



תל אביב, ה' בטבת, תשפ"ג

29 בדצמבר, 2022

חוזר מס' מ-406 - 01

לכבוד,

מיופי הכוח בתמורה

הנדון: הוראה מספר 406 בנושא "ניהול סיכונים אבטחת מידע והגנת הסייבר" למיופה כוח בתמורה

כללי

1. פעילות מיופה כוח בתמורה מתבטאת לרוב בקבלה ושמירה של דוחות ריכוז נתונים של לקוחות, לצורך מתן שירותי ייעוץ פיננסי ללקוח בתחום האשראי בהתאם לתקנה 6 בתקנות נתוני אשראי, התשע"ח-2017, וסעיף 13 בכללי נתוני אשראי (הוראות שונות), התשע"ח-2017. שירותי ייעוץ פיננסי יכולים לכלול, בין השאר: ייעוץ בדבר סבירות תנאי האשראי שקיבל הלקוח מנותני אשראי שונים, הצגת תנאי אשראי רצויים או עדיפים לעומת אלו שקיבל או עשוי לקבל מנותני אשראי, ייעוץ בדבר דירוג האשראי של הלקוח וכיצד ניתן לשפרו ועוד. במסגרת שירותים אלו, מיופה כוח בתמורה נחשף ומחזיק מידע רגיש אודות הלקוחות שמקורו במאגר נתוני אשראי, ולפיכך נדרש לקבוע עקרונות מינימליים לניהול והגנה על נכסי המידע המוחזקים על ידי מיופה הכוח בתמורה, וזאת במטרה להגן על פרטיות הלקוחות ולמזער את הסיכון לחשיפה או להעברת המידע לגורמים שאינם מורשים.
2. קיימת שונות רבה בין הגופים הפועלים כמיופי כוח בתמורה, אשר מתבטאת באופן ההתאגדות (כחיד או כחברה), במספר בעלי ההרשאה שיש להם גישה למאגר המידע המנוהל על ידי מיופה הכוח בתמורה, במספר הלקוחות שקיים לגביהם מידע במאגר המידע, במספר הלקוחות עבורם נמשכו דוחות ריכוז נתונים, בשירותים המוצעים על ידם ובערוצים בהם ניתנים השירותים, וכן במורכבות המערכת הטכנולוגית המופעלת על ידם, ועוד.
3. נוכח השונות הקיימת בין מיופי הכוח בתמורה כמפורט לעיל ועל מנת להבטיח את פעילותם התקינה בהיבטי אבטחת מידע, הגנת הסייבר והגנת הפרטיות, עולה הצורך בקביעת דרישות רגולטוריות מדורגות, התואמות את היקף ומורכבות פעילותם.
- מחד, גישה זו מאפשרת להבטיח את תקינות פעילות מיופי הכוח בתמורה תוך הגנה על לקוחותיהם, ומאידך, גישה זו מכירה בעובדה כי פעילותם של חלק ממיופי הכוח בתמורה הינה רחבת היקף ומורכבת ולפיכך הדרישות הפיקוחיות הינן רחבות יותר.
4. מודגש כי ההוראה אינה גורעת מהוראות דין רלוונטיות אחרות, לרבות חוק הגנת הפרטיות, התשמ"א-1981, תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן – "תקנות הגנת הפרטיות (אבטחת מידע)"), או כל דין רלוונטי אחר.

המדרג הרגולטורי

5. דרישות ההוראה נקבעו בהתאם למדרג רגולטורי, הכולל שלוש רמות יישום בהתאם לפרמטרים המצביעים על היקף הפעילות ועל רמת המורכבות, ולפיכך על הסיכון והחשיפה הפוטנציאליים לנזק כתוצאה מפעילות מיופה הכוח בתמורה. רמות היישום נקבעו באופן המביא בחשבון את מספר בעלי ההרשאה המורשים לגשת למאגר המידע, מספר הלקוחות שעליהם נשמר מידע במאגר המידע, וכן היקף דוחות ריכוז הנתונים שנמשכו על ידי מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים.

