תל אביב, ז׳ תשרי, תשפ״ו
29 ספטמבר, 2025
חוזר מס׳ מ-406-02

לכבוד
<u>מיופי כוח בתמורה</u>

הנדון: <u>תיקון הוראה מס׳ 406 בנושא ״ניהול אבטחת מידע והגנת סייבר״ בעקבות תיקון 13 לחוק הגנת הפרטיות, התשמ״א-1981 ונושאים נוספים</u>

<u>מבוא</u>

1. בעקבות תיקון 13 לחוק הגנת הפרטיות, התשמ״א-1981 (להלן – ״**חוק הגנת הפרטיות**״, ״**תיקון 13 לחוק הגנת הפרטיות**״), בוצעו תיקונים בהוראת ממונה מס׳ 406 בנושא ״ניהול סיכוני אבטחת מידע והגנת הסייבר״ (להלן - ״**ההוראה**״, ״**הוראה 406**״) המסדירה כללים לניהול והגנה על נכסי המידע שבידי מיופה כוח בתמורה. כמו כן, בוצעו כמה תיקונים נוספים להוראה לצרכי הבהרה ועדכוני ניסוח.
2. בתיקון 13 לחוק הגנת הפרטיות נקבעה, בין השאר, חובת מינוי ממונה על הגנת הפרטיות בגופים המנויים בסעיף 17ב1(א) לחוק הגנת הפרטיות, שיפעל להבטחת קיום ההוראות לפי החוק האמור, ולקידום השמירה על הפרטיות ואבטחת המידע במאגרי המידע.
בהתאם לכך, אנו מבקשים להפנות את תשומת הלב לכך שמיופי כוח בתמורה המסווגים לפי ההוראה לקבוצה 3 נמנים על הגופים הנדרשים במינוי ממונה על הגנת הפרטיות לפי חוק הגנת הפרטיות. מיופי כוח בתמורה אחרים, נדרשים לבחון את חובתם למינוי ממונה הגנת הפרטיות על פי החוק. לעניין זה יצוין, כי הוראות הממונה אינן כוללות את החובה למינוי ממונה הגנת הפרטיות מאחר שחובת מינוי כאמור ותפקידי ממונה על הגנת הפרטיות עוגנו בחוק הגנת הפרטיות ויאכפו לפיו.
3. ההוראה לא מלווה בפרסום דוח קביעת אסדרה לפי חוק עקרונות האסדרה, התשפ״ב-2021 (להלן – ״**חוק עקרונות האסדרה**״) בהתאם לפטור הקבוע בסעיף 34(ג)(2) לחוק עקרונות האסדרה, שכן ההשפעות הישירות והעקיפות שצפויות להיות לאסדרה על הגורמים שעליהם היא נועדה לחול או על אינטרסים מוגנים אחרים, לרבות עלות הציות לה, אינן מהותיות. זאת מאחר שעיקר התיקונים הם כאמור בעקבות תיקון 13 לחוק הגנת הפרטיות.
4. להוראה לא נדרשת בחינה תקופתית כאמור בסעיף 36(א) לחוק עקרונות האסדרה בהתאם לפטור הקבוע בסעיף 36(א)(1) לחוק עקרונות האסדרה, וזאת מאחר שהתיקונים אינם מהותיים, ועיקרם הינו כאמור בעקבות תיקון 13 לחוק הגנת הפרטיות, בעוד שהקצאת המשאבים הנדרשת לשם בחינה כאמור היא בלתי סבירה בהתחשב בעלות הציות לתיקונים כאמור ובהשלכות שלהם על נטל אסדרה זו.
5. להלן פירוט עיקרי התיקונים שבוצעו בהוראה.

פרק א' - כללי

6. בסעיף 3 – עודכנו ונוספו הגדרות, כמפורט להלן:

6.1. עודכנה הגדרת "אבטחת מידע" כך שההגדרה תכלול גם הגנה על מידע מפני עיבוד ללא רשות כדין, וכן הוחלף המונח "הגנה מפני תקיפות מערכות המידע" במונח "הגנה מפני תקיפת סייבר". כמו כן, נוספו הגדרות של המונחים הכלולים בהגדרת אבטחת מידע – "סודיות", "שלמות", "זמינות".

