

Cyber-Security, Data Protection and Privacy

הטלת חובות בדבר ניהול הגנת סייבר על בעלי רישיונות תקשורת



לאחרונה פורסמה [החלטת משרד התקשורת](#) בעניין ניהול הגנת הסייבר ("ההחלטה"), שמטרתה להביא להיערכות בעלי רישיונות תקשורת כלליים ומיוחדים מסוגים שונים (רישיון מפ"א, רישיון רט"ן, רישיון אחוד וכיו"ב) להגנה מפני איומי סייבר על רשתות התקשורת והמשתמשים בהן. ההחלטה פורסמה בשים לב, בין היתר, לכך שרשתות התקשורת נחשבות תשתית לאומית חיונית, אשר משמשת הן בשגרה והן בחירום את גופי הביטחון, רשויות המדינה והציבור הרחב לאחסון והעברת מידע רב, ומשכך מהוות יעד אטרקטיבי לתקיפות סייבר. יצוין כי ההחלטה התפרסמה בהמשך לשימוע ציבורי שערך משרד התקשורת בנושא וכן לאחר ביצוע הליך של הערכת השפעות רגולציה חדשה (RIA) בשיתוף מערך הסייבר הלאומי.

ביום 12 במאי 2022 תוקנו הרישיונות שהוענקו לחברת התקשורת כאמור ונוסף להם נספח הגנת סייבר ("נספח הסייבר"). הוראות נספח הסייבר נבנו, בין היתר, בהתאם למסמך תורת ההגנה בסייבר של מערך הסייבר הלאומי, אשר מגדיר מתודולוגיה סדורה לניהול סיכונים בסייבר ולהתמודדות עימם, בהתאם לחקיקה והרגולציה הישראלית ובהתאם לתקינה הבינלאומית בנושא. עיקרו של נספח הסייבר בהטלת חובה על בעלי רישיונות התקשורת לערוך תכנית להגנה בסייבר, שמטרתה לאפשר לבעל הרישיון להיערך לאירוע סייבר ולהמשיך לפעול במהלכו באופן רציף, תוך הגבלת הפגיעה במתן השירות ותוך שמירה על פרטיות המנויים. בין השאר, נספח הסייבר כולל דרישות בקשר עם שלב בניית התכנית ומניעת אירועי סייבר, שלב הטמעת התכנית באמצעות תרגול וניטור אירועי סייבר וצעדים נוספים, ושלב ניהול אירוע הסייבר וההתאוששות ממנו.

נספח הסייבר כולל הוראות פרטניות ביחס לפעולות אותן בעל רישיון נדרש לנקוט ביחס לכל אחד מהשלבים המפורטים בו (זאת, מבלי לגרוע מהוראות כל דין החלות על בעל הרישיון). במסמך זה, ריכזנו את העקרונות המרכזיים המשתקפים בנספח הסייבר:

- **מיפוי והערכת סיכונים:** בעל רישיון נדרש למפות את סוגי נכסי הסייבר שתפקודם חיוני לרציפות השירות, ובהתאם לנתח ולסווג את סיכוני הסייבר הפוטנציאליים. בעלי רישיונות מסוימים נדרשים גם לבצע סקר סיכוני סייבר לפחות אחת לשנה, לבצע מבדקי חדירה על-ידי גורם חיצוני ולערוך סקרי אבטחת מידע אצל ספקי מיקור החוץ המאחסנים מידע של בעל הרישיון.
- **הגדרת אחריות הדירקטוריון:** נספח הסייבר מתייחס במפורש לאחריות המוטלת על הדירקטוריון וקובע כי הדירקטוריון נדרש, לפחות אחת לשנה, לאשר את התכנית להגנה בסייבר, תוך התייחסות למתאר העדכני של איומי הסייבר. בנוסף, נדרש בעל רישיון לדווח לדירקטוריון על איתור אירוע סייבר, התקדמות הטיפול בו, החזרה לשגרה ותהליך התחקור.
- **מינוי ועדת היגוי ומנהל הגנת סייבר:** בעל רישיון נדרש למנות ועדה בראשות מנכ"ל התאגיד, אשר תתכנס לפחות אחת לרבעון, שתפקידה להנחות ולפקח על פעילות הגנת הסייבר אצל בעל הרישיון. בנוסף, נדרש בעל רישיון למנות מנהל הגנת סייבר שיהיה אחראי, בין השאר, על עמידת בעל הרישיון בדרישות נספח הסייבר.

- **קביעת נהלים:** חלק משמעותי מנספח הסייבר עוסק בקביעת נהלים ברורים ביחס לכל אחד מהשלבים הנוגעים לבניית התכנית והטמעתה, ובכלל זה נהלים לבקרת גישה וניהול חשבונות משתמשים, שימוש בשירותי ענן, רכש והתקשרות עם ספקים ונותני שירותי, היערכות וניהול אירועי סייבר ועוד.
- **תחילה:** מועד תחילת מרבית ההוראות בנספח הוא שישה חודשים מיום תיקון הרישיון, אולם מועד תחילתן של חלק מההוראות יהיה 12 חודשים ממועד התיקון (למשל, הוראות הנוגעות לבקרת גישה וניהול משתמשים ואבטחת מדיה לאחסון מידע) או 18 חודשים ממועד התיקון (למשל, הוראות הנוגעות לעריכת סקר סיכוני סייבר).
- **תחולה:** מרבית ההוראות בנספח הסייבר חלות על בעל רישיון המספק שירות ל-50,000 מנויים ומעלה, אולם נקבעו גם הוראות מיוחדות שחלות על בעל רישיון המספק שירות ל-200,000 מנויים ומעלה (למשל, עריכת סקרי סיכוני סייבר ותרגול המערכים הרלוונטיים להתמודדות עם אירוע סייבר) או כזה המספק שירות ללמעלה ממיליון מנויים (למשל הטמעת מערכת SIEM לתיעוד וניטור אירועים חשודים). בעלי רישיונות המספקים שירות לפחות מ-50,000 מנויים פטורים מהוראות נספח הסייבר.

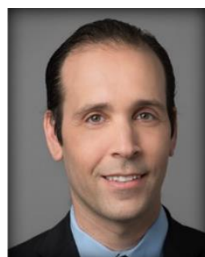
הטמעת הוראות נספח הסייבר תוכל לסייע לארגונים לעמוד לא רק בהוראות הרגולציה אלא גם בסטנדרטים בינלאומיים של אבטחת סייבר, ובהתאם – למזער באופן משמעותי את החשיפה להתרחשות אירוע סייבר ולהעניק לארגונים כלים משמעותיים להתמודדות עם אירועי סייבר.

אנו עומדים לרשותכם בכל שאלה.

לפרטים נוספים:



עו"ד רבקה גניס
rebeccage@gornitzky.com



עו"ד אסף אבטובי, שותף
asafa@gornitzky.com



עו"ד אסף הראל, שותף
assafh@gornitzky.com



עו"ד ליאור פורת, שותף מנהל
porat@gornitzky.com