רשומות

הצעות חוק

הממשלה

י"א בסיוון התשפ"ו | 1955 | 27 במאי 2026

עמוד

מתפרסמת בזה הצעת חוק מטעם הממשלה:

הצעת חוק הגנת הסייבר הלאומית, התשפ"ו–2026

פרק א': הגדרות

הגדרות

1. בחוק זה –

דברי הסבר

כללי מרחב הסייבר מהווה מרחב פעולה מערכתי, חוצה גבולות ורב־ממדי, המשמש תשתית אסטרטגית לפעילות אנושית, כלכלית וחברתית. מרחב זה הוא בעל השפעה מכרעת על תהליכים ומגמות ועל עיצוב פני התקשורת האנושית.

בעשור האחרון הפך מרחב הסייבר לזירת עימות מרכזית, המציבה איומים הולכים וגוברים על מדינות וארגונים ברחבי העולם. איום זה הופך מוחשי במיוחד לנוכח התלות הכמעט מוחלטת של החברה והמשק המודרני במערכות דיגיטליות, וכן בשים לב לכך שתקיפות הסייבר הולכות והופכות ממוקדות, מתוחכמות ומורכבות יותר.

מדינת ישראל היא אחת המדינות המותקפות ביותר בעולם במרחב הסייבר. מתחילת הלחימה במסגרת מלחמת "חרבות ברזל", שהחלה בכ"ב בתשרי התשפ"ד (7 באוקטובר 2023), ניכרה עלייה משמעותית בהיקף ובעוצמה של תקיפות הסייבר נגד גופים אזרחיים במשק הישראלי. מטרתן של תקיפות סייבר אלה היא לפגוע, פעמים רבות כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי. תקיפות אלה אף עלולות להביא לפגיעה בחיי אדם, הן בשגרה והן בחירום. האיום בולט במיוחד בנוגע לארגונים חיוניים במגזרי המשק המרכזיים השונים דוגמת מגזר האנרגיה, הבריאות, התחבורה, התקשורת ועוד, כמו גם ביחס לארגונים שונים במגזר השירותים הדיגיטליים ושירותי האחסון. מדובר בארגונים שפוטנציאל הפגיעה בהם, מעצם מהותם, חורג מהנזק העלול להיגרם לארגון הבודד שנתקף, ועלול להביא לפגיעה רחבה יותר בציבור או במשק. בהקשר זה, הערכת הגורמים המקצועיים היא כי היקף תקיפות הסייבר האמורות לא יפחת, ולכן נדרשת חקיקה שתבטיח את ההגנה הנדרשת בסייבר על הארגונים, ועל ידי כך תבטיח הגנה גם על המשק, על החוסן הלאומי, על ביטחון המדינה, על ביטחון הציבור ועל רציפות אספקתם של שירותים חיוניים.

על אף חומרת הסיכון הנשקף מתקיפות סייבר והנזקים שעלולים להיגרם מהן, כמו גם התועלת הברורה שבהתגוננות מפני תקיפות ומניעתן לעומת התמודדות עם השלכות התקיפה ועלויות ההתאוששות והשיקום לאחריה, ארגונים רבים במשק הישראלי לא נוקטים אמצעים מספקים להגנה בסייבר, בעיקר לנוכח אי־הפנמת הסיכון הגלום בתקיפות כאמור. הדבר מביא לעלייה משמעותית בהסתברות למתקפות סייבר מזיקות ובעלות השלכות קשות.

לנוכח הסיכון וכשלי השוק, קיימת זה מכבר במרבית מדינות המערב אסדרה מתקדמת בתחום הגנת הסייבר. אסדרה כאמור קיימת במדינות דוגמת בריטניה, אוסטרליה וקנדה, וכן במדינות האיחוד האירופי. הדירקטיבה האירופית בנושא הגנת סייבר (NIS Directive) שהתקבלה בשנת 2016, עודכנה בשנת 2022 ומיושמת בהתאם ללוח הזמנים המדורג שנקבע בה. הדירקטיבה העדכנית (NIS2) הרחיבה את מספר המגזרים המפוקחים ואת היקף הגופים המפוקחים בכל מגזר, וכן חיזקה את סמכויות הפיקוח והאכיפה, זאת נוסף על החובות שכבר מוטלות על המדינות מתוקף NIS Directive, ובהן גיבוש אסטרטגיית הגנת סייבר, הקמת גופים לאומיים מוסמכים בתחום הסייבר וגיבוש אסדרה לתשתיות קריטיות וחיוניות.

בישראל, על אף חשיבותו המכרעת של מרחב הסייבר, בולטת בהעדרה מסגרת חקיקתית, ייעודית ומקיפה, המסדירה את התחום בראייה לאומית. מצב זה יוצר פער משמעותי בין רמת האיום הגבוהה לבין ההגנה הנדרשת על נכסים ותשתיות בעלי חשיבות לאומית. סיכוני הסייבר בישראל והשלכותיהם האפשריות, ובהתאם לכך החיוניות של חקיקה לאומית הנדרשת לאסדרת תחום זה, קיבלו ביטוי, בין השאר, בדוחות שונים של מבקר המדינה.

מטרת החוק המוצע היא להביא להגנה לאומית טובה יותר על תפקודו הרציף והבטוח של מרחב הסייבר הלאומי, כחלק מחוסנה וביטחונה הלאומי של מדינת ישראל, בדגש על הגנת ארגונים חיוניים וספקי שירותים דיגיטליים ושירותי אחסון כהגדרתם המוצעת בחוק. החוק המוצע מבוסס על הצרכים והאיומים בראייה לאומית, על החלטות הממשלה ומדיניותה בתחום הגנת הסייבר, על התפיסה העומדת בבסיס החלטות הממשלה האמורות ועל הניסיון שנצבר מאז קבלתן, זאת בייחוד לנוכח לקחי מלחמת "חרבות ברזל" והלחימה מול איראן במסגרת מבצע "עם כלביא" בחודש יוני 2025 ומבצע "שאגת הארי" בחודשים פברואר עד אפריל 2026.

מדובר בהסדר המבוסס על ניהול סיכונים ואיזון רגולטורי בהתאם לרמת הסיכון הנשקפת בכל מגזר, ומתמקד בעיקר במגזרים המצויים בליבת הרציפות התפקודית והעסקית של המשק בישראל ובארגונים חיוניים הפועלים בהם.

"ארגון" – מוסד כהגדרתו בסעיף 35 לפקודת הראיות [נוסח חדש], התשל"א–1975[1];

"ארגון חיוני" – כמשמעותו בסעיף 8(א);

"ארגון חיוני למערכת הביטחון" – ארגון שקבע שר הביטחון לפי סעיף 20;

"גוף מונחה" – גוף המנוי בפרטים 2 ו־3 לתוספת הראשונה לחוק להסדרת הביטחון בגופים ציבוריים, וכן גוף המנוי בתוספת הרביעית או בתוספת החמישית לאותו חוק;

"הגופים המיוחדים" – מערך הסייבר הלאומי, משרד הביטחון לרבות הממונה על הביטחון במערכת הביטחון, צה"ל, שירות הביטחון הכללי, המוסד למודיעין ולתפקידים מיוחדים ומשטרת ישראל;

"גוף ממשלתי" – גוף כאמור בטור א' לתוספת השנייה, לרבות יחידותיו ויחידות הסמך שלו, ולמעט גוף מהגופים המיוחדים וגוף מונחה; לעניין זה, "גוף מונחה" – למעט משרד האוצר בנושא שקבעה הממשלה כאמור בתוספת החמישית לחוק להסדרת הביטחון;

"גורם מאסדר של תחום הגנת הסייבר", "גורם מאסדר" – שר המנוי בטור ד' לתוספת הראשונה, האמון על האסדרה של תחום הגנת הסייבר במגזר המנוי בטור א' לצידו;

דברי הסבר

בהתאם לכך, מוצע לעגן בחוק את מסגרת האסדרה והפיקוח על הגנת הסייבר הלאומית, תוך עיגון רוחבי של סמכויות וכלי הגנת הסייבר של המאסדרים הממשלתיים השונים, קביעת עקרונות פעולה מוגדרים ומנגנוני פיקוח ואסדרה סדורים. זאת, תוך קביעת חובות שיוטלו על הארגונים, בדגש על הארגונים החיוניים, לפעול להגנת הסייבר, הן בהעלאת חוסן בשגרה לשיפור רמת המוכנות והן בעת התמודדות עם תקיפת סייבר. כל זאת, תוך הקפדה על שימור הגמישות הנדרשת בשל ההתפתחות הטכנולוגית המתמדת והשוני בין ארגונים.

להשלמת התמונה יצוין כי החוק המוצע נועד להביא לאסדרה של הגנת הסייבר הלאומית בראייה כוללת, כהשלמה להסדרה הלאומית הקיימת לעניין תשתית מדינה קריטית בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998 (להלן – חוק להסדרת הביטחון), וכן כהשלמה להסדרים החלים במגזרים השונים במשק, אם קיימים.

פרק א': הגדרות

סעיף 1 ותוספות ראשונה ושנייה

בסעיף זה מוצע להגדיר מונחים שונים שנעשה בהם שימוש בחוק המוצע.

מוצע להגדיר את המונח "ארגון" בחוק המוצע כמוסד כהגדרתו בסעיף 35 לפקודת הראיות [נוסח חדש], התשל"א–1975. לפי הגדרה מוצעת זו, ארגון הוא מונח הכולל את המדינה, רשות מקומית, וכן כל עסק או כל מי שמספק שירות לציבור.

