בנק ישראל

מזכירות הוועדה המייעצת

פרוטוקול מישיבת הוועדה המייעצת להוראות הממונה על שיתוף בנתוני אשראי

שהתקיימה <u>באמצעי תקשורת</u> בתאריך 2.11.2022

משתתפים מקרב חברי הוועדה:	פרופ' רות שנער – יו"ר הוועדה המייעצת יובל טלר חסון כרמי אור רונן הורוביץ אוריאל לדרברג רני נויבאר
חברי ועדה שנעדרו	עו"ד ראובן אידלמן פרופ' עדית סולברג
משתתפים מקרב עובדי הבנק:	אייל חדד, הממונה על שיתוף בנתוני אשראי (להלן – הממונה) חן הולצמן – מזכירת הוועדה המייעצת עו"ד שירלי אבנר, המחלקה המשפטית <u>עובדי הממונה</u>: איריס אהרון ערן ביטנר אירית זמיר עדו שגב איתי דגני גילי קרן יניב פוגל נופר חי רוית מזרחי מגי סודאי אופיר אפריאט נירית קאולי יעקב רוטנברג ויסאם נאטור איילת רוזנבליט
מוזמנים נוספים	עו"ד לירון הופפלד– הרשות להגנת הפרטיות, משרד המשפטים

עיקרי הדיון:

נושא 1 בסדר היום: עדכוני הממונה	
הממונה	מספר עדכונים חשובים לידיעת חברי הוועדה: הנגיד הודיע בעיתונות שברצונו לממש את סעיף 112 לחוק נתוני אשראי, התשע"ו-2016 ולהרחיב את התחולה גם על תאגידים. על פי החוק, הרחבת התחולה היא בהתייעצות השר ובאישור ועדת הכלכלה של הכנסת. ככל שיוחלט על הרחבה זו, ייתכנו בעתיד הוראות ממונה חדשות, שיועלו לדיון בוועדה המייעצת.

נושא 2 בסדר היום: טיוטת הוראה 406 בנושא "ניהול סיכוני אבטחת מידע והגנת הסייבר" למיופה כוח בתמורה	
עובדת הממונה	כחלק מאסדרת הפעילות של מיופי הכוח בתמורה ובהתאם למדיניות הממונה שגובשה בנושא, נכתבה טיוטת הוראה חדשה (מס' 406) בנושא 'אבטחת מידע והגנת הסייבר' שתחול על מיופי הכוח בתמורה. מיופי הכוח בתמורה חשופים למידע רגיש של לקוחות, ובפרט לנתוני אשראי שמקורם ממאגר נתוני אשראי, ולכן נדרש להסדיר הוראה בנושא. טיוטת הוראה זו מחלקת את מיופי הכוח בתמורה ל-3 קבוצות יישום, על פי מדרג שנקבע בהתאם לרמות הפעילות שלהם. אציג מידע כללי על מיופי הכוח בתמורה. תהליך הרישום כמיופה כוח בתמורה, על פי החוק, נעשה באמצעות הגשת בקשה לממונה, ובדיקה של צוות הממונה אם יש רישום פלילי של המבקש ועמידה בכמה קריטריונים נוספים. כשמיופה כוח בתמורה מאושר על ידי הממונה ונרשם במערכת, מוטלת עליו האחריות לעמוד בהוראות החוק. כיום רשומים במערכת כ-950 מיופי כוח בתמורה, אבל מעט מהם פעילים, כך לדוגמה: רק כ-20 מיופי כוח בתמורה שולפים כ-50% מסך הדוחות הנשלפים על ידי מיופי כוח בתמורה מהמערכת. מתוך סך מיופי הכוח בתמורה, הרוב המוחלט הם יחידים וכ-7% בלבד הם תאגידים. בעקבות חוק שירות מידע פיננסי,תשפ"ב-2021, המודעות וההתעניינות בנושא של פעילות באמצעים דיגיטליים עלתה, וכמו כן, גם מגפת הקורונה, האיצה תהליכים של מתן שירות באמצעים דיגיטליים, ועל רקע האמור, היקף מיופי הכוח בתמורה שמעוניינים לתת שירות ללקוחות באמצעים דיגיטליים הולך וגדל. המצב המתואר, העלה את הצורך והחשיבות של הסדרת נושא אבטחת מידע והגנת הסייבר בפעילותם של מיופי הכוח בתמורה. על פי ההנחיות בהוראה, האחריות לסיווג לקבוצות מוטלת על מיופה הכוח בתמורה. ובמסגרת זו, על מיופה הכוח בתמורה לבדוק באופן שוטף את הסיווג בהתאם לקריטריונים בהוראה, לתעד את הסיווג לקבוצה ולעדכן את הממונה אם חל שינוי בסיווג לקבוצות. על פי בדיקות שערכנו, נראה כי מרבית מיופי הכוח בתמורה צפויים להיכלל בקבוצה הראשונה. הסיווגים לקבוצות כאמור, לוקחים בחשבון את תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017:

קבוצה 1 רמת יישום בסיסית- נכון להיום, על פי הערכה שביצענו נכון לנקודת הזמן הזו, כ-98 אחוזים ממיופי הכוח בתמורה משתייכים לקבוצה זו. ועיקר המאפיינים של קבוצה זו:

- ביצוע פעילויות ידניות;
- היקף פעילות מצומצם (מספר הדוחות שמוציאים מתוך המערכת);
- מספר מועט של לקוחות, שאינו עולה על 300;
- מספר בעלי ההרשאות לא עולה על 10.

מיופי כוח מקבוצה זו נדרשים לעמוד בתקנות הגנת הפרטיות (אבטחת מידע) תשע"ז- 2017, החלות על מאגרים ברמת האבטחה הבסיסית.

קבוצה 2 רמת יישום בינונית- מיופה כוח בתמורה השייך לקבוצה זו מאופיין בהיקף פעילות בינוני. ההנחיות לקבוצה זו מקבילות במידה רבה להנחיות החלות על מאגרים שחלה עליהם רמת האבטחה הבינונית לפי תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז- 2017, תוך הרחבות ותוספות על התקנות כאמור.

קבוצה 3 רמת יישום גבוהה- מיופה כוח בתמורה השייך לקבוצה זו מאופיין בהיקף פעילות גבוה או בפעילות באמצעות פלטפורמה דיגיטלית. מיופי כוח בתמורה שיסווגו לקבוצה זו יחויבו לפעול לפי ההנחיות המפורטות בהוראה החלות על קבוצה 2 וגם על פי ההנחיות שהתווספו החלות על קבוצה 3 כמפורט בהוראה. בקבוצה זו, ההנחיות מקבילות במידה רבה להנחיות החלות על מאגרים שחלה עליהם רמת האבטחה הגבוהה לפי תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, תוך הרחבות ותוספות.

טיוטת ההוראה מאפשרת זמן היערכות במעבר בין קבוצות הסיווג, כדלקמן:
המעבר מקבוצה 1 לקבוצה 2 או 3 קצוב לכ-6 חודשים; והמעבר מקבוצה 2 לקבוצה 3 קצוב לכ-3 חודשים, כיוון שהרבה הוראות בתחום אבטחת המידע חלות כבר על קבוצה 2, המעבר לסיווג מסוג 2 ל-3 אמור להיות משמעותי פחות.

נעבור עתה להציג סעיפים עיקריים בהוראה:

סעיף 5 בהוראה 'עריכת ביקורת'- בטיוטת ההוראה נקבע כי כל מיופי הכוח בתמורה נדרשים לערוך ביקורת ע"י מבקר חיצוני אחת ל-18 חודשים לפחות. ההוראה קובעת בהתאם לסיווג הקבוצות, תוך כמה זמן תתבצע הביקורת הראשונה מיום הרישום במערכת.