6. מיופה כוח בתמורה נדרש לשייך את עצמו לאחת משלוש רמות היישום בהתאם לתנאים שנקבעו בהוראה, כמפורט להלן:
- 6.1. קבוצה 1 (רמת יישום בסיסית) - בקבוצה זו ייכלל מיופה כוח בתמורה שמתקיימים לגביו כל התנאים המפורטים להלן:
- 6.1.1. מספר בעלי ההרשאה בו אינו עולה על 10.
- 6.1.2. מספר לקוחותיו אינו עולה על 300.
- 6.1.3. מספר דוחות ריכוז הנתונים שמשך מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, אינו עולה על 1,000.
- 6.1.4. מיופה הכוח בתמורה **אינו** מספק שירות ללקוחותיו באמצעות פלטפורמה דיגיטלית. ככל שאחד התנאים לא מתקיים נדרש לבחון שיוך לקבוצה הבאה.
- 6.2. קבוצה 2 (רמת יישום בינונית) - בקבוצה זו ייכלל מיופה כוח בתמורה שאינו נכלל בקבוצה 1 ומתקיימים לגביו כל התנאים המפורטים להלן:
- 6.2.1. מספר בעלי ההרשאה בו אינו עולה על 100.
- 6.2.2. מספר לקוחותיו אינו עולה על 10,000.
- 6.2.3. מספר דוחות ריכוז הנתונים שמשך מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, אינו עולה על 10,000.
- 6.2.4. מיופה הכוח בתמורה **אינו** מספק שירות ללקוחותיו באמצעות פלטפורמה דיגיטלית. ככל שאחד התנאים לא מתקיים נדרש לבחון שיוך לקבוצה הבאה.
- 6.3. קבוצה 3 (רמת יישום גבוהה) - בקבוצה זו ייכלל מיופה כוח בתמורה שמתקיימים לגביו אחד או יותר מהתנאים המפורטים להלן:
- 6.3.1. מספר בעלי ההרשאה בו עולה על 100.
- 6.3.2. מספר לקוחותיו עולה על 10,000.
- 6.3.3. מספר דוחות ריכוז הנתונים שמשך מיופה הכוח בתמורה במהלך אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, עולה על 10,000.
- 6.3.4. מיופה הכוח בתמורה **מספק** שירות ללקוחותיו באמצעות פלטפורמה דיגיטלית.
- להלן דוגמה: לצורך סיווג לקבוצה 1, נדרש קיומם של 3 התנאים הבאים יחדיו: מספר בעלי ההרשאה נדרש להיות עד 10, מספר הלקוחות נדרש להיות עד 300, ומספר דוחות ריכוז הנתונים שנמשכו על ידי מיופה הכוח בתמורה במהלך כל אחד מתוך ארבעת הרבעונים הקלנדריים האחרונים, אינו עולה על 1,000. כאשר אחד התנאים אינו מתקיים, מיופה הכוח בתמורה יסווג לקבוצה גבוהה יותר. כך למשל, במקרה שבו מספר בעלי ההרשאה הינו 8 ומספר הלקוחות הינו 310, מיופה הכוח בתמורה יסווג לקבוצה 2.
7. מיופה כוח בתמורה המסווג לקבוצה 1 הינו גוף הפועל בהיקף פעילות נמוך. בהתאם, היקף הדרישות שהוחל עליו בהוראה הינו מצומצם וכולל דרישה לעמידה בתקנות הגנת הפרטיות (אבטחת מידע) לעניין מאגר שחלה עליו רמת אבטחה בסיסית, לכל הפחות. ההוראה כוללת דרישה לעריכת ביקורת על ידי מבקר, העומד בדרישות אשר נקבעו בהוראה, לבחינת עמידת מיופה הכוח בתמורה בתקנות הגנת הפרטיות (אבטחת מידע) כאמור. ביקורת המבקר תתבצע לראשונה בתוך 3 חודשים מיום רישומו של מיופה הכוח בתמורה במרשם הממונה, ולאחר מכן אחת ל-18 חודשים לפחות. אישורי המבקר יועברו לידי הממונה.
8. מיופה כוח בתמורה המסווג לקבוצה 2 או לקבוצה 3, הינו גוף הפועל בהיקפי פעילות גבוהים יותר ויסווג לקבוצה באופן מדורג בהתאם להיקף פעילותו, או שהינו מספק שירותים באמצעות פלטפורמה דיגיטלית ובמקרה כזה יסווג לקבוצה 3. היקפי הפעילות ואופי הפעילות של מיופי כוח בתמורה אלו עלולים לחשוף