בהגדרה "הגופים המיוחדים" מוצע לכלול את משטרת ישראל, שירות הביטחון הכללי, המוסד למודיעין ולתפקידים מיוחדים, מערך הסייבר הלאומי ומשרד הביטחון לרבות הממונה על הביטחון במערכת הביטחון (להלן – מלמ"ב) ויחידות הסמך של משרד הביטחון וצבא ההגנה לישראל, אשר בהתאם למוצע, הוראות חוק זה לא יחולו עליהם.

כמו כן, מוצע להגדיר "גוף מונחה" כגוף המנוי בפרטים 2 ו־3 לתוספת הראשונה לחוק להסדרת הביטחון, כלומר משרד הביטחון ו"מפעלי מערכת הביטחון" כפי שיוגדרו בצו בידי שר הביטחון, וכן גוף המנוי בתוספת הרביעית או בתוספת החמישית לחוק האמור. גם גופים מונחים מוחרגים על פי המוצע מהוראות החוק, והם ימשיכו להיות כפופים להוראות מכוח החוק להסדרת הביטחון שקובעות רמת הגנת סייבר גבוהה התואמות לרמת הסיכון בהם.

המונחים "מגזר", "גורם מאסדר של תחום הגנת הסייבר" או "גורם מאסדר" ו"הרשות המוסמכת" יוצרים את התשתית לאסדרה הדיפרנציאלית של הגנת הסייבר בתחומי הפעילות השונים במשק, כמו גם בפעילות משרדי הממשלה. כך, לצד ההגדרה של "מגזר", מוצע לקבוע את הרשות המוסמכת, מנהל הרשות המוסמכת והגורם המאסדר שיפעלו ביחס לכל מגזר, הכול כפי שיפורט להלן.

על פי המוצע, "מגזר" הוא תחום פעילות במשק, המנוי בטור א' לתוספת הראשונה, או תחום פעילות משרדי הממשלה, כמפורט בטור א' לתוספת השנייה. על פי המוצע, ארגונים הפועלים במגזרים אלה, העומדים בתנאים המוצעים בתוספת השלישית, יוגדרו כארגונים חיוניים לעניין החוק המוצע.

עוד מוצע להגדיר את המונח "גורם מאסדר של תחום הגנת הסייבר" בהתייחס למגזרים המנויים בתוספת הראשונה. על פי המוצע, גורם מאסדר כאמור הוא שר,

[1] דיני מדינת ישראל, נוסח חדש 18, עמ' 421.

"חומר מחשב", "מחשב", "פלט" ו"תוכנה" – כהגדרתם בחוק המחשבים;

"חוק האזנת סתר" – חוק האזנת סתר, התשל"ט–1979[2];

"חוק הגנת הפרטיות" – חוק הגנת הפרטיות, התשמ"א–1981[3];

"חוק המחשבים" – חוק המחשבים, התשנ"ה–1995[4];

"חוק להסדרת הביטחון בגופים ציבוריים" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998[5];

"חוק העונשין" – חוק העונשין, התשל"ז–1977[6];

"יחידת סייבר מגזרית" – כמשמעותה בסעיף 5;

"מגזר" – כל אחד מאלה:

(1) תחום פעילות במשק המנוי בטור א' לתוספת הראשונה;

(2) תחום פעילות הממשלה, כמפורט בטור א' לתוספת השנייה;

"מידע אישי" – כהגדרתו בחוק הגנת הפרטיות;

"מנהל בכיר במערך" – עובד בכיר במערך הסייבר הלאומי, שדרגתו ראש אגף לפחות, אשר ראש מערך הסייבר הלאומי הסמיך לעניין חוק זה;

"מנהל בכיר ברשות מוסמכת" – עובד בכיר ברשות מוסמכת שדרגתו ראש אגף לפחות, אשר מנהל הרשות המוסמכת הסמיך לעניין חוק זה;

"מנהל הרשות המוסמכת" – המנהל או המנהל הכללי של רשות מוסמכת או גורם אחר העומד בראש רשות מוסמכת, המנוי בטור ג' לתוספת הראשונה או לתוספת השנייה לצד אותה רשות;

דברי הסבר

המנוי בטור ד' לתוספת הראשונה, האמון על האסדרה של היבט הגנת הסייבר במגזר המנוי לצידו.

מוצע להגדיר "רשות מוסמכת" כמשרד ממשלתי, יחידה או יחידת סמך במשרד כאמור או תאגיד שהוקם בחוק, המנויים בטור ב' לתוספת הראשונה או השנייה, המוסמכים לעניין פעילות בתחום הגנת הסייבר של ארגונים הפועלים במגזר המנוי בטור א' לאותה תוספת. כלומר, הסמכויות יוקנו לרשות המוסמכת ביחס למגזר מסוים.

יצוין כי בהתאם למוצע בתוספת השנייה, מערך הדיגיטל הלאומי יהיה "רשות מוסמכת" לעניין החוק המוצע, בכל הנוגע לפעילות של גופים ממשלתיים (כאמור, למעט הגופים המיוחדים וגופים מונחים, ולעניין זה, "גוף מונחה" – למעט משרד האוצר בנושא שקבעה הממשלה כאמור בתוספת החמישית לחוק להסדרת הביטחון) שאינה נוגעת למידע מסווג. כמו כן מוצע למעט מהגופים הממשלתיים שמערך הדיגיטל יהיה הרשות המוסמכת לגביהם את משרד ראש הממשלה ואת משרד החוץ שמוצע לגביהם הסדר בסימן ה' בפרק ה' לחוק המוצע, וכן בתי חולים ממשלתיים אשר פועלים במגזר הבריאות שנכלל בתוספת הראשונה לחוק המוצע (פרט 3), ולכן מהווים ארגון חיוני.

על פי המוצע, "מנהל הרשות המוסמכת" הוא המנהל או המנהל הכללי של הרשות המוסמכת או גורם אחר העומד בראש רשות כאמור, המנוי בטור ג' לתוספת הראשונה או השנייה לצד אותה רשות. בין השאר, מוצע כי מנהל הרשות המוסמכת יסמיך עובדים מוסמכים מגזריים שיפעילו סמכויות פיקוח לפי החוק המוצע (ראו דברי ההסבר לפרק ד' לחוק המוצע).

נוסף על כך, מוצע להגדיר "מנהל בכיר במערך" כעובד בכיר במערך הסייבר הלאומי (להלן – מערך הסייבר הלאומי או המערך) שדרגתו ראש אגף לפחות, שיוסמך לעניין החוק המוצע בידי ראש מערך הסייבר הלאומי (להלן – ראש המערך).

כמו כן, מוצע להגדיר "מנהל בכיר ברשות מוסמכת" כעובד בכיר ברשות מוסמכת שדרגתו ראש אגף לפחות, אשר מנהל אותה רשות מוסמכת הסמיך לעניין החוק המוצע.

[2] ס"ח התשל"ט, עמ' 118.
[3] ס"ח התשמ"א, עמ' 128.
[4] ס"ח התשנ"ה, עמ' 366.
[5] ס"ח התשנ"ח, עמ' 348.
[6] ס"ח התשל"ז, עמ' 226.

"נכס מידע משמעותי" – מידע או מאגר מידע שתקיפת סייבר נגדו עלולה להביא לפגיעה חמורה בביטחון המדינה או בשלום הציבור;

"ספק שירותים דיגיטליים או שירותי אחסון" – אחד מאלה:

(1) ארגון שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, ומתקיים חיבור פיזי או לוגי, קבוע או עיתי, או שמתבצעת העברת חומר מחשב קבועה או עיתית, ממחשביו למחשבי מקבל השירות;

(2) ארגון שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי אחסון או שירותים דיגיטליים;

"עובד המדינה" – כהגדרתו בסעיף 7 לפקודת הנזיקין [נוסח חדש], התשכ"ח–1968[7];

"עובד מוסמך במערך" – כמשמעותו בסעיף 6(א);

"עובד מוסמך מגזרי" – כמשמעותו בסעיף 6(ב);

"פגיעות חמורה" – נקודת תורפה במחשב או בחומר מחשב שאפשר לנצל לביצוע תקיפת סייבר (Vulnerability), ושעובד המערך מצא כי בשל מאפייניה נוצר סיכון משמעותי לתקיפת סייבר;

"פעולה להגנת סייבר בחומר מחשב" – מתן הוראות למחשב בשפה קריאת מחשב לשם הגנת סייבר, ובכלל זה הוראה לסריקה, לעיבוד או להסרה של חומר מחשב הנוגע לתקיפת סייבר, להתקנת תוכנה מסוג שפעולתו מוגבלת לרשת הארגון בלבד, לחסימה או לניתוק של מחשב או ליצירת עותק של חומר המחשב;

"צה"ל" – צבא הגנה לישראל;

דברי הסבר

מנהל בכיר במערך הסייבר הלאומי ומנהל בכיר ברשות מוסמכת, מוסמכים בין השאר, לפי העניין, לקבל דיווחים של ארגונים חיוניים על תקיפות משמעותיות נגדם בהתאם למוצע בסעיף 12 להצעת החוק; לקבוע שתקיפת סייבר היא תקיפה חמורה, לדרוש ידיעות ומסמכים לשם קבלת החלטה אם תקיפה היא תקיפה חמורה, ועוד.