6.2. הגדרת "מידע רגיש" תוקנה כך שבמקום "מידע רגיש כהגדרתו בחוק הגנת הפרטיות" יבוא "מידע בעל רגישות מיוחדת כהגדרתו בחוק הגנת הפרטיות" וזאת בעקבות שינויים שנכללו בהגדרות בתיקון 13 לחוק הגנת הפרטיות. כמו כן, הובהר שנתוני אשראי ודירוג אשראי כהגדרתם בחוק נתוני אשראי, התשע"ו-2016 (להלן – **"החוק"**) הינם מידע רגיש. בהתאם לכך, נמחקו לאורך ההוראה כמה מופעים של המילים "לרבות נתוני אשראי" מאחר שנתוני אשראי נכללים כאמור בהגדרת "מידע רגיש".

6.3. נוספה הגדרת "עיבוד מידע", "שימוש במידע". ההגדרה נועדה להבהיר את המונחים "עיבוד מידע" או "שימוש במידע" המופיעים לאורך ההוראה, והיא מרחיבה וכוללת כל פעולה המבוצעת על מידע, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו. ההגדרה התבססה על הגדרת "עיבוד", "שימוש" שבתיקון 13 לחוק הגנת הפרטיות, תוך התאמתה להוראה זו העוסקת בסוגי מידע רבים ולא רק במידע אישי.

6.4. עודכנה הגדרת "פלטפורמה דיגיטלית" באופן המדייק את האמצעים הדיגיטליים שבאמצעותם ניתן השירות ללקוחות, ותוך התאמה להגדרת "עיבוד מידע" שנוספה להוראה.

פרק ג' – דיווחים לממונה

7. בסעיף הדיווח על אירוע שנעשה בו שימוש במידע בלא הרשאה או בחריגה מהרשאה - נמחקו המילים "או גישה למידע או העברת מידע", וזאת בשל היותן כלולות בהגדרת "שימוש במידע" שנוספה להוראה (סעיף 8.2.1.2).

פרק ה' - דרישות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 2

8. נוספו דרישות לנושאים שיש לכלול במסמך המדיניות לניהול סיכוני אבטחת מידע, כמפורט להלן:

8.1. קביעת תהליכי עבודה ובקרה שיבטיחו כי מאגרי המידע מנוהלים בהתאם למטרות שלשמן נאסף המידע, ולשימושים המותרים במידע (סעיף 14.1).

8.2. התייחסות לשירותי מחשוב ענן, ככל שרלוונטי (סעיף 14.5).

9. נוסף פירוט כי הדרישה להכין תכנית לבקרה שוטפת על ידי הגורם האמון על תחום אבטחת מידע הינה בהתייחס לעמידה בדרישות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (סעיף 20).

10. פורטו חובות נוספות החלות על דירקטוריון מיופה כוח בתמורה שהתאגד כחברה והמשתייך לקבוצה 2:

10.1. דיון במסמך המדיניות לניהול סיכוני אבטחת מידע ואישורו לפחות אחת לשנה, בעת ביצוע שינוי מהותי במערכות המידע או בתהליכי העבודה, כאשר נודע על חשיפה לסיכונים טכנולוגיים חדשים הנוגעים למערכות המידע, לאחר אירוע אבטחת מידע משמעותי.

10.2. דיון באירועי אבטחת מידע מהותיים שהתרחשו, בהחלטות ובפעולות שבוצעו (סעיף 21).

11. נוספה חובה להצפין במנוחה דירוג אשראי כהגדרתו בחוק, בנוסף להצפנה כאמור של נתוני אשראי כהגדרתם בחוק, וזאת מאחר שגם דירוג אשראי כאמור נחשב מידע רגיש ולפיכך נדרשת אבטחת מידע ברמה גבוהה עבורו (סעיף 45).

