אל: לקוחות המשרד 06 בנובמבר 2016

**ניהול סיכוני סייבר בגופים מוסדיים**

ביום ה- 31 באוגוסט 2016 התפרסם חוזר משרד האוצר בנושא **ניהול סיכוני סייבר בגופים מוסדיים**, אשר מרבית הוראותיו צפויות להיכנס לתוקף ביום ה- 2 לאפריל 2017 (לחוזר משרד האוצר לחץ כאן).

על פי החוזר, שפורסם על ידי **הממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר**, יוטלו על הגופים המוסדיים, לרבות חברת ביטוח או חברה המנהלת קופת גמל, קרן פנסיה או קרן השתלמות, חובות מגוונים בהיבטי הגנת הסייבר במטרה להבטיח את שמירת זכויות העמיתים והמבוטחים על ידי שמירה על סודיות, שלמות וזמינות נכסי המידע, מערכות המידע, התהליכים העסקיים ופעילותו התקינה בכללותו של הגוף המוסדי.

רגולציה זו בתחום הסייבר המוטלת על הגופים המוסדיים, מצטרפת למגמה הולכת וגוברת של החלת אחריות במרחב הסייבר על ידי הרגולטורים בישראל על הגופים המונחים, כדוגמת ההוראה של המפקח על הבנקים בנושא ניהול הגנת הסייבר שפורסמה לפני כשנה וחלה על גופים פיננסים מפוקחים בישראל, לרבות בנקים וחברות כרטיסי האשראי (להוראת המפקח על הבנקים לחץ כאן). מגמה רגולטורית זו בישראל, תואמת את החלטת הממשלה מיום ה- 15 בפברואר 2015, לפיה: "אסדרת היערכות הארגונים במשק בתחום הגנת הסייבר תיעשה מתוך כוונה שלא להוסיף למשק עוד רגולטורים, אלא באמצעות העצמה של הרגולטורים הקיימים" (להחלטת הממשלה בנושא לחץ כאן).

החוזר מתווה עקרונות לניהול סיכוני סייבר בגוף המוסדי, תוך הטלת אחריות על הדירקטוריון והנהלת הגוף המוסדי להתנהלות המבוססת על עקרונות ממשל תאגידי נאותים, הכוללים התייחסות לשיטות, לתהליכים ולבקרות, במטרה להתמודד עם איומי סייבר ולנהל אירועי סייבר באופן אפקטיבי. החוזר כולל בין היתר את ההנחיות הבאות:

1. הגופים המוסדיים נדרשים **לאמץ מדיניות ותכנית עבודה לניהול סיכוני סייבר** ולאשרה בדירקטוריון לפחות אחת לשנה, לצד מינוי של ועדת היגוי לניהול סיכוני סייבר ומנהל אבטחת סייבר בעל מומחיות וניסיון ניהולי בתחום הגנת הסייבר.
2. **מנכ"ל הגוף מוסדי אחראי להבטחת ניהולו התקין של תחום סיכוני הסייבר**, לצד ועדת היגוי שתמונה על ידי הדירקטוריון ושתתכנס אחת לרבעון (ולפחות אחת לשנה), ותסייע למנכ"ל הגוף המוסדי לקבל החלטות ולבצע את תפקידיו בכל הקשור לניהול סיכוני הסייבר.
3. על הגוף המוסדי **לקבוע מדיניות כללית לניהול סיכוי סייבר וכן נהלים מפורטים המגדירים את תהליכי הגנת הסייבר בארגון**. הנהלים יגזרו מהמדיניות כאמור ומהנחיות חיצוניות (כגון אסדרה או מחויבויות חוזיות).
4. הגוף המוסדי נדרש **לדווח בהקדם האפשרי** לדירקטוריון ולממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר **על אירועי סייבר** משמעותיים שהתרחשו ברשתותיו ובנכסיו הדיגיטליים.

5. גוף מוסדי יישם סקרי אבטחת מידע ומבחני חדירה המכסים את המערכות והתהליכים הארגוניים באופן תדיר, לרבות אצל ספקי מיקור חוץ, המעבדים או מאחסנים נתונים של הגוף המוסדי.

6. הגוף המוסדי נדרש **לאסוף מודיעין ביחס לאיומים בתחום הסייבר** על ידי איסוף וניתוח של מידע רלוונטי, לצורך יצירת תפיסה כוללת ועדכנית של איום הסייבר וחשיפת הגוף המוסדי למול האיום.

7. כחלק מהסכמי מיקור חוץ, נדרש הגוף המוסדי **ליישם אמצעי הצפנה לכל אורך נתיב ההתקשרות** מרחוק עם נותן שירות מיקור החוץ, לרבות הצפנת מידע רגיש בשירותי מחשוב "ענן" מחוץ לישראל. בנוסף, יכלול הגוף המוסדי בהסכם ההתקשרות עם ספק מחשוב "ענן" יכולת שליטה ובקרה שלו על הספק וכן אפשרות חד צדדית להפסקת השימוש בשירותי ספק המחשוב.

8. על הגוף המוסדי **להגדיר תכנית היערכות וניהול אירועי סייבר**, בהתאם להערכת סיכונים ולניתוח תרחישי קיצון, התוכנית תכלול התייחסות לשלבי הגילוי, הערכת מצב, הכלה, בלימה, התאוששות וחזרה לשגרה.

כאמור החוזר לניהול סיכוני סייבר בגופים מוסדיים צפוי כאמור להיכנס לתוקף במהלך שנת 2017. משרד **גולדפרב זליגמן ושות'** ישמח לייעץ וללוות את כל לקוחותיו בתחום רגולציית הסייבר המתפתחת בישראל, בדגש על השפעותיה המעשיות והמשפטיות על פעילות הגוף המוסדי מחד וחברות המפתחות טכנולוגיות רלבנטיות מאידך.

* * *

**נשמח לעמוד לרשותכם בכל שאלה ו/או הבהרה**

* * *

**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 שרון גזית, ראש מחלקת חברות וטכנולוגיה, בדוא"ל:** Sharon.Gazit@goldfarb.com **ו/או בטלפון: 03-7101645, או אל עו"ד ברק פומרנץ בדוא"ל:** Barak.Pomeranice@goldfarb.com **ו/או בטלפון: 03-7101661.**