עוד מוצע להגדיר את המונחים "עובד מוסמך במערך" ו"עובד מוסמך מגזרי". עובדים אלה מקבלים את הסמכתם לפי סעיף 6(א) ו־(ב) לחוק המוצע, בהתאמה.

מוצע לעשות שימוש במונחים שונים מחוק המחשבים, התשנ"ה–1995 (להלן – חוק המחשבים) ובהם המונחים "חומר מחשב", "מחשב", "פלט", ו"תוכנה". זאת בשים לב לפרשנות של אותם מונחים כאמור מחוק המחשבים בפסיקה, אשר מייחסים משקל גם להתפתחות הטכנולוגית המהירה, ולהמשיך וליחס משקל להתפתחות הטכנולוגית בפרשנות עתידית של מונחים אלה. כך, נקבע בפסיקה כי בגדרי "מחשב" נכללים מגוון רחב של מכשירים דיגיטליים, לרבות טלפונים חכמים, מצלמות, וכן רשת המחשבים ורכיבי תקשורת בין מחשבים. נוסף על כך, נקבע בפסיקה כי בגדרי "חומר מחשב" נכללים מגוון רחב של תכנים המאוחסנים במכשירים שונים, לרבות מידע דיגיטלי מכל סוג המעובד במערכות הממוחשבות גם אם הוא מוצג למשתמש בשפה אנושית וכן נתוני שליטה ותפעול של מערכות. כמו כן, נקבע בפסיקה כי בגדרי המונח "פלט" נכללים כל הנתונים המוצגים מתוך המחשב, בכל צורה שהיא, לרבות תמונות, וידאו ושמע, וכי בגדרי המונח "תוכנה" נכללים כלל היישומים והוראות ההפעלה המאפשרים את פעולת המחשב ועיבוד הנתונים בו וחלקי תוכנה שאינם באים לידי ביטוי בקוד הכתוב, בלא הבדל בין צורות שונות של תוכנה (ראו לדוגמה בש"פ 1758/20 אוריך נ' מדינת ישראל (אר"ש, 26.1.2021); דנ"פ 1062/21 אוריך נ' מדינת ישראל (נבו, 11.1.2022); בש"פ 6071/17 מדינת ישראל נ' רונאל (נבו, 27.8.2017); רע"פ 8464/14 מדינת ישראל נ' עזרא (נבו, 15.12.2015); ע"פ 1242/06 צור נ' מדינת ישראל, פ"ד סב(2) 271 (נבו, 13.6.2007); בש"פ 2235/24 פלד נ' מדינת ישראל (נבו, 15.12.2024); ע"א 2392/99 אשרז עיבוד נתונים בע"מ נ' טרנסבטון בע"מ, פ"ד נז(5) 255 (נבו, 22.7.2003); ה"ס 82202–07–25 בלוק נ' מדינת ישראל (נבו, 8.3.2026)).

על פי המוצע, "נכס מידע משמעותי" הוא מידע או מאגר מידע שתקיפת סייבר נגדו עלולה להביא לפגיעה בביטחון המדינה או בשלום הציבור. פגיעה במהימנות או בזמינות נכס מידע משמעותי או זליגתו, עלולות להיות בעלות השלכות הרות גורל על ביטחון המדינה או ביטחון הציבור. בהתאם, וכפי שיפורט להלן, אחת העילות שבהתקיימן תוטל חובה על ארגון חיוני לדווח על תקיפת סייבר משמעותית לרשות המוסמכת ולמערך הסייבר

[7] דיני מדינת ישראל, נוסח חדש 10, עמ' 266.

"רשות מוסמכת", "רשות" – כל אחת מאלה:

(1) משרד ממשלתי, יחידה או יחידת סמך במשרד כאמור או תאגיד שהוקם בחוק, המנויים בטור ב' לתוספת הראשונה, אשר מוסמכים לעניין פעילות בתחום הגנת הסייבר של ארגונים הפועלים במגזר המנוי בטור א' לצידם;

(2) משרד ממשלתי, יחידה או יחידת סמך במשרד כאמור, המנויים בטור ב' לתוספת השנייה, אשר מוסמכים לעניין פעילות בתחום הגנת הסייבר של ארגונים הפועלים במגזר המנוי בטור א' לצידם;

"רשות מקומית" – עירייה, מועצה אזורית או מועצה מקומית;

"שירותי אחסון" – שירותי אחסון של חומר מחשב הניתנים בעבור אחר, או שירותי אספקת תשתית לאחסון או לעיבוד של חומר מחשב;

"שירותים דיגיטליים" – שירות שהוא אחד מאלה, הניתן בעבור אחר:

(1) שירותי תוכנה, לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח של תוכנה, למעט תוכנה הניתנת כשירות (SAAS) באמצעות מחשוב ענן (Cloud Computing) על ידי ארגון שמחזור העסקאות השנתי שלו בישראל אינו עולה על 5 מיליון שקלים חדשים;

(2) שירותי ניהול או הפעלה של מערכות מחשבים המשלבות חומרה, תוכנה וטכנולוגיות תקשורת;

(3) שירותי עיבוד נתונים, הזנתם או שחזורם, התקנה והגדרת תצורה של מחשבים, התקנת תוכנה או שירותי הגנת סייבר;

(4) אספקה או התקנה של מחשבים או של ציוד בקרה, המהווים חלק ממכונות וציוד תעשייתי;

דברי הסבר

הלאומי, לפי סעיף 12 לחוק המוצע, היא שהתקיפה עלולה להביא לפגיעה בנכס מידע משמעותי או לגישה של גורם שאינו מורשה לנכס כאמור. נוסף על כך מוצע, בסעיף 13 לחוק המוצע, לקבוע, כאחת החלופות להגדרת תקיפת סייבר כתקיפת סייבר חמורה, תקיפה שעלולה לאפשר גישה לגורם שאינו מורשה לנכס מידע משמעותי של ארגון חיוני.

מוצע להגדיר "שירותי אחסון" כשירותי אחסון של חומר מחשב הניתנים בעבור אחר, או שירותי אספקת תשתית לאחסון או לעיבוד של חומר מחשב. כמו כן מוצע להגדיר "שירותים דיגיטליים" כאחד משורה של השירותים המנויים בהגדרה, הניתן בעבור אחר. בהמשך לכך, מוצע להגדיר מי ייחשב ל"ספק שירותים דיגיטליים או שירותי אחסון".

על פי המוצע, "פגיעות חמורה" היא נקודת תורפה במחשב או בחומר מחשב שאפשר לנצל לביצוע תקיפת סייבר, אשר עובד מערך הסייבר הלאומי מצא כי בשל מאפייניה נוצר סיכון משמעותי לתקיפת סייבר. יובהר כי בהפעלת שיקול דעתו, ייקח העובד בחשבון, בין השאר, את מאפייניה הטכנולוגיים של הפגיעות, קיומן של שיטות ואמצעים לניצולה לתקיפת סייבר או העדר שיטות ואמצעים למנוע את ניצולה לתקיפת סייבר, את שכיחותה הפוטנציאלית של הפגיעות ואת סוגי הארגונים שבהם היא עלולה להימצא. זאת, לצד שימוש בשיטות מקובלות בעולם לקביעת רמת החומרה של הפגיעות, דוגמת CVSS ובפרסומים גלויים לגבי ניצול פגיעויות (Vulnerabilities) בעולם. כפי שיפורט להלן בדברי ההסבר לסעיף 50 לחוק המוצע, מוצע לעגן בו את פעילות מערך הסייבר הלאומי לאיתור פגיעויות חמורות המוכרות למערך ולמתן התרעה עליהן.

כמו כן, מוצע להגדיר "פעולה להגנת סייבר בחומר מחשב" כמתן הוראות למחשב בשפה קריאת מחשב לשם הגנת סייבר, ובכלל זה הוראה לסריקה, לעיבוד או להסרה של חומר מחשב הנוגע לתקיפת סייבר, להתקנת תוכנה מסוג שפעולתו מוגבלת לרשת הארגון בלבד, לחסימה או לניתוק של מחשב או ליצירת עותק של חומר המחשב. כפי שיפורט להלן, הגדרה זו מתייחסת לסמכויות שיהיה ניתן להפעיל בנסיבות שבהן ארגון הותקף בתקיפה חמורה ולא פעל באופן הולם לצורך איתור התקיפה, מניעתה או בלימתה.

מוצע להגדיר "תקיפת סייבר" כפעולה שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב השמור בו, ומוצע למנות שורה של פעולות שעשויות להיחשב לתקיפה כאמור. כפי שיפורט להלן, הגדרה זו מהווה את הבסיס להגדרת תקיפת סייבר משמעותית או תקיפת סייבר חמורה לפי החוק המוצע.

"תקיפת סייבר" – פעולה שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב השמור בו, לרבות –

(1) שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;

(2) מחיקת חומר מחשב, שינויו, שיבושו, פגיעה במהימנותו או הפרעה לשימוש בו;

(3) חדירה שלא כדין לחומר מחשב, כהגדרתה בסעיף 4 לחוק המחשבים;

(4) האזנת סתר לתקשורת בין מחשבים, כמשמעותה בחוק האזנת סתר;

(5) גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הוצאה שלא כדין של מידע כאמור לרבות בדרך של העתקתו על ידי גורם כאמור;

(6) הפרעה או מניעת נגישות של מחשב לרשת תקשורת.