12. עודכנה המגבלה המפורטת בסעיף כך שתתייחס לאחסון והעברה של מידע רגיש מחוץ לישראל, והובהר כי מגבלה זו אינה גורעת מהחובות החלות על מיופה הכוח בתמורה בהתאם לכל דין, לרבות בהתאם לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001 (סעיף 73).

13. נוספה דרישה כי תכנית ההדרכה לעובדים תכלול גם נושאי הגנת הפרטיות, בנוסף לנושאי אבטחת מידע ונושאים אחרים המפורטים בסעיף (סעיף 94).

פרק ו' - דרישות נוספות שיחולו על מיופה כוח בתמורה הנכלל בקבוצה 3

14. כחלק מהחובות הנוספות על סעיפים 13-21 להוראה, הובהר כי במסגרת הדיון שיתקיים בדירקטוריון על מסמך המדיניות לניהול סיכוני אבטחת מידע, הדירקטוריון ידון באפקטיביות המדיניות, ויקיים פיקוח נאות על יישום המדיניות על ידי ההנהלה, וזאת בכדי לחזק את הממשל התאגידי ופיקוח הדירקטוריון של מיופה כוח בתמורה. כמו כן, פורטה חובה לפיה, מסמך המדיניות יכלול כללים לקביעת רמת רגישות המידע, בין היתר לצורך הגדרתו כ"מידע רגיש", וכי המידע יסווג לקטגוריות (סעיף 103).
במקביל לאמור, נמחק סעיף 106 והועברה לסעיף 103 החובה שהייתה בו לדיון של הדירקטוריון במסמך המדיניות בתדירות ובנסיבות שבסעיף.

15. הובהר כי הדרישה שהממונה על אבטחת מידע והגנת הסייבר יכין תכנית לבקרה שוטפת הינה בהתייחס לעמידה בדרישות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (סעיף 107).

16. נוספה הבהרה לפיה, דרישות הכשירות לממונה אבטחת המידע והגנת הסייבר, אינן גורעות מהאמור בסעיף 17ב(ג) לחוק הגנת הפרטיות לפיו, לא ימונה כממונה על אבטחת מידע מי שהורשע בעבירה שיש עמה קלון או בעבירה על הוראות חוק הגנת הפרטיות.
כמו כן, נמחקו ההסמכות מסוג CCSA ו- CCNA כמתאימות לצורך מינוי לתפקיד ממונה אבטחת מידע והגנת הסייבר, וזאת מכיוון שלאחר עיון מחדש בטיבן של הסמכות אלו, נמצא כי אינן נותנות מענה הולם לידע המקצועי הנדרש לתפקיד (סעיף 108).

17. נוסף פירוט לפיו, מבחני החדירה שנדרש מיופה הכוח בתמורה לעשות יהיו תשתיתיים ואפליקטיביים, וכן כי סקר הסיכונים ומבחני החדירה יתייחסו גם לחשיפות הנובעות משימוש במיקור חוץ ומחשוב ענן (סעיפים 114-115).

18. נוספה חובה כי תכנית ההדרכה לעובדים תכלול נושאי הגנת הפרטיות, וזאת בנוסף לאבטחת מידע ונושאים אחרים (סעיף 159).

תחילה והוראות מעבר

19. תחילתם של התיקונים להוראה 2 חודשים מיום פרסום חוזר זה באתר האינטרנט של מערכת נתוני אשראי (להלן – "**יום התחילה**"), ואולם, מיופה כוח בתמורה רשאי ליישמם טרם יום התחילה. מובהר שאין באמור לגרוע מחובת מיופה כוח בתמורה לעמוד בחובות שחלות עליו לפי חוק הגנת הפרטיות במועד הנדרש לפי תיקון 13 לחוק האמור.

20. לחוזר זה מצורפת ההוראה המתוקנת.

בכבוד רב,

אייל חדד
הממונה על שיתוף בנתוני אשראי