דוחות הביקורות יישמרו אצל מיופי הכוח בתמורה לתקופה של 7 שנים. טיוטת ההוראה מגדירה גם קריטריונים ל"מבקר" שיוכל לבצע את הביקורת החיצוני. הקריטריונים שהוגדרו הם בדומה לקריטריונים שנקבעו על ידי הרשות לניירות ערך בהוראה למתן שירות מידע פיננסי.

פרק ג' - דיווחים:

הפיקוח על מיופי הכוח בתמורה יתבצע באמצעות הדיווחים שלהם אל הממונה, ולכן הוסדרו בטיוטת ההוראה דיווחים שנתיים ודיווחים שוטפים. כמפורט להלן:

<u>דיווחים שנתיים</u> – אחת לשנה יש להעביר לממונה דיווח הכולל: מיפוי של מספר בעלי הרשאה; מספר לקוחות; מספר דוחות ריכוז נתונים שהוצאו על ידי מיופה

	הכוח בתמורה מהמערכת בכל אחד מהרבעונים במהלך השנה הקלנדרית האחרונה; והסיווג לקבוצה אליה משתייך מיופה הכוח בתמורה. מאחר שהממונה נדרש להיערך מיכונית לקליטת הדיווחים כאמור, התחילה של דיווחים אלו תתבצע בשלב מאוחר יותר. <u>דיווחים שוטפים</u> – • כאשר מיופה כוח בתמורה שמשתייך לקבוצת סיווג מסוימת, עובר לקבוצת סיווג אחרת, הוא צריך לדווח על כך לא יאוחר מ- 30 יום. גם סעיף יוחל עם השלמת ההיערכות המיכונית לקליטת הדיווחים. • <u>דיווח על אירוע משמעותי</u> – הכוונה לאירוע משמעותי בתחום אבטחת המידע. הוגדרו מספר תרחישים של אירועים משמעותיים, בדומה לסטנדרט הקיים בהוראות הממונה (לדוגמה: בהוראה 301 בנושא ניהול המידע והגנתו ללשכות ועוד) ולסטנדרטים של רגולטורים נוספים. סעיף זה יוחל באופן מיידי עם פרסום ההוראה. חשוב לציין כי הוראות אלו, אינן מייתרות את החובה של מיופה הכוח בתמורה להוראות כל דין, לרבות ההוראות של הרשות להגנת הפרטיות, והדיווחים הנדרשים לרשות על אירועי אבטחת מידע.
חבר הוועדה המייעצת	מדוע הוריתם לדווח תוך שעתיים, ולמה לא להורות שהדיווח יינתן תוך שעה.
עובדת הממונה	מסקירה רגולטורית השוואתית שערכנו עלה שהסטנדרט הקיים היום לדיווח על אירוע אבטחת מידע, כפי שבא לידי ביטוי גם בהוראות של רגולטורים מקבילים (כמו הממונה על שוק ההון ביטוח וחיסכון, והמפקח על הבנקים), הוא שעתיים.
עובדת הממונה	**פרק ד' – דרישות שיחולו על מיופי כוח בתמורה הנכללים בקבוצה 1** חשוב לציין כי טיוטת ההוראה אינה מחילה הוראות אבטחת מידע בנוסף לנדרש היום מקבוצה זו על פי תקנות הגנת הפרטיות (אבטחת מידע), למעט הדרישה שמבקר חיצוני יאשר שמיופה הכוח בתמורה עומד בתקנות, אלא הממונה מבקש לוודא עמידה בתקנות הגנת הפרטיות (אבטחת מידע), רמת האבטחה הבסיסית עבור קבוצה זו, בגלל רגישות המידע לו נחשפים מיופי הכוח בתמורה. **פרק ה' - דרישות שיחולו על מיופי כוח בתמורה הנכללים בקבוצה 2** אחריות הנהלה – הדרישה היא לכתוב מדיניות ונהלים ולחזק את רמת האבטחה. רמת הפירוט בהוראה גבוהה, מכיוון שאנו רואים חשיבות בכך שהדברים יהיה מפורטים וברורים. **פרק ו' - דרישות שיחולו על מיופי כוח בתמורה הנכללים בקבוצה 3** בקבוצה השלישית הדרישות גבוהות יותר, אך ברמה נמוכה מזו שבהוראת הממונה מס' 301 בנושא "ניהול המידע והגנתו" שחלה על לשכות האשראי. בקבוצה זו, הנהלת מיופה הכוח בתמורה נדרשת למנות גורם ייעודי שיהיה אמון על תחום אבטחת המידע בארגון.