פרק ב': מערך הסייבר הלאומי

מערך הסייבר הלאומי

2. (א) במשרד ראש הממשלה יפעל גוף מבצעי־טכנולוגי, שיהיה מופקד על קידום הגנת הסייבר הלאומית, ובכלל זה, בהתאם לצורך, על תיאום והפעלה של מאמצי הגנת הסייבר הלאומית ועל ביצוע של פעולות הנדרשות לכך (בחוק זה – מערך הסייבר הלאומי או המערך).

(ב) המערך יהיה עצמאי בהפעלת סמכויותיו לשם מילוי תפקידיו לפי חוק זה.

(ג) ראש הממשלה הוא השר הממונה על מערך הסייבר הלאומי מטעם הממשלה.

תפקידי מערך הסייבר הלאומי

3. (א) לעניין סעיף 2 יפעל מערך הסייבר הלאומי, בין השאר –

(1) ליזום ולקדם מדיניות ואסטרטגיה לאומית בתחום הגנת הסייבר;

(2) לגבש תמונת מצב של רמת הגנת הסייבר הלאומית;

דברי הסבר

פרק ב': מערך הסייבר הלאומי

סעיף 2 הגנת סייבר לאומית אפקטיבית מבוססת, בין השאר, על ניהול ותכלול לאומי של תחום הגנת הסייבר, על מכלול היבטיו, בעשייה של כלל השותפים הנוגעים לעניין. להבדיל מטיפול מגזרי נפרד לשם כך, פועל מערך הסייבר הלאומי, למעלה מעשור, בכמה אפיקים ובהם ביצוע פעולות להגנה על המשק מפני תקיפות סייבר, קידום רמת ההגנה והחוסן בשגרה, תכלול הניהול הלאומי של מאמצי הגנת הסייבר, ועוד. עד כה הוסדרה עיקר פעילותו של מערך הסייבר הלאומי בהחלטות ממשלה, לרבות בהחלטת ממשלה מס' 2443, שעניינה "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" מיום כ"ו בשבט התשע"ה (15 בפברואר 2015) (להלן – החלטת ממשלה 2443), בהחלטת ממשלה מספר 2444, שעניינה "קידום ההיערכות הלאומית להגנת הסייבר" מיום כ"ו בשבט התשע"ה (15 בפברואר 2015) (להלן – החלטה 2444), ובחוק להסדרת הביטחון.

מוצע לעגן בחוק המוצע את מסגרת הפעילות של מערך הסייבר הלאומי, ובתוך כך לקבוע, בסעיף קטן (א) לסעיף המוצע, שבמשרד ראש הממשלה יפעל גוף מבצעי־טכנולוגי, שיהיה מופקד על קידום הגנת הסייבר הלאומית, ובכלל זה, בהתאם לצורך, על תיאום והפעלה של מאמצי הגנת הסייבר הלאומית ועל ביצוע של פעולות הנדרשות לכך. כמו כן, למען הסר ספק, מוצע לקבוע במפורש, בסעיף קטן (ב) לסעיף המוצע, כי המערך יהיה עצמאי בהפעלת סמכויותיו לשם מילוי תפקידיו. עוד מוצע לקבוע בסעיף קטן (ג) לסעיף המוצע כי ראש הממשלה הוא השר הממונה על מערך הסייבר הלאומי מטעם הממשלה.

סעיף 3 במסגרת הסדרת פעילות מערך הסייבר הלאומי, מוצע לקבוע, בסעיף קטן (א) לסעיף המוצע, תפקידים שימלא המערך. בין השאר, מוצע כי המערך ייזום ויקדם מדיניות ואסטרטגיה לאומית בתחום הגנת הסייבר (פסקה (1)), וכן יגבש תמונת מצב של רמת הגנת הסייבר הלאומית (פסקה (2)). תמונת מצב זו תגובש, בין השאר, בתיאום עם הגורמים הנוגעים לעניין.

תפקיד נוסף של המערך הוא, על פי המוצע, לפעול לחזק את החוסן הלאומי בהיבטי הגנת סייבר, ובכלל זה את המוכנות לתקיפות סייבר, ולשפר את ההתמודדות של המשק עם תקיפות סייבר (פסקה (3)). זאת, גם לעניין סיכונים בתחום הסייבר דוגמת תקיפות סייבר ופגיעויות.

(3) לחזק את החוסן הלאומי בהיבטי הגנת סייבר, ובכלל זה את המוכנות לתקיפות סייבר, ולשפר את ההתמודדות של המשק עם תקיפות סייבר;

(4) להעלות את המודעות בקרב הציבור להתנהגות בטוחה במרחב הסייבר, ולפרסם לציבור התרעות על סיכונים בתחום הסייבר (בחוק זה – סיכוני סייבר) והמלצות להעלאת רמת הגנת הסייבר;

(5) לקדם ולעודד פיתוח ידע ופתרונות בתחום הגנת הסייבר הלאומית;

(6) לקדם בחינה והטמעה של טכנולוגיות חדשות להגנת סייבר;

(7) לקדם שיתוף פעולה בתחום הגנת הסייבר במישור הבין־לאומי, בין השאר באמצעות כריתת הסכמי שיתוף פעולה בתחום הגנת הסייבר;

(8) לייעץ לראש הממשלה ולממשלה בתחום הגנת הסייבר.

(ב) לצורך ביצוע תפקידיו, מערך הסייבר הלאומי, בין השאר –

(1) יפעיל מרכז לאומי לסיוע בהתמודדות עם אירועי סייבר (Computer Emergency Response Team – CERT) (להלן – ה־CERT), הכולל, בין השאר, מרכז לקבלת דיווחים על תקיפות סייבר ופניות שעניינן הגנת סייבר, ומרכז לאומי לשליטה ובקרה על סיכוני סייבר (National Security Operations Center – NSOC) (להלן – ה־NSOC);

(2) ינחה מקצועית את יחידות הסייבר המגזריות, בין השאר לעניין אופן היישום השנתי והרב־שנתי של המדיניות והאסטרטגיה הלאומית בתחום הגנת הסייבר, לצורך שיפור רמת הגנת הסייבר במגזר שהן פועלות בו, ולעניין ההתמודדות במגזר עם תקיפות סייבר חמורות, ובכלל זה יפעל, בהתאם לכל דין או הסכם, לשתף עימן –

(א) תמונת מצב של רמת הגנת הסייבר הלאומית שגובשה לפי סעיף קטן (א)(2);

דברי הסבר

עוד מוצע כי המערך יפעל להעלות את המודעות בקרב הציבור להתנהגות בטוחה במרחב הסייבר, ולפרסם לציבור התרעות על סיכונים בתחום הסייבר (להלן – סיכוני סייבר) והמלצות להעלאת רמת הגנת הסייבר (פסקה (4)). נוסף על כך, מוצע כי המערך יפעל לקדם ולעודד פיתוח ידע ופתרונות בתחום הגנת הסייבר הלאומית (פסקה (5)), ולקדם בחינה והטמעה של טכנולוגיות חדשות להגנת סייבר (פסקה (6)). יצוין כי תפקיד זה נדרש לנוכח קצב התפתחות הטכנולוגיה המשפיע על היכולות ועל הדרכים לביצוע תקיפות במרחב הסייבר, הצורך להבטיח את המשך הימצאותה של מדינת ישראל בחזית הטכנולוגית העולמית של הגנת סייבר וכן לנוכח התפתחויות טכנולוגיות נוספות המשפיעות על תחום הגנת הסייבר, דוגמת התפתחות הבינה המלאכותית והמחשוב הקוואנטי.

תפקיד נוסף של המערך הוא לפעול לקדם שיתוף פעולה בתחום הגנת הסייבר במישור הבין־לאומי, בין השאר, באמצעות כריתת הסכמי שיתוף פעולה בתחום הגנת הסייבר (פסקה (7)). זאת, בהתאם לכללים ולנהלים הרלוונטיים ולפרקטיקה המקובלת בתחום, לרבות התקנון לעבודת הממשלה והנחיית היועצת המשפטית לממשלה מספר 10.300, שעניינה "התקשרות המדינה בהסכמים בין־לאומיים ועבודה משפטית במסגרת גופים בין־לאומיים".

לבסוף, מוצע למנות בסעיף את תפקידו של המערך כגורם שמייעץ לראש הממשלה ולממשלה בתחום הגנת הסייבר (פסקה (8)).

עוד מוצע לעגן בחוק המוצע את פעילות המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר (Computer Emergency Response Team – CERT) (להלן – ה־CERT) כחלק מהפעילות שהמערך מבצע לצורך מילוי תפקידיו. על פי המוצע, המרכז האמור כולל, בין השאר, מרכז לקבלת דיווחים על תקיפות סייבר ופניות שעניינן הגנת סייבר, ומרכז לאומי לשליטה ובקרה על סיכוני סייבר (National Security Operations Center – NSOC) (להלן – ה־NSOC).

נוסף על כך, ובמסגרת עיגון האסדרה הלאומית של תחום הגנת הסייבר בחוק המוצע, מוצע לקבוע שלשם ביצוע תפקידיו, מערך הסייבר הלאומי ינחה מקצועית את יחידות הסייבר המגזריות, כמפורט בסעיף קטן (ב)(2) לסעיף המוצע, וכן יפעל לשתף עימן, בהתאם לכל דין והסכם,

(ב) הערכות מקצועיות של המערך ומידע, ובכלל זה מידע על תקיפות סייבר והתרעות, לרבות התרעות לעניין פגיעויות חמורות, שהמערך מצא כי הם נדרשים להגנת הסייבר באותו מגזר;

(ג) אמצעים טכנולוגיים העומדים לרשות המערך, שהמערך מצא כי הם נדרשים להגנת הסייבר באותו מגזר.