אותם לסיכוני אבטחת המידע והגנת הסייבר והגנת הפרטיות בהיקף נרחב יותר, ולפיכך נקבעו דרישות רגולטוריות רחבות משמעותית בהשוואה לאלו שנקבעו עבור קבוצה 1, ובאופן מדורג בין קבוצה 2 לקבוצה 3. לגבי שתי קבוצות אלו, ההוראה כוללת דרישה לעריכת ביקורת על ידי מבקר, כהגדרתו בהוראה, לבחינת עמידת מיופה הכוח בתמורה בהנחיות ההוראה, אחת ל-18 חודשים לפחות. ביקורת המבקר תתבצע לראשונה במהלך חצי השנה הראשונה לאחר רישומו של מיופה הכוח בתמורה במרשם הממונה.

מבנה ההוראה ועיקרי הנושאים שנכללו בה

9. סעיפים 1-3 להוראה כוללים: מבוא, תחולה והגדרות.
10. סעיף 4 להוראה כולל: פירוט כללי הסיווג לקבוצות, רמות היישום ושינוי סיווג קבוצה. בעת שינוי סיווג מקבוצה אחת לקבוצה אחרת שחלות עליה דרישות מחמירות יותר, תחול תקופת מעבר כמפורט להלן:
 - 10.1. בעת מעבר מקבוצה 1 לקבוצה 2 או 3, תחול תקופת מעבר ליישום הדרישות הנוספות של 6 חודשים.
 - 10.2. בעת מעבר מקבוצה 2 ל-3, תחול תקופת מעבר ליישום הדרישות הנוספות של 3 חודשים.
11. סעיף 5 להוראה כולל דרישה לעריכת ביקורת אחת ל-18 חודשים לפחות, על ידי מבקר, כהגדרתו בהוראה, בדבר עמידת מיופה הכוח בתמורה בדרישות ההוראה.
12. סעיף 6 להוראה כולל הנחיות לנושא הפעלת שירות חדש באמצעות פלטפורמה דיגיטלית. במסגרת זו מיופה הכוח בתמורה נדרש לדווח לממונה לפחות 90 יום טרם הפעלת שירות כאמור ויהיה רשאי להפעילו, ובלבד שהממונה לא התנגד לכך בתקופה זו. טרם פנייה לממונה, מיופה הכוח בתמורה נדרש, בין השאר, לערוך סקר סיכונים מפורט בדגש על סיכוני אבטחת מידע והגנת הסייבר, לקיים דיון בדירקטוריון ובהנהלה על השירות החדש ולקבל את אישורם.
13. סעיפים 7-9 להוראה כוללים דרישות דיווח לממונה, אשר נועדו לאפשר לממונה לפקח על פעילות מיופה הכוח בתמורה. דרישות הדיווח כוללות:
 - 13.1. דיווחים שנתיים לגבי מספר בעלי הרשאה, מספר לקוחות שנשמר לגביהם מידע ע"י מיופה הכוח בתמורה, מספר דוחות ריכוז נתונים שנמשכו על ידי מיופה הכוח בתמורה בכל אחד מהרבעונים בשנת הדיווח הקלנדרית, ועל בסיס הפרמטרים כאמור - הקבוצה אליה משתייך מיופה הכוח בתמורה;
 - 13.2. דיווחים מיידיים/שוטפים בנושאים הבאים: שינוי סיווג קבוצה, דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש שיש לו השפעה מהותית על ניהול המידע והגנתו, דיווח על אירוע צפוי בעל השפעה מהותית על ניהול המידע והגנתו, וכן דיווח על הפעלת שירות חדש באמצעות פלטפורמה דיגיטלית;
 - 13.3. דיווח החל על קבוצה 1 בלבד, המחייב העברת אישור מבקר על עמידת מיופה הכוח בתמורה בדרישות תקנות הגנת הפרטיות (אבטחת מידע), ברמת האבטחה הבסיסית לפחות.
14. סעיפים 10-12 (כוללים בפרק ד' להוראה), מפרטים את הדרישות החלות על מיופה כוח בתמורה המסווג לקבוצה 1. דרישות אלו כוללות, בין היתר: חובת עמידה בתקנות הגנת הפרטיות (אבטחת מידע) לעניין מאגר שחלה עליו רמת אבטחה בסיסית, לכל הפחות, ודרישה לעריכת ביקורת על ידי מבקר לבחינת עמידת מיופה הכוח בתמורה בתקנות הגנת הפרטיות (אבטחת מידע) כאמור.
15. סעיפים 101-13 (כוללים בפרק ה' להוראה), מפרטים את הדרישות החלות על מיופה כוח בתמורה המסווג לקבוצה 2. דרישות אלו כוללות, בין היתר, את הנושאים הבאים:
 - 15.1. חובות החלות על הנהלת מיופה כוח בתמורה, לרבות: מינוי גורם ייעודי שיהיה אמון על תחום אבטחת המידע, חובת הגדרת מסמך מדיניות, נהלים ותכנית עבודה שנתיים לניהול סיכוני אבטחת מידע (סעיפים 13-21).
 - 15.2. חובות בקרה וניטור, לרבות: יישום מנגנון תיעוד אוטומטי עבור פעולות המתבצעות במערכות המידע ובתשתיות שתומכות במאגר המידע ומנהלות מידע רגיש על לקוחות, ובמערכות מידע שרמת החשיפה