	בנושאים רגישים מסוימים, הפירוט והדרישות בטיוטת הוראה לגבי קבוצה זו רחבים יותר מקבוצה 2, כגון: גישה מרחוק והצורך בתהליך זיהוי חזק; הצפנה של מידע רגיש; ניהול הרשאות; מיקור חוץ ומחשוב ענן. כמו כן, טיוטת ההוראה מפרטת גם דרישות הנוגעות לכוח האדם כמו למשל: הצורך בהדרכות, ביצוע הצהרות וחתימה על סודיות. סעיף 100 בטיוטת ההוראה מחייב את מיופי הכוח בתמורה, הנכללים בקבוצה השלישית לפעול כחברה החלות עליה חובות נוספות וזאת בכדי להבטיח התנהלות בהתאם לכללי ממשל תאגידי הולמים. סקר סיכוני אבטחת מידע ומבחני חדירה - מיופה כוח בתמורה המסווג בקבוצה השלישית נדרש לבצע סקר סיכוני אבטחת מידע בתדירות שלא תפחת מאחת ל 18 חודשים. **פרק ז' - תחילה**: הכוונה להחיל את ההוראה בתחילת שנת 2023. לאחר הדיון היום ולאחר פרסום הטיוטה וקבלת הערות הציבור. עבור מיופי כוח בתמורה שכבר רשומים במערכת, ניתנת בטיוטת ההוראה תקופת היערכות של 3 חודשים ליישום ההוראה.
חבר הוועדה	לדעתי, הסף העליון של עד 100,000 לקוחות בקבוצה 2 הוא גבוה מידי. סבור שהסף העליון של קבוצה 2 צריך להיות נמוך יותר, בסביבות ה-10,000 לקוחות למשל. המשמעות היא שכבר מעל 10,000 לקוחות, הסיווג של מיופה הכוח בתמורה יהיה לקבוצה 3.
עובדת הממונה	החלוקה לקבוצות לקחה בחשבון את תקנות הגנת הפרטיות, לפיהן במאגרים שחלה עליהם רמת האבטחה הגבוהה, נכללים מאגרים בהם קיים מידע על אודות מעל 100 אלף אנשים או מעל 100 מורשי גישה, ובהתאמה נקבעו ספים דומים בקבוצה 3. בכל מקרה נבחן את הצעתך לעדכון הספים. המשמעות היא החמרה ביחס לתקנות הגנת הפרטיות.
חבר הוועדה	ההגדרה של "פלטפורמה דיגיטלית" בטיוטת ההוראה לא ברורה. למשל האם שימוש בדואר אלקטרוני מהווה פלטפורמה דיגיטלית?
עובדת הממונה	בחנו רבות את ההגדרה וזה הנוסח שחשבנו שמשקף בצורה הטובה ביותר מהי פלטפורמה דיגיטלית. הכוונה היא שכאשר ניתן שירות ללקוח על ידי מיופה הכוח בתמורה באמצעות שימוש באתר אינטרנט או באפליקציה המשמעות היא שיש שימוש בפלטפורמה דיגיטלית. אין הכוונה לשליחת מיילים, שכן נכון להיום שימוש במייל הוא מאד נפוץ וכמעט בלתי אפשרי שלא להיעזר במיילים.
חבר הוועדה	אם אני עומד בהגדרה של פלטפורמה דיגיטלית אני עובר אוטומטית לקבוצה 3 ?
עובדת הממונה	כן. כך הוגדר בקריטריונים לסיווג לקבוצות.
עו"ד אבנר	אולי כדאי לחדד את ההגדרה בהתאם להערה. האם יש לך הצעה לנוסח ברור יותר?
חבר הוועדה	אני אסביר את כוונתי. אם יש לי 50 אלף לקוחות ואני מתקשר איתם במייל ופרצו לי למייל ומאגר הלקוחות נגנב, זה אירוע סייבר לא פשוט, ולכן צריך להגדיר מהי