ראש מערך הסייבר הלאומי

4. (א) הממשלה, לפי הצעת ראש הממשלה, תמנה את ראש מערך הסייבר הלאומי, בהתאם להוראות חוק שירות המדינה (מינויים), התשי"ט–1959[8].

(ב) ראש מערך הסייבר הלאומי מופקד על ניהול המערך ועל ביצוע תפקידיו, ויהיו נתונות לו כל הסמכויות הנתונות בחוק זה לעובדי המערך.

(ג) ראש מערך הסייבר הלאומי רשאי לאצול למנהל בכיר במערך סמכות הנתונה לו לפי חוק זה, למעט הסמכות לפי סעיף 11(א).

פרק ג': יחידת סייבר מגזרית

יחידת סייבר מגזרית

5. ברשות מוסמכת תפעל יחידה שמטרתה קידום הגנת הסייבר במגזר שבתחום פעילותה של הרשות, בהתאם להנחיה המקצועית של מערך הסייבר הלאומי, ובין תפקידיה –

(1) לפעול לשיפור רמת הגנת הסייבר במגזר בהתאם למדיניות ולאסטרטגיה הלאומית בתחום הגנת הסייבר, בין השאר באמצעות קידום קביעתם, בידי הגורם הממונה ברשות המוסמכת מכוח סמכות הנתונה לו לפי דין, של חיקוקים, הוראות או הנחיות מקצועיות בתחום האמור, שיחולו לעניין ארגונים במגזר או חלק ממנו;

(2) למפות באופן שוטף את הארגונים החיוניים במגזר;

דברי הסבר

תמונת מצב של רמת הגנת הסייבר הלאומית, הערכות מקצועיות של המערך ומידע, ובכלל זה מידע על תקיפות סייבר והתרעות שהמערך מצא כי הם נדרשים להגנת הסייבר באותו מגזר, וכן אמצעים טכנולוגיים העומדים לרשות המערך אם מצא שהם נדרשים להגנת הסייבר באותו מגזר.

יובהר כי אין באמור לעיל כדי לגרוע מתפקידים שממלא מערך הסייבר הלאומי מכוח הוראות של דינים אחרים, ובכלל זה החוק להסדרת הביטחון, וכן מכוח החלטות הממשלה, כגון תפקידו של המערך לשמש נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק.

סעיף 4 מוצע לקבוע בסעיף קטן (א) לסעיף המוצע שראש מערך הסייבר הלאומי ימונה על ידי הממשלה, לפי הצעת ראש הממשלה, בהתאם להוראות חוק שירות המדינה (מינויים), התשי"ט–1959 (להלן – חוק שירות המדינה (מינויים)).

יצוין כי חוק זה אינו גורע מהחלטת ממשלה מספר 3270 מיום כ"ט בכסלו התשע"ח (17 בדצמבר 2017), שעסקה במבנה הארגוני ובתפקידים ותנאי שכר במערך הסייבר הלאומי (להלן – החלטת ממשלה 3270), ונקבע בה, בין השאר, כי ראש המערך יהיה בעל מומחיות, רקע וניסיון בתחומים הנוגעים לענייני הסייבר של מדינת ישראל. כמו כן, נקבע בהחלטת הממשלה האמורה פטור מחובת המכרז הפומבי למשרת ראש המערך, בהתאם לסעיף 21 לחוק שירות המדינה (מינויים). עוד נקבע שמינוי ראש המערך יהיה בידי ראש הממשלה, באישור הממשלה, לאחר קבלת חוות דעתה של ועדת המינויים בכל הנוגע לכישוריו של המועמד והתאמתו למשרה בהתאם להחלטת הממשלה מספר 345, שעניינה "משרות שהמינוי להן נעשה על ידי הממשלה או באישורה – פטור ממכרז לפי סעיף 21 לחוק שירות המדינה (מינויים), התשי"ט–1959" מיום ד' בתשרי התש"ס (14 בספטמבר 1999).

נוסף על כך, מוצע לקבוע בסעיף קטן (ב) לסעיף המוצע שראש המערך מופקד על ניהול המערך ועל ביצוע תפקידיו, ושיהיו נתונות לו כל הסמכויות הנתונות בחוק המוצע לעובדי המערך. בסעיף קטן (ג) לסעיף המוצע, מוצע לאפשר לראש המערך לאצול למנהל בכיר במערך את סמכויותיו לפי החוק המוצע, למעט הסמכות לתת, בנסיבות מסוימות, הוראות דחופות למניעת סיכון סייבר משמעותי בארגון חיוני לפי סעיף 11 לחוק המוצע, לרבות באופן שבו הוחל לפי סעיף 21 לחוק המוצע.

פרק ג': יחידת סייבר מגזרית

סעיף 5 מודל האסדרה הממשלתי הקיים בישראל בתחום הגנת הסייבר, המבוסס בעיקרו על החלטת ממשלה 2443, הוא במהותו מודל מבוזר ברובו, המקנה בעיקרו אחריות למאסדרים בקידום הגנת הסייבר

[8] ס"ח התשי"ט, עמ' 86.

(3) לרכז את הנתונים לגבי רמת הגנת הסייבר בארגונים החיוניים במגזר, ולהעבירם למערך באופן שוטף, ולכל הפחות אחת לרבעון;

(4) לוודא שמבוצע פיקוח על ביצוע הוראות החוק וכן לוודא את קיומו של מנגנון לאכיפת ההוראות לפי החוק, לגבי המגזר;

(5) לפעול להנחיית ארגונים חיוניים במגזר לגבי טיפול בתקיפות סייבר חמורות, לרבות בדרך של מתן הוראות לארגון כאמור בידי הגורם המוסמך לכך לפי סימנים ג׳ ו־ד׳ לפרק ה׳;

(6) לקדם תהליכים של שיתוף מידע וידע מקצועי הנוגעים להגנת סייבר במגזר, בכפוף לכל דין, בין השאר בדרך של שיתוף מידע וידע כאמור עם ה־NSOC, לרבות באמצעות הפעלת מרכז לשליטה ובקרה על סיכוני סייבר (Security Operations Center) במגזר (להלן – SOC מגזרי);

(7) לפעול להעלאת המודעות לסיכוני סייבר במגזר, ולפרסם, בהתייעצות עם המערך, התרעות על סיכוני סייבר והמלצות להעלאת רמת הגנת הסייבר במגזר;

(8) להכין תוכנית עבודה שנתית או רב־שנתית, בין השאר בהתאם לעקרונות שהתווה המערך, ולאחר התייעצות עם המערך; תוכנית כאמור תאושר בידי מנהל הרשות המוסמכת והעתק ממנה יועבר למערך;

(9) להכין סיכום שנתי בדבר פעילות היחידה, שיכלול, בין השאר, את הנתונים שלהלן, ויועבר למערך:

(א) נתונים בעניינים האמורים בפסקאות (2) ו־(3);

(ב) נתונים בדבר פעולות לפיקוח ואכיפה שבוצעו כלפי ארגונים חיוניים במגזר, ובכלל זה הליכים להטלת עיצום כספי על ארגונים כאמור;

(ג) נתונים בדבר פעולות שבוצעו לפי פסקאות (6) ו־(7);

(ד) נתונים על תקיפות סייבר חמורות כהגדרתן בסעיף 13, נגד ארגונים במגזר;

(ה) נתונים על הוראות שניתנו לארגונים במגזר לפי סעיפים 14 או 15.

דברי הסבר

במגזר שהם אמונים על אסדרתו. הניסיון הנצבר מאז התקבלה ההחלטה האמורה בשנת 2015, מלמד שקיימת שונות רבה בין התשומות, המשאבים, היכולות והכלים שהמאסדרים השונים משקיעים בתחום הגנת הסייבר. שונות זו מביאה, בין השאר, לפערים ניכרים במצב הגנת הסייבר במגזרים שונים במשק. במהלך עבודת מטה שנערכה במסגרת גיבוש הצעת חוק זו, נבחנו שתי חלופות: האחת – מעבר למודל לאומי ריכוזי מובהק, שבו כלל הסמכויות נתונות בידי מערך הסייבר הלאומי; והשנייה – עיגון המודל הקיים, תוך מתן מענה לפערים הקיימים ודגש על תכלול לאומי בתחום הגנת הסייבר. בשים לב להיכרות המעמיקה של המאסדרים עם המגזרים שהם אמונים על אסדרתם, הוחלט לשמר ולעגן בחוק את המודל המבוזר שהותווה בהחלטת ממשלה 2443, תוך שימור, עיגון וחידוד של מודל ההנחיה הלאומי, לרבות ההנחיה המקצועית של מערך הסייבר הלאומי את היחידות המגזריות, הכול בשים לב לכך שהמערך הוא הגורם המדינתי בעל המיומנות והידע בתחום הגנת הסייבר, המחזיק בתמונה הלאומית הכוללת בתחום.