- שלהן לביצוע פעילות בלתי מורשית הינה גבוהה, הוראות לעניין חובת הפעלת מערך לניטור מערכות מידע (מערך SIEM) (סעיפים 22-28).
- 15.3. חובות לעניין אבטחת רשת וגישה מרחוק, לרבות: הגדרת כלים המסדירים תעבורת רשת, הטמעת אמצעי אבטחה לזיהוי ומניעת קוד עויין במערכות המידע, חסימת אפשרות לחיבור התקן זיכרון חיצוני למחשבים (ככל שישנה הצדקה עסקית לשימוש בהתקן זיכרון חיצוני יש לקיים מנגנוני הגנה ובקורות, כמפורט בסעיף), וידוא כי ננקטים אמצעים לצמצום החשיפה לסיכוני אבטחת מידע (לרבות חסימת ערוצי תקשורת שאינם נחוצים, שימוש בפרוטוקולי תקשורת מאובטחים ועוד), וכן גישה למערכות מידע שהוערכו כבעלות סיכון גבוה או בגישה מרחוק למערכות מידע תוך שימוש ב Multi Factor Authentication (MFA) (סעיפים 29-35).
- 15.4. חובות לעניין אבטחת מערכות ועדכון, לרבות: הקפדה על יישום עדכוני אבטחה שוטפים והטמעת חוקים ייעודיים במערכות ההגנה, הבקרה והניטור (סעיפים 36-38).
- 15.5. חובת הפרדה בין סביבת הייצור לסביבות אחרות (סעיפים 40-41).
- 15.6. חובת וידוא כי הגורם שאליו מיופה הכוח בתמורה מעביר את המידע הנוגע למתן השירות הוא הלקוח, או גורם מטעמו (סעיף 42).
- 15.7. חובת הצפנת תעבורה בתווך (Data In Transit), והצפנת נתוני אשראי במנוחה (Data At Rest) (סעיפים 43-46).
- 15.8. חובות לעניין מתן הרשאות גישה למשתמשים, הזדהות באמצעות (MFA) Multi Factor Authentication למשתמשים בעלי הרשאות חזקות, תיעוד תהליך ניהול והענקת הרשאות למשתמשים, שימוש בחשבונות משתמש אישיים (למעט מקרים מיוחדים שעבורם יוגדרו תהליכים מתאימים), יישום מדיניות סיסמאות בהתאם לסטנדרטים מקובלים ועוד (סעיפים 47-62).
- 15.9. חובת הגדרת תכנית היערכות לניהול אירועי אבטחת מידע הכוללת התייחסות לאופן התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע, ודיון בתכנית לפחות אחת לשנה ובכל עת שנעשה שינוי מהותי באופן פעילות מיופה הכוח בתמורה (סעיפים 63-64).
- 15.10. חובות לעניין אבטחת שרשרת אספקה ומיקור חוץ, לרבות: איסור על העברת פעילות מהותית הקשורה למתן שירות ללקוח למיקור חוץ, בחינה לפני ביצוע התקשרות עם ספק מיקור חוץ את סיכוני אבטחת המידע הכרוכים בהתקשרות, התייחסות בהסכם לנושאים המפורטים בהוראה, אחריות מיופה הכוח בתמורה לכל פעולה הנעשית בהסכמתו על ידי הספק, נקיטה באמצעי בקרה ופיקוח על עמידת הספק בהסכם ההתקשרות, הזדהות באמצעות MFA של הספק לצורך כל גישה מרחוק (סעיפים 65-69).
- 15.11. חובות לעניין שירותי מחשוב ענן, אשר נחשבים כמיקור חוץ ולפיכך כפופים להנחיות בנושא מיקור חוץ כאמור, לרבות: הערכת סיכונים בטרם שימוש במחשוב ענן, הגדרת מדיניות לשימוש במחשוב ענן, אפשרות לאחסון מידע רגיש מחוץ לגבולות מדינת ישראל רק לאחר וידוא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לרגולציית הגנת המידע של האיחוד האירופי (GDPR - General Data Protection Regulation) או רגולציה מקבילה אחרת, גישה לנתונים באמצעות דרכי גישה מאובטחות, יישום בקורות על הנתונים המאוחסנים בענן, וידוא כי עבור ערוצי הגישה מספק הענן ואלו קיימים אמצעים להגנת הסייבר ואבטחת מידע (סעיפים 70-78).
- 15.12. חובות לעניין מסירת מידע באמצעים דיגיטליים (סעיפים 79-80).
- 15.13. חובות לעניין אבטחה פיזית וסביבתית, לרבות: שמירה במקום מוגן של תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע, השמדה של רכיבי מידע המכילים נתוני אשראי לצמיתות, גישה פיזית למתחם מיופה הכוח בתמורה לאחר ביצוע תהליך זיהוי, יישום מערך הגנה הכולל אמצעי אבטחה

