הגנת הסייבר;

- 5.5 מוסמך טכנולוגיות הגנת סייבר - בעל ידע תיאורטי מקיף ומעמיק במכלול נושאי טכנולוגיות הגנת הסייבר.
6. לוחות זמנים - המרשם יוקם בשנת 2017. בהתאם לכך, הבחינות לרמת המוסמך הבסיסי ייערכו החל משנת 2017, והבחינות לרמת המומחה יחלו בשנת 2021. הבחינות התקופתיות לבדיקת שמירה על כשירות מקצועית יחלו בשנת 2020.
7. השלכות על שוק העבודה -
- 7.1 קביעת חובת רישוי לשם עיסוק בהגנת סייבר נמצאה כפוגעת בחופש העיסוק באופן לא מידתי. משכך, ככלל, ההסמכה לא תהווה תנאי לעיסוק בתחום. עם זאת, במשרדי הממשלה, כל עובד חדש בתחום הגנת הסייבר יידרש לעמוד בהסמכות הרלבנטיות, ובתום חמש שנים כלל העוסקים בהגנת סייבר יידרשו להיות מוסמכים.
- 7.2 במגזר הפרטי, יוטל על הרגולטורים בענפי המשק השונים לקבוע דרישות באשר לעיסוק בתחום הגנת הסייבר בהתאם לנסיבות, כלומר רישום לא יהיה תנאי סף לעיסוק, אלא בשיקול דעת הרגולטור ככל שיימצא לנכון בכל תחום פעילות. בתוך כך, גופים ייחודיים שיוגדרו על-ידי הרשות הלאומית להגנת הסייבר תחת מטה הסייבר הלאומי כ"בעלי נזק פוטנציאלי משמעותי כתוצאה מפגיעה במערכות הממוחשבות שלהם", בהתאם לאופי פעילותם, תלותם במערכות מחשוב, תלות גופים אחרים בהם ועוד - יחויבו לעמוד בהסמכות רלבנטיות.
8. מימוש האסדרה יופקד תחת אחריות יחידה ייעודית ברשות הלאומית להגנת הסייבר, אשר תעסוק, בין היתר, בעריכת הבחינות, בהגדרת רמות ההסמכה והקריטריונים לעמידה בכשירות מקצועית ובקידום חקיקה בנושא.
9. הנוסח המלא של מסמך המדיניות נמצא באתר מטה הסייבר בקישור שלהלן:

<http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf>

ב. פיקוח על יצוא בטחוני בתחום הסייבר

10. ביום 7 בינואר 2016, פרסם אגף הפיקוח על היצוא הביטחוני במשרד הביטחון ("אפ"י") פניה לציבור לעיון ולהגשת התייחסות לטיטות נוסח הגדרת מוצרים וידע לפיקוח בתחום הסייבר ("טיטות הצו"), המרחיבה את הפיקוח על יצוא טכנולוגיות ביטחוניות בתחום הסייבר, אף מעבר לסטנדרטים בינלאומיים מוסכמים.
11. במסמך ההסבר הנלווה לטיטות הצו, צוין כי ענף הסייבר בישראל מהווה מנוע צמיחה אסטרטגי אשר כרוכות בו טכנולוגיות שהגעתן ליעדים עוינים עלולה לסכן אינטרסים ביטחוניים ומדיניים של ישראל. משכך, עלה צורך בהוספת תחום יצוא מוצרי הסייבר לרשימת הנושאים הכפופים לפיקוח הביטחוני. טיטות הצו עתידה להקל על היצואנים באמצעות הסרת אי ודאות והתווית כללים ברורים.
12. טיטות הצו עוסקת בהרחבת הפיקוח על טכנולוגיות סייבר התקפיות, כך שיחול גם על יצוא הטכנולוגיות עצמן (ולא רק על יצוא תשתיות לפיתוחן); וכן עוסקת בפיקוח על טכנולוגיות התקפיות שיעודן הדמיה של פעילות מהסוג האמור; פיקוח על ידע בנושא פגמים בקוד אשר ניתן לנצלם לצורך פגיעת סייבר; פיקוח על

מוצרי הגנת סייבר המיועדים לשימוש כוחות ביטחון, לרבות ציוד לחימה או ביון; ופיקוח על יכולות השגת מידע דיגיטלי באמצעות חיבור פיזי למערכת הנתקפת.

13. לאחר כניסת הצו לתוקף, כל חברה שתהא מעוניינת לייצא טובין המוגדרים בצו, תחויב להחזיק ברשיון יצוא. **ניתן להעריך כי רגולציה נוספת זו תכביד על הענף, שכן חברות רבות שעד עתה לא נדרשו להחזיק ברשיונות, תחויבנה לאחוז ברשיון יצוא.** משמעות משטר הפיקוח באה לידי ביטוי בחובת ניהול רישום ודיווח בקשר לעסקאות הנוגעות למוצרים מפוקחים, חובת החזקה ברשיון (במקרים מסוימים אף טרם ניהול מ"מ), מינוי עובד שישמש כממונה פיקוח בחברה, ועוד.

14. נוסף ונציין כי בעקבות הצו והידוק משטר הפיקוח, יעדי היצוא עשויים להצטמצם, ומוצרים שלא הוכפפו לפיקוח בעבר ויוצאו באופן חופשי לכל מדינה, עלולים להיאסר ביצוא למדינות מסוימות.

15. ניתן להגיש התייחסות לטיוטת הצו, לפי שעה, עד ליום **7 בפברואר 2016**.

16. עוד יצוין כי אפ"י בוחן אפשרות להקמת צוות עבודה, אשר יכלול נציגי יצואני טכנולוגיות סייבר, לצורך קיום דיון בטיוטת הצו ותיקונה ככל שימצא לנכון.

17. המלצתנו היא לבחון את השלכות הרגולציה המתהווה על פעילותכם העסקית בהקדם. לאור חשיבות העניין, משרדנו מתעתד לקיים פנייה מסודרת שתכלול התייחסות מקיפה לטיוטה המוצעת. חברות המעוניינות להציע הערות והסתייגויות שיועלו בפני המחוקק והרגולטור, מוזמנות לשלוח התייחסותן לדוא"ל המופיע מטה.

הנוסח המלא של טיוטת הצו, וכן מסמך הסבר נלווה לה, מצויים באתר האינטרנט של אפ"י בקישור שלהלן: <http://www.exportctrl.mod.gov.il/ExportCtrl/WhatsNew/Cyber.htm>

* * *

הסקירה לעיל הינה בבחינת תמצית. המידע הכלול בה נמסר למטרות אינפורמטיביות בלבד ואין במידע כדי להוות ייעוץ משפטי. לקבלת פרטים נוספים, אנא פנו לעו"ד נגה רובינשטיין, ראש מחלקת רגולציה ותחרות ו/או עו"ד גיל נדל, ראש תחום דיני יבוא, יצוא וסחר בינלאומי, בדוא"ל: Noga.Rubinstein@goldfarb.com או בטלפון: 03-6089843, ובדוא"ל:

Gill.Nadel@goldfarb.com או בטלפון: 03-6089979.