	פלטפורמה דיגיטלית. הרבה מהאירועים שקרו היו דווקא במאגר המיילים שהכיל את כל המידע.
עובדת הממונה	בקבוצה 2 ההוראות די מחמירות. ניסינו להיות מידתיים כדי לא לפגוע בעסקים יש הוראות די מחמירות לגבי הצפנת מידע בעת העברתו לגורמים מחוץ למיופה הכוח בתמורה. לעניין היקף לקוחות, אני מבינה את ההערה ונבחן את זה. במידה ונחליט להוריד את הסף של קבוצה 2 כפי ההערה הקודמת, לדוגמה ל-10,000, אז מאגר הכולל מיילים בהיקפים שציינת, צפוי להיכלל בקבוצה 3.
הממונה	יכול להיות שאפשר לעשות תנאי שיכיל את שתי ההערות. האם יש לך הצעה בהקשר של הסיווג לקבוצה 2?
חבר הוועדה	הייתי מוריד את הסף של קבוצה 2. אם אני אחשוב על משהו, אשלח לכם. מדוע נדרש כי קבוצה 1 תבצע ביקורת חיצונית ראשונה תוך שלושה חודשים, ואילו קבוצות 2 ו-3 תוך שנה? אני מציע שבקרב כל הקבוצות הביקורת הראשונה תהיה תוך 3 עד 4 חודשים. ביקורת מהירה עשויה לצלם תמונת מצב איפה ישנם פערים ועל זה תתבסס תכנית העבודה. אם התקבל אישור לפעול ורק כעבור שנה תתבצע ביקורת, זה המון זמן, ועלולים לקרות אירועים בזמן הזה. לדעתי, חשוב לעשות ביקורת מהר כי הביקורת ממפה את הפערים שנצברו. יש פערים שניתן לחכות איתם, אבל יש פערים שכדאי, מניסיוני, לפעול מהר.
עובדת הממונה	הזמנים הוקצו בכדי לאפשר למיופי הכוח בתמורה זמן מספק להיערכות להוראה. אנחנו נבחן לקצר את הזמן של הביקורת הראשונה. עם זאת, תקופה של 3, 4 חודשים נראית, על פניו, קצרה מידי ותקשה על ההיערכות.
חבר הוועדה	בפרק הדיווחים לממונה בסעיף 8.2.1.2 – ההוראה היא כי בהשבתה מעל 3 שעות עליהם לדווח לכם. אני מציע לעלות הזמן, כי ישנן השבתות של 3 שעות ללא קשר לאבטחת מידע והגנת סייבר. הסף הזה, לדעתי, עלול לגרום לכם ל"רעש" ותהיו מוצפים בדיווחים. אני חושב שכדאי לעלות את זה ל-6 או 8 שעות.
עובדת הממונה	גם במקרה הזה, נצמדנו לסף לפי הסטנדרט המקובל אצל רגולטורים דומים. זה גם קיים בהוראת הממונה בנושא ניהול המידע והגנתו ללשכות האשראי.
חבר הוועדה	בנוסף, לא מצאתי אזכור להוראות הגנת הפרטיות והרבה מההנחיות נוגעות בהגנת הפרטיות או שפספסתי.
עובדת הממונה	יש לנו אמירה כללית במבוא להוראה, שיש חובה לעמוד בחוק הגנת הפרטיות, והתקנות מכוחו.
עו"ד אבנר	ההוראה לא מתייחסת בהכרח להגנת הפרטיות. זה עולם חופף אבל שונה, ולכן יש התייחסות במבוא כדי להגיד שזה לא מחליף את החובות החלות בתקנות של הגנת הפרטיות.
עו"ד הופפלד	הדיווח על האירועים האלה חשוב, ולכן אם ניתן יהיה להוסיף את זה בצורה מפורשת שיהיה מובן שזה לא יחליף את הוראה של הרשות להגנת הפרטיות לדיווח על אירועים.
עובדת הממונה	נעדכן זאת בהוראה.