שיכללו בקרות מונעות ובקרות מגלות, סקירה שוטפת של רשימת מורשי הגישה למתחם מיופה הכוח בתמורה, ועוד (סעיפים 81-89).

15.14. חובות לעניין משאבי אנוש והדרכה, לרבות: הגדרת תהליך מיון וגיוס מועמדים בטרם העסקתם ובטרם שינוי שימוש בהרשאות גישה לעובדים קיימים, הגדרת כללי התנהגות ונהלים לעובדים בהיבטי אבטחת מידע והגנת הפרטיות, חתימת עובדים על נספח אבטחת מידע והצהרת שמירה על סודיות, הדרכות אבטחת מידע (סעיפים 90-96).

15.15. חובת עריכת ביקורת תקופתית על ידי מבקר בדבר עמידת מיופה הכוח בתמורה בדרישות ההוראה, וחובת דיון בדוח הביקורת בהנהלת מיופה הכוח בתמורה, לרבות יישום ההמלצות וקביעת תכנית עבודה שתכלול לוח זמנים לטיפול בליקויים, ככל שנמצאו (סעיפים 97-99).

15.16. חובות לעניין שמירה, גיבוי ושחזור של נתונים ומידע, ולתקופה שלא תפחת מ 24 חודשים או מ 7 שנים, בהתאם למפורט בהוראה, ולרבות חובת גיבוי באופן שיאפשר שחזור הנתונים למצבם המקורי.

16. סעיפים 102-164 (כלולים בפרק ו' להוראה), מפרטים את הדרישות החלות על מיופה כוח בתמורה המסווג לקבוצה 3. דרישות אלו מהוות **דרישות תוספתיות** לדרישות שפורטו בפרק ה'. דרישות תוספתיות אלו כוללות, בין היתר, את הנושאים הבאים:

16.1. מיופה כוח בתמורה הנכלל בקבוצה 3 יתאגד כחברה, כהגדרתה בחוק החברות, תשנ"ט-1999. זאת, בכדי להבטיח התנהלות על פי כללי ממשל תאגידי המחייבים פעילות חברה (סעיף 102).

16.2. חובות הנוגעות לאחריות הדירקטוריון, ובכלל זאת: קביעת מדיניות לניהול המידע והגנתו, חובת דיון בחשיפה לסיכונים כפי שהם מוצגים בסקרי הסיכונים, מבחני החדירה ודוחות ביקורת, וכן חובת דיון בתכנית להפחתת סיכונים וכן באירועי אבטחת מידע ככל שהתרחשו (סעיפים 103-106).