בהתאם, במסגרת האסדרה הלאומית של תחום הגנת הסייבר, מוצע, בין השאר, לעגן בחוק את ההסדר שלפיו ברשות מוסמכת תפעל יחידה שמטרתה קידום הגנת הסייבר במגזר שבתחום פעילותה של הרשות המוסמכת, וזאת בהתאם להנחיה המקצועית של מערך הסייבר הלאומי (להלן – יחידה מגזרית). בפסקאות (1) עד (9) של סעיף 5 לחוק המוצע, מוצע למנות באופן מפורט את עיקרי התפקידים שעל יחידות כאמור למלא, ויובהר כי הן עשויות למלא תפקידים נוספים, בהתאם לצורכי המגזר המסוים שלגביו הן פועלות.

פרק ד': עובדים מוסמכים

עובד מוסמך במערך הסייבר הלאומי ועובד מוסמך מגזרי

6. (א) ראש מערך הסייבר הלאומי רשאי להסמיך מקרב עובדי המערך, עובד, אחד או יותר, שיהיו נתונות לו הסמכויות הנתונות לעובד מוסמך במערך לפי חוק זה, כולן או חלקן, לשם ביצוע הוראות חוק זה.

(ב) מנהל הרשות המוסמכת רשאי להסמיך מקרב עובדי הרשות עובד, אחד או יותר, שיהיו נתונות לו הסמכויות הנתונות לעובד מוסמך מגזרי לפי חוק זה, כולן או חלקן, לשם ביצוע הוראות חוק זה.

תנאים להסמכת עובד מוסמך

7. לעובד מוסמך במערך או לעובד מוסמך מגזרי, יוסמך רק מי שמתקיימים בו כל אלה:

(1) משטרת ישראל הודיעה, לא יאוחר משלושה חודשים מיום קבלת פרטי העובד, כי היא אינה מתנגדת למינויו מטעמים של ביטחון הציבור, לרבות בשל עברו הפלילי;

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה ראש מערך הסייבר הלאומי;

(3) מנהל הרשות המוסמכת מצא שהוא בעל הידע והכישורים הנדרשים למילוי תפקידו בצורה נאותה, ובכלל זה ידע מעמיק בהגנת סייבר.

פרק ה': אסדרה לאומית בתחום הגנת הסייבר

סימן א': ארגון חיוני

ארגון חיוני – מהו

8. (א) ארגון חיוני הוא גוף שמתקיים לגביו אחד מאלה:

דברי הסבר

פרק ד': עובדים מוסמכים

סעיף 6 בסעיף 6(א) לחוק המוצע, מוצע לקבוע שראש מערך הסייבר הלאומי יוכל להסמיך מקרב עובדי המערך, עובד, אחד או יותר, שיהיו נתונות לו הסמכויות הנתונות לעובד מוסמך במערך לפי החוק המוצע, כולן או חלקן, זאת לשם ביצוע הוראות החוק המוצע, דוגמת סמכות למתן הוראות שתהיה נתונה לעובד מוסמך במערך בהתקיים התנאים הקבועים בסעיף 16 לחוק המוצע.

עוד מוצע כי מנהל רשות מוסמכת, יהיה רשאי להסמיך מקרב עובדי הרשות, עובד אחד או יותר, שיהיו נתונות לו הסמכויות הנתונות לעובד מוסמך מגזרי לפי החוק המוצע, כולן או חלקן, ויובהר כי העובדים האמורים יוכלו להפעיל את סמכויותיהם רק לתכלית של ביצוע הוראות החוק המוצע במגזר שהרשות המוסמכת (שמנהלה הסמיך אותם) פועלת לגביו. בסמכויות האמורות ניתן לציין את הסמכות לדרישת ידיעות ומסמכים שיש בהם כדי להבטיח את ביצוען של ההוראות לפי סעיף 23 לחוק המוצע; סמכות כניסה למקום לפי סעיף 24 לחוק המוצע לשם פיקוח על עמידה בהוראות סעיף 9(ב) עד (ה) לחוק המוצע שעניינו רמת הגנת סייבר בארגונים חיוניים, ובהוראות סעיף 12 לחוק המוצע שעניינו חובת דיווח על תקיפת סייבר משמעותית נגד ארגון חיוני; או סמכות לתת הוראות לארגון חיוני בעת תקיפת סייבר חמורה לפי הוראות סעיפים 14 ו־15 המוצעים, לפי העניין. מובהר כי במסגרת המודל הלאומי המבוזר, פעולות הפיקוח כלפי ארגונים חיוניים, כמו גם הטלת עיצומים עליהם, ייעשו על ידי עובדים מוסמכים מגזריים ברשויות המוסמכות, בלבד, ולא בידי עובדים מוסמכים במערך, אלא אם כן המערך הוא הרשות המוסמכת לגבי אותו מגזר.

סעיף 7 כדי להבטיח שהפעלת הסמכויות לפי החוק המוצע תיעשה בידי עובדים בעלי כשירות ומיומנים לכך, מוצע לקבוע כי יוסמך לעובד מוסמך במערך או לעובד מוסמך מגזרי, רק מי שמתקיימים בו התנאים המנויים בפסקאות (1) עד (3), שעניינם אישור משטרה (פסקה (1)), קבלת הכשרה מתאימה בתחום הסמכויות (פסקה (2)) והחזקה בידע וכישורים שמתאימים לדעת מנהל הרשות המוסמכת למילוי התפקיד, ובכלל זה ידע מעמיק בהגנת סייבר (פסקה (3)). על פי המוצע, ההכשרה הנדרשת כאמור בתחום הסמכויות, ובכלל זה תוכנה והיקפה, תיקבע בידי ראש המערך.

פרק ה': אסדרה לאומית בתחום הגנת הסייבר

סימן א': ארגון חיוני

סעיף 8 ותוספת שלישית כאמור, החוק המוצע בא להסדיר, בין השאר, את פעילותם של ארגונים חיוניים למשק בהיבטי הגנת סייבר, בחלוקה למגזרים השונים. בכלל זה, מבקש החוק המוצע להבטיח כי ארגון חיוני ינקוט את הפעולות הדרושות להבטחת רמת הגנת הסייבר הנדרשת לפי החוק, ידווח על תקיפות סייבר משמעותיות נגדו ויתמודד כנדרש עם תקיפות כאמור.

(1) הוא גוף ממשלתי;

(2) הוא ארגון הפועל במגזר או בתת־מגזר המנוי בטור א׳ או ב׳ לתוספת השלישית, שמתקיימים לגביו התנאים המפורטים בטור ג׳ לצידו, למעט גוף מונחה או ארגון שגורם מאסדר קבע, לפי הוראות סעיף קטן (ב), שלא יראו אותו לעניין חוק זה כארגון חיוני;

(3) הוא ארגון שגורם מאסדר קבע לפי הוראות סעיף קטן (ב) שיראו אותו לעניין חוק זה כארגון חיוני.

(ב) (1) גורם מאסדר רשאי, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, לקבוע כי ארגון הנמנה עם מגזר או עם תת־מגזר המנוי בטור א׳ או ב׳ לתוספת השלישית, שהגורם המאסדר אמון על האסדרה של תחום הגנת הסייבר בו, שאינו גוף מונחה או ארגון חיוני במגזר אחר, יראו אותו לעניין חוק זה כארגון חיוני אף על פי שלא מתקיימים לגביו התנאים המפורטים בטור ג׳ לצידו, אם מצא כי מתקיימות נסיבות חריגות המצדיקות קביעה כאמור, בהתחשב –

דברי הסבר

המגזרים שמוצע לכלול בשלב זה בהסדר המוצע בחוק, נוסף על משרדי הממשלה, הם: תקשורת; אנרגיה; מים וביוב; בריאות; כימיקלים, רעלים וחומרים מסוכנים; תחבורה; רשויות מקומיות; מזון ואספקת מוצרים ושירותים חיוניים; שירותים דיגיטליים ושירותי אחסון; וחקלאות. מגזרים אלה מצויים בליבת הרציפות התפקודית והעסקית של המשק בישראל. ההצעה לקבוע שארגונים מסוימים הפועלים במגזרים אלה ייחשבו לארגונים חיוניים לפי החוק המוצע, נשענת על כמה שיקולים, ובהם: מידת החיוניות של המגזר ביחס לרציפות התפקודית של המשק; מידת הבולטות שלו בהשוואה בין־לאומית; איום הייחוס; קיומה של תשתית אסדרתית הולמת במגזר להגנת סייבר; וכן שיקולים של ישימות תפעולית, לנוכח היותו של ההסדר המוצע בחוק הסדר ראשון מסוגו בישראל.

ככלל, מספר המגזרים שמוצע לכלול בהסדר המוצע בחוק נמוך ממספר המגזרים שכלולים בהסדרים דומים במדינות האיחוד האירופי. פער זה נובע מאימוץ גישה של אסדרה הדרגתית, ממוקדת ודיפרנציאלית, השואפת לאיזון רגולטורי המתאים לעת הנוכחית. בעוד הדירקטיבה האירופית (NIS2) שואפת להרמוניזציה רחבה וכוללת באסדרה גם מגזרים כגון מחקר וייצור של מוצרים שונים, המודל הישראלי מבקש לתת בשלב זה מענה ראשוני ודחוף לעניינים הנמצאים בליבת התפקוד של המשק ולשירותים שהפגיעה בהם עלולה להביא לנזק רחב. כמו כן יצוין כי הרחבת המגזרים המאוסדרים תחת הדירקטיבה האירופית העדכנית נעשתה בעיקרה בשלב השני של החקיקה. בשים לב למכלול השיקולים המתוארים לעיל, הוחלט, בין השאר, כי המגזר הפיננסי לא ייכלל בחוק המוצע, שכן במגזר זה קיימת תשתית נורמטיבית מבוססת ומתקדמת המעניקה מענה להיבטי הגנת הסייבר, ניהול סיכונים ורציפות תפקודית, וכמו כן יש לו מאפיינים תפעוליים ייחודיים, שבשלהם, יחד עם התשתית הנזכרת לעיל, ניתן לומר שלעת הזו, המענה הרגולטורי הקיים מספק.