חבר הוועדה	בנושא תכנית היערכות לניהול אירוע שמתרחש – ההמלצה שלי שההוראות בעניין זה החלות על קבוצה 3 יחולו גם על קבוצה 2. אני חושב שזה סעיף חשוב מאוד, ואם מסתכלים על אירועים בארץ קיימות טעויות בהתנהלות סביב אירועים, ולכן התוכנית איך מתכוננים לאירוע זה חשובה. לחילופין, ניתן להוריד את הסף בקבוצה 2, כפי שציינתי קודם.
עובדת הממונה	נבחן אם יש מקום לעבות את ההוראות בנושא זה בקבוצה 2.
חבר הוועדה	חובת מערך MDM על טלפונים ניידים – מניסיוני, הדרישות יהיו קשות ליישום. עלולה להיות התנגדות גדולה מצד העובדים של הארגונים על התקנת מערך MDM. תחשבו על זה. בפן האישי, לכל אחד בטלפון הפרטי שלו המון מידע אישי, והמעסיק רוצה להתקין מערכת ש"תשתלט" על הטלפון, זה עלול להיות בעייתי.
עובדת הממונה	אציין שגם בטיוטת תיקון הוראת ממונה מס' 301 בנושא "ניהול המידע והגנתו" על לשכות האשראי הוספנו חובה זו. הסעיף מבוסס, בין השאר, על מסמך של מערך הסייבר בנושא במסגרתו הוא ממליץ על התקנת מערכת לניידים מסוג זה.
חבר הוועדה	נכון, אבל יש המון התנגדות להמלצה, עובדים בחברות לא מסכימים לשתף פעולה עם זה.
הממונה	נעשה על זה דיון פנימי, אם יש לך המלצות בהקשר זה, אשמח לשמוע.

נושא 3 בסדר היום: הוראה 301 בנושא "ניהול המידע והגנתו" ללשכת אשראי – עדכון הוראה קיימת	
עובדת הממונה	הוראת הממונה מס' 301 בנושא "ניהול המידע והגנתו" התפרסמה לראשונה בשנת 2018 ועודכנה בשנת 2019. זו הוראה שחלה על לשכות האשראי ונמצאת ב"פוקוס הפיקוחי" של הממונה. בין צוות הממונה ולשכות האשראי יש ממשקים רבים ושוטפים בנושאים הללו. למשל באירועים משמעותיים בארץ ולעיתים בחו"ל, צוות הממונה מוודא שלשכות האשראי מכירות ומפיקות לקחים. על סמך הידע שנצבר הוחלט לעדכן כמה סעיפים בהוראה זו. רוב הדברים שעודכנו עלו מתהליכי ביקורת שנעשו, ולשכות האשראי כבר מודעות ואף מיישמות חלק מהעדכונים בפועל. אזכיר חלק מהשינויים החשובים בהוראה : • הורחבו הסעיפים המתייחסים לאחריות הדירקטוריון וההנהלה, לצורך חיזוק המעקב והפיקוח אחר ניהול המידע והגנתו בלשכה, וכן עודכנו חובות החלות על ממונה אבטחת המידע. • נוסף נושא חדש - "תכניות בתחום ניהול המידע והגנתו" אשר מרכז בפרק אחד את כלל התכניות שהלשכה נדרשת לאשר בתחום זה, לרבות חובת עריכת תכנית עבודה רב שנתית.