16.3. חובות הנוגעות לאחריות ההנהלה, ובכלל זאת: מינוי ממונה על אבטחת מידע והגנת הסייבר כמפורט בהוראה, בחינה שוטפת של סיכוני אבטחת מידע וסייבר, בחינת החשיפות לסיכונים כפי שהם מוצגים בסקרי הסיכונים, מבחני החדירה ודוחות ביקורת, וכן חובת קביעת תכנית להפחתת סיכונים והעמדת משאבים נאותים לצורך כך (סעיפים 107-111).

16.4. חובות לעניין עריכת סקר סיכוני אבטחת מידע ומבחני חדירה, לפי פרקטיקה מקובלת ובתדירות שלא תפחת מ-18 חודשים, ובהתאם למפורט בהוראה (סעיפים 112-116).

16.5. חובת ביצוע תהליכי פיתוח ותחזוקה באופן מאובטח (SSDLC), לרבות בהתאם לשלבים נדרשים כמפורט בהוראה (סעיפים 117-122).

16.6. חובות לעניין אבטחת רשת, לרבות יישום מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית או פיסית שלה והגדרת כלים לזיהוי נזקות (סעיפים 123-124).

16.7. חובות לעניין אבטחת מערכות ועדכון, לרבות נקיטת אמצעים הולמים לצורך צמצום החשיפה לסיכוני אבטחת מידע והטמעת כלי אוטומטיים לסריקת חולשות אבטחה במערכות ובתשתיות (סעיפים 125-127).

16.8. חובות לעניין הפרדה בין סביבות, לרבות הפרדת הסביבה בה ינוהלו נתוני אשראי של לקוחות פרטיים ממערכות מידע וסביבות אחרות, וניהול הרשאות משתמשים לסביבת ייצור בנפרד מהרשאות לסביבות אחרות (סעיפים 128-130).

16.9. חובות לעניין ניהול הרשאות ובקרת גישה, לרבות: הגדרת הליך תקופתי לטיוב פרופילי הרשאות כמפורט בהוראה, חסימת גישה אוטומטית לחשבונות משתמשים שלא מתקיימת בהם פעילות לאורך זמן ממושך, הפרדת סמכויות בפרופילי הרשאות המשתמשים (סעיפים 131-136).

16.10. חובת יישום מנגנונים ובקורות למניעת דלף מידע ואובדן מידע (סעיף 137).

16.11. חובת שימוש בתעודה דיגיטלית למיופה כוח בתמורה הפועל באמצעות פלטפורמה דיגיטלית.

16.12. חובות לעניין ניהול משתמשים, לרבות: תיעוד, ניטור ובקרה שוטפים אחר משתמשים וחקירת אנומליות או חריגות, והוראות לעניין ניהול חשבונות משתמשים בעלי הרשאות חזקות כמפורט בהוראה (סעיפים 139-140).