בסעיף 8 לחוק המוצע, מוצע לקבוע את התנאים להגדרת ארגון כארגון חיוני לעניין החוק המוצע, בחלוקה למגזרים השונים. לצד זאת, מוצע לקבוע מנגנון המאפשר שינויים והתאמות למצבים חריגים, שבהם אף על פי שמתקיימים התנאים להגדרת הארגון כארגון חיוני, יהיה ניתן להחליט כי הוא לא ייחשב לכזה לעניין החוק המוצע, או לחלופין, למצבים שבהם אף על פי שלא מתקיימים התנאים האמורים, יהיה ניתן להגדיר את הארגון כארגון חיוני לעניין החוק המוצע, הכול כמפורט להלן.

לסעיפים קטנים (א) ו־(ו)

על פי המוצע בסעיף קטן (א)(1) לסעיף המוצע, כל גוף ממשלתי, לרבות יחידות הסמך שלו ובסייגים המפורטים בהגדרה "גוף ממשלתי" בסעיף 1 לחוק המוצע, קרי, שהוא אינו גוף מונחה ואינו נמנה עם הגופים המיוחדים כהגדרתם המוצעת, וכן בסייגים המנויים בטור א׳ לתוספת השנייה – הוא ארגון חיוני. להשלמת התמונה יצוין כי אף על פי שמשרד ראש הממשלה ומשרד החוץ נחשבים לארגון חיוני לפי החוק המוצע, כמו שאר משרדי הממשלה, הרי כאמור, לגבי משרדים אלה, למעט יחידות הסמך שלהם, מוצע שהגורם המוסמך יהיה שירות הביטחון הכללי (וראו לעניין זה גם את דברי ההסבר לסימן ה׳ בפרק ה׳). באופן דומה, מוצע שבתי חולים ממשלתיים ייחשבו לארגון חיוני לפי החוק לפי המגזר שעליו הם נמנים, ולא כגוף ממשלתי.

באשר לארגונים שאינם מוגדרים כ"גוף ממשלתי", מוצע לקבוע, בסעיף קטן (א)(2), שארגון שמתקיימים לגביו התנאים המפורטים בתוספת השלישית כנוסחה המוצע לעניין המגזר או תת־המגזר שבו הוא פועל (להלן – תנאים מגזריים), ייחשב לארגון חיוני לצורך ההסדר המוצע בחוק, זאת אלא אם כן הוא גוף מונחה או שהגורם המאסדר במגזר שבו הוא פועל קבע, לפי סעיף קטן (ב)(2) המוצע, שלא יראו אותו כארגון חיוני לעניין החוק המוצע. לצד זאת מוצע, בסעיף קטן (ב)(2) המוצע, לאפשר לגורם מאסדר

(א) בסוג הארגון, במאפייני פעילותו ובהשלכות האפשריות של תקיפת סייבר נגדו, ובכלל זה פגיעה בביטחון המדינה, בביטחון הציבור, בחיי אדם, בכלכלת המדינה או ברציפות אספקתם של שירותים חיוניים לציבור;

(ב) בשירות שמספק הארגון, ובכלל זה בהתחשב בחשיבות זמינות השירות, בחלופות לשירות, במספר המשתמשים הנזקקים לו, בנתח השוק של הארגון באספקת השירות, בפריסה הגאוגרפית של השירות או בתלות של ארגונים אחרים בשירות.

(2) גורם מאסדר רשאי, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, לקבוע כי ארגון הנמנה עם מגזר או עם תת־מגזר המנוי בטור א׳ או ב׳ לתוספת השלישית שהגורם המאסדר אמון על האסדרה של תחום הגנת הסייבר בו, לא יראו אותו לעניין חוק זה כארגון חיוני אף אם מתקיימים לגביו התנאים המפורטים בטור ג׳ לצידו, אם מצא כי מתקיימות נסיבות חריגות המצדיקות קביעה כאמור, כאמור בפסקה (1)(א) או (ב).

(3) גורם מאסדר יקבע כאמור בפסקאות (1) או (2) לאחר שקיבל את עמדת הוועדה המייעצת שהוקמה לפי פסקה (4); פנה גורם מאסדר לוועדה המייעצת לקבלת עמדה כאמור, תעביר אליו הוועדה את עמדתה בתוך 30 ימים מיום הפנייה.

(4) (א) תוקם ועדה מייעצת לעניין קביעת גורם מאסדר לפי פסקאות (1) או (2), שאלה חבריה:

(1) עובד בכיר ברשות המוסמכת, שיסמיך הגורם המאסדר, והוא יהיה היושב ראש;

(2) נציג מערך הסייבר הלאומי שיקבע ראש מערך הסייבר הלאומי;

(3) נציג משרד האוצר שיקבע שר האוצר;

דברי הסבר

לקבוע שארגון שלא מתקיימים לגביו התנאים הנזכרים לעיל, ייחשב לארגון חיוני לעניין החוק המוצע, ובהתאם, ארגון שנקבע לגביו כאמור, ייחשב גם הוא לארגון חיוני (סעיף קטן (א)(3)).

בהתאם לכלל המוצע לעניין ההגדרה של ארגון חיוני, שלפיו מדובר בהגדרה תלוית מגזר, מוצע לקבוע בתוספת האמורה, לעניין כל מגזר מהמגזרים הנזכרים לעיל, תנאים ייעודיים ודיפרנציאליים לארגון חיוני באותו מגזר. גישה זו נבחרה מתוך רצון להבטיח ניהול סיכונים מדויק ככל האפשר ורמה גבוהה של ישימות, כמו גם לנוכח הצורך בהסתגלות הדרגתית ובהתמקדות בגופים בעלי השפעה מערכתית. לעניין התנאים המגזריים, יצוין כי ככלל, דירקטיבת NIS2 מחילה את הוראותיה על ארגונים במגזר המסווגים כבינוניים (Medium–sized enterprises) ומעלה, בהתאם להגדרות האיחוד האירופי. תנאים אלה מהווים אמת מידה מרכזית לתחולת החובות הרגולטוריות באירופה, לצד שיקולים נוספים הנוגעים לאופי הפעילות, לרמת הסיכון ולמידת ההשפעה המערכתית של הארגון. בחוק המוצע, מוצע לקבוע בשלב זה תנאים מצומצמים בשים לב לשיקולים המתוארים לעיל.

כך לדוגמה, מוצע לקבוע כי במגזר התקשורת, ארגון חיוני יהיה ספק מורשה כהגדרתו בחוק התקשורת (בזק ושידורים), התשמ״ב–1982, ובלבד שיש לו 200,000 מנויים לפחות; במגזר האנרגיה, מוצע לקבוע כי ארגון חיוני בתחום החשמל יהיה, בין השאר, ארגון שבבעלותו או בשליטתו הישירה או העקיפה מיתקנים המשמשים לייצור חשמל בהספק מצטבר העולה על 100 מגה־וואט; ובמגזר המים והביוב מוצע לקבוע כי ארגון יהיה ארגון חיוני אם הוא (בין השאר) תאגיד מים כמשמעותו בחוק תאגידי מים וביוב, התשס״א–2001, שלו יותר מ־500,000 צרכנים.

בחלק מהמקרים מוצע לקבוע כמה תנאים חלופיים לקביעת החיוניות של הארגון באותו מגזר, כדי לתת מענה למגוון סוגי הפעילות בתוך המגזר, כמו גם לתלות האפשרית בשיקולים שונים המעידים על חשיבות הארגון לרציפות התפקודית. שיקולים שונים כאלה עשויים לכלול את היקף המשתמשים בשירותי הארגון, או החזקה של הארגון ברישיונות ספציפיים המעידים על חשיבותו ומרכזיותו בפעילות המגזר. במקביל, וכמפורט לעיל, מוצע לקבוע בחוק המוצע מנגנון סדור שיאפשר בחינה פרטנית של קביעת ארגון כארגון חיוני גם במקרים שבהם לא מתקיימים התנאים האמורים, כדי לאפשר את המענה הלאומי הנדרש.

(4) נציג משרד הביטחון שיקבע שר הביטחון;

(5) נציג שירות הביטחון הכללי שיקבע ראש שירות הביטחון הכללי;

(6) נציג היועץ המשפטי לממשלה.

(ב) המניין החוקי בישיבות הוועדה המייעצת הוא רוב חבריה, ובהם יושב ראש הוועדה ונציג המערך.

(ג) החלטות הוועדה יתקבלו ברוב דעות החברים המשתתפים בישיבה; היו הדעות שקולות, תכריע דעתו של יושב ראש הוועדה.

(ג) קבע גורם מאסדר כאמור בסעיף קטן (ב), ימסור הודעה על כך לארגון ולמערך בתוך 14 ימים מיום הקביעה, בצירוף נימוקי ההחלטה; קביעת הגורם המאסדר תיכנס לתוקף במועד מסירת ההודעה כאמור לארגון.

(ד) על אף הוראות סעיף קטן (ג), ארגון שנקבע שיראו אותו לעניין חוק זה כארגון חיוני, לפי הוראות סעיף קטן (ב)(1), יחולו לגביו ההוראות לפי סעיף 9(ב) עד (ה) החל מתום 12 חודשים ממועד מסירת ההודעה על הקביעה לארגון.