	• בקשר לדיווחים לממונה, עודכנו חלק מדרישות הדיווח לממונה לגבי אירועים בתחום ניהול המידע והגנתו, בהתאם לפרקטיקה מקובלת. • נוסף נושא חדש – "איסוף מודיעין" אשר לפיו, בין היתר, נדרש לאסוף ולנתח מידע רלוונטי ממקורות פנימיים וחיצוניים (כגון מערך הסייבר הלאומי), לבצע מעקב אחר איומי סייבר משמעותיים בישראל ובעולם, לבסס תמונת מצב ולנקוט צעדים בהתאם. • נוספו דרישות בנוגע לתהליכי פיתוח, תחזוקה וניהול שינויים, והובהר כי על תהליכי הפיתוח בלשכה להתבצע בהתאם לפרקטיקה המקובלת לביצוע תהליכי פיתוח מאובטח (SSDLC). • נוסף נושא חדש "מניעת דלף מידע ואבדן מידע". בין היתר, נכללה דרישה להגדיר תכנית למניעת דלף מידע ואבדן מידע, שתשלב כלים טכנולוגיים, הטמעת תהליכים ובקרות, ונקיטת פעולות להעלאת מודעות העובדים. • נוספה דרישה להצפנה במנוחה של נתוני אשראי וכן מידע אחר הנכלל בסעיף 1(3)(ז) ו- 1(3)(ח) בתוספת הראשונה לתקנות הגנת הפרטיות. • נוסף נושא חדש "שימוש במכשירים ניידים". כאשר חלק מהסעיפים כוללים דרישות המתייחסות לכלל המכשירים הניידים, וחלק למכשירים ניידים שאינם מוגדרים ברשת הארגונית של הלשכה ולכן יש חשיבות מיוחדת באסדרת הנושא. בין השאר, נכללה דרישה להטעמת מערך מרכזי לניהול מכשירים ניידים (MDM), בדומה לדרישה שנכללה בטיוטת ההוראה של מיופי כוח בתמורה. • התווספו הרחבות לעניין תהליך הזדהות חזקה באמצעות MFA, עבור משתמשים בעלי הרשאות חזקות, וכן בעת גישה למערכות בסיכון גבוה או בגישה מרחוק. • בנוגע לתכנית היערכות לניהול אירועי אבטחת מידע, נוספה הבהרה לעניין תכולת התרגול השנתי לתכנית ההיערכות לניהול אירועי אבטחת מידע, כך שהנ"ל יכלול הן תרגול עיוני אסטרטגי והן תרגיל מעשי.
חבר הוועדה	בהתייחס לאחריות ההנהלה להקצות משאבים הולמים לצורך מתן מענה לדרישות אבטחת מידע, אני מציע לנסח כך שההנהלה תהיה אחראית לתקצב את התחום.
עובדת הממונה	הכוונה במשאבים הינה הן למשאבים כספיים, כלומר תקציב, והן למשאבי כוח אדם.
חבר הוועדה	סעיף 25 בהוראה – למיטב ידיעתי, ברגולציות רבות הביקורת היא כל 18 חודשים. כדאי לשקול להתיישר לפי זה.
עובדת הממונה	נבדוק זאת ונתקן ככל שיידרש.

נושא 4 בסדר היום: הוראות הדיווח 308 ו-308A ללשכות אשראי – עדכון הוראות קיימות

עובדת הממונה	עדכון הוראות אלו נעשה בהתאמה לשינויים שנערכו כאמור בהוראה 301 בנוגע לדיווח לממונה על אירועים בתחום ניהול המידע והגנתו, בהתאם לפרקטיקה מקובלת. מקוצר הזמן, לא אפרט את השינויים, האם יש למישהו מהחברים הערות או שאלות?
יו"ר הוועדה המייעצת	משבחת את העבודה המקצועית והמקיפה על ההוראות.

02.1.2023

תאריך אישור הפרוטוקול

חתימה יו"ר הוועדה