16.13. חובת הגדרת תכנית היערכות לניהול אירועי אבטחת מידע בהתאם להערכת סיכונים ולניתוח תרחישי איום, דיון בתכנית אחת לרבעון, והקמת צוות תגובה להתמודדות עם אירועי אבטחת מידע (סעיפים 141-143).

16.14. חובות לעניין אבטחת שרשרת אספקה ומיקור חוץ, לרבות: מיפוי שוטף של הספקים ובחינת הסיכונים הנגזרים מאופי פעילותם והבקורות הנקטות לצמצום הסיכונים (סעיפים 144-146).

16.15. חובות לעניין התקשרות עם ספק שירותי ענן המוגדר כספק מהותי (סעיף 147).

16.16. חובות למיפוח כוח בתמורה העושה שימוש במכשירים ניידים, לרבות: גיבוש מדיניות ארגונית לשימוש במכשירים ניידים, תהליך לניהול מכשירים ניידים, והטעמת חוקים ייעודיים והתראות במערכת ה SIEM עבור מכשירים ניידים שאינם מוגדרים ברשת הארגונית. כמו כן, נקבע כי לא יתאפשר מתן שירות ללקוחות באמצעות מכשירים ניידים שאינם מוגדרים ברשת הארגונית (סעיף 148).

16.17. חובות לעניין מסירת מידע באמצעים דיגיטליים, לרבות: זיהוי מבקש המידע, קבלת הסכמתו להעברת מסרים ובדיקה כי הוא רשאי לקבל את המידע, שמירת מידע תפעולי הנוגע למשלוח מידע באמצעים דיגיטליים, הטמעת חוקים ייעודיים והתראות במערכות ההגנה, ומתן הנחיות ללקוחות המסייעות לנקיטת אמצעי זהירות לשמירה על פרטיות המידע (סעיפים 149-152).

16.18. חובות לעניין ניהול סיסמאות לקוח, לרבות: הגדרת נהלים, הנחיות לעניין מתן סיסמה ראשונית ללקוח, נקיטת אמצעים להגנה על המכשירים המשמשים את הלקוח להתקשרות (סעיפים 153-157).

16.19. חובות לעניין משאבי אנוש והדרכה, לרבות: הגדרת רמת סיווג עבור כל תפקיד הקיים בחברה ובדיקות רקע שיש לבצע למועמדים בטרם העסקתם, הקפדה על תיעוד תהליך הגיוס באופן נאות, עריכת תכנית הדרכה מקיפה כמפורט בהוראה, וביצוע קמפיינים להעלאת מודעות העובדים בנושא הנדסה חברתית (סעיפים 158-161).

16.20. חובת שמירת עותק גיבוי של הנתונים הנדרשים לשמירה בסעיפים 100.1-100.4 בהוראה (סעיף 162).

17. נספחים א-ה' (כלולים בפרק ח' להוראה), כוללים פורמטים להעברת דיווחים לממונה בהתאם למפורט בסעיף 13 לעיל.

מועד תחילת ההוראה

18. תחילתה של הוראה זו הינה ביום פרסומה באתר האינטרנט של מערכת נתוני אשראי בבנק ישראל (להלן – "יום התחילה"); ואולם, מיופה כוח בתמורה שרשום במרשם נכון ליום התחילה (להלן – מיופה כוח בתמורה רשום), יישמה לא יאוחר מ- 3 חודשים מיום התחילה.

19. על אף האמור בסעיף 18, תחילתו של פרק ג' להוראה (דיווחים לממונה) ביום 5.9.2023.

20. על אף האמור בסעיפים 18 ו-19, תחילתו של סעיף 8.2 (דיווח על אירוע משמעותי שהתרחש או כמעט והתרחש בתחום ניהול המידע והגנתו) ביום התחילה גם לגבי מיופה כוח בתמורה רשום.

בכבוד רב,



אייל חדד

הממונה על שיתוף בנתוני אשראי