דברי הסבר

נוסף על כך, כדי לשמר את הגמישות הנדרשת שתאפשר לעדכן את רשימת המגזרים בתוספת השלישית, כמו גם את התנאים המגזריים, ולהתאימם לשינויי הזמן והצרכים, מוצע לקבוע בסעיף קטן (ו) לסעיף המוצע, שהגורם המאסדר, בהתייעצות עם ראש מערך הסייבר הלאומי ועם שר האוצר, ובאישור ועדת החוץ והביטחון של הכנסת, יהיה רשאי, בצו, לשנות את התוספת השלישית.

שינוי התוספת ייעשה, על פי המוצע, על בסיס כללים ואמות מידה מקצועיים המיושמים במדינות מפותחות בעלות שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת.

לסעיף קטן (ב)

מוצע לקבוע מנגנון המאפשר שינויים והתאמה למצבים חריגים.

על פי המוצע בפסקה (1), גורם מאסדר יוכל לקבוע, ביחס לארגון הפועל במגזר שהוא אמון על אסדרתו, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, כי הארגון הוא ארגון חיוני גם אם לא מתקיימים לגביו התנאים המגזריים, ובתנאי שאינו גוף מונחה או ארגון חיוני במגזר אחר. כל זאת אם מצא כי מתקיימות נסיבות חריגות המצדיקות קביעה כאמור, בהתחשב במאפיינים המנויים בפסקאות משנה (א) ו־(ב).

עוד מוצע לקבוע, בפסקה (2), שגורם מאסדר יהיה רשאי לקבוע ביחס לארגון הפועל במגזר שהוא אמון על אסדרתו, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, כי אף על פי שמתקיימים לגבי הארגון התנאים המגזריים, הארגון לא ייחשב לארגון חיוני לעניין ההסדר המוצע, וזאת אם מצא כי מתקיימות נסיבות חריגות המצדיקות קביעה כאמור בהתחשב באותם היבטים המנויים בפסקאות משנה (א) ו־(ב) הנזכרות לעיל. קביעה זו יכולה להתבצע גם על פי פנייה של הארגון החיוני לגורם המאסדר בבקשה להחריגו.

על פי המוצע בפסקה (3), גורם מאסדר יידרש, טרם קבלת החלטה בנושא, לשמוע את עמדתה של ועדה מייעצת שתוקם לצורך כך (להלן – הוועדה המייעצת). בראש הוועדה המייעצת יעמוד עובד בכיר ברשות המוסמכת שהסמיך הגורם המאסדר, ויהיו חברים בה נציג מערך הסייבר הלאומי, נציג משרד האוצר, נציג משרד הביטחון, נציג שירות הביטחון הכללי ונציג היועצת המשפטית לממשלה. חברי הוועדה יוכלו לבחון את הנושא מנקודת מבטם וגם בראיית רוחב. הוועדה המייעצת תעביר את עמדתה לגורם מאסדר שפנה אליה בתוך 30 ימים. עוד מוצע לקבוע כי המניין החוקי בישיבות הוועדה המייעצת הוא רוב חבריה, ובהם יושב ראש הוועדה ונציג המערך, וכי החלטות הוועדה יתקבלו ברוב דעות החברים המשתתפים בישיבה, אך אם היו הדעות שקולות, תכריע דעתו של יושב ראש הוועדה.

לסעיף קטן (ג)

מוצע לקבוע כי אם גורם מאסדר קבע, לפי הוראות סעיף קטן (ב) המוצע, שארגון ייחשב לארגון חיוני או שארגון חיוני לא ייחשב לכזה, באופן המפורט לעיל, הוא יידרש להודיע על כך לארגון וכן ליידע את מערך הסייבר הלאומי בתוך 14 ימים מיום שקבע כאמור, ויצרף להודעתו את נימוקי ההחלטה. על פי המוצע, קביעת הגורם המאסדר תיכנס לתוקף במועד מסירת ההודעה לארגון.

לסעיף קטן (ד)

מוצע לקבוע שאם נקבע ארגון כארגון חיוני בהתאם לסעיף (ב) המוצע, בקביעה פרטנית, תינתן לו שהות לנקוט את הצעדים הנדרשים כדי לעמוד במלוא הדרישות לעניין רמת הגנת סייבר לפי החוק המוצע, כך שהחובה לעמוד ברמת ההגנה הבסיסית בהתאם לסעיף 9(ב) עד (ה) לחוק המוצע, תחול לגביו רק בחלוף 12 חודשים מהמועד שבו נכנסה לתוקף קביעתו כארגון חיוני. זאת, מתוך הבנה כי נדרש פרק זמן להיערכות כדי לעמוד ברמת ההגנה הנדרשת כאמור.

(ה) ארגון חיוני כאמור בסעיף קטן (א)(2) שמתקיימים לגביו התנאים האמורים באותו סעיף קטן לעניין יותר ממגזר אחד כאמור בו, רשאי לפנות לגורמים המאסדרים, האמונים על האסדרה של תחום הגנת הסייבר באותם מגזרים, בבקשה שיקבעו את המגזר האחד שלגביו ייחשב הארגון לארגון חיוני לעניין חוק זה; פנה כאמור, יקבעו הגורמים המאסדרים האמורים, יחד, לאחר התייעצות עם המערך, את המגזר האמור; קבעו כאמור, ייחשב הארגון לארגון חיוני לעניין המגזר שנקבע, בלבד, החל ממועד מסירת ההודעה על הקביעה לארגון.

(ו) גורם מאסדר, בהתייעצות עם ראש מערך הסייבר הלאומי ועם שר האוצר, ובאישור ועדת החוץ והביטחון של הכנסת, רשאי, בצו, לתקן את התוספת השלישית, ובכלל זה לשנות את התנאים המנויים בטור ג' לאותה תוספת, לעניין המגזר או תת־מגזר שבו הוא אמון על האסדרה של תחום הגנת הסייבר, ובלבד ששינוי התנאים כאמור ייעשה על בסיס כללים ואמות מידה מקצועיים המיושמים במדינות מפותחות עם שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת.

סימן ב': רמת הגנת סייבר, מניעת סיכון סייבר משמעותי בארגון חיוני וחובת דיווח על תקיפת סייבר משמעותית נגד ארגון חיוני

רמת הגנת סייבר

9. (א) (1) ארגון ינקוט אמצעים סבירים להגנת סייבר בפעילותו, באופן התואם את אופי פעילותו ואת רמת הסיכון הנובעת ממנה.

(2) לעניין פסקה (1), יובאו בחשבון, בין השאר –

(א) סוג השימוש במחשב או סוג חומר המחשב השמור בו והיקף השימוש בהם;

דברי הסבר

לסעיף קטן (ה)

מוצע לקבוע כי ארגון שמתקיימים לגביו התנאים המגזריים, קרי התנאים האמורים בסעיף קטן (א)(2) המוצע, ביותר ממגזר אחד, רשאי לפנות לגורמים המאסדרים של אותם מגזרים, כדי שהם יקבעו, בהתייעצות עם מערך הסייבר הלאומי, את המגזר האחד שבו יוגדר הארגון כארגון חיוני לעניין החוק המוצע, זאת כדי לייצר ודאות בעבור ארגונים במשק באשר לזהות המאסדר שסמכויותיו חלות ביחס אליהם. על פי המוצע, אם התקבלה החלטה כאמור, ייחשב הארגון לארגון חיוני לעניין המגזר שנקבע בלבד, החל ממועד מסירת ההודעה על הקביעה לארגון.

סימן ב': רמת הגנת סייבר, מניעת סיכון סייבר משמעותי בארגון חיוני וחובת דיווח על תקיפת סייבר משמעותית נגד ארגון חיוני

סעיף 9 ותוספת רביעית לסעיף קטן (א)

מאחר שמרחב הסייבר מאופיין בקישוריות גבוהה ולנוכח הסיכונים לתקיפות סייבר, מוצע להבהיר, למען הסר ספק, את המצב המשפטי הקיים, שבו כל ארגון נדרש לנקוט אמצעים סבירים להגנת סייבר בפעילותו, באופן התואם את אופי פעילותו ואת רמת הסיכון הנובעת ממנה. זאת על אף שהחוק המוצע אינו קובע כלי אכיפה או סנקציה ייעודית בהקשר זה.

מאחר שהחוק המוצע מתייחס כאמור לנקיטת אמצעים סבירים באופן התואם את אופי פעילות הארגון ורמת הסיכון הנובעת ממנה, ולא קובע חובות מפורטות החלות על כלל הארגונים, מוצע, לשם הבהירות, לפרט בפסקה (2) שורה של שיקולים או היבטים שיובאו בחשבון על ידי הארגון בקיום החובה האמורה. בין השאר, יובאו בחשבון סוג השימוש במחשב או סוג חומר המחשב השמור בו והיקף השימוש בהם. נוסף על כך, יובאו בחשבון סיכוני הסייבר והנזק שעלול להיגרם לארגון, לציבור או לצדדים שלישיים, ובכלל זה לקוחות, במקרה של תקיפת סייבר נגד הארגון או באמצעותו (למשל כשתקיפה נגד הארגון משמשת גם לתקיפה נגד ארגון אחר), ככל שביכולתו של הארגון לצפות אותם. יתר על כן, תובא בחשבון העלות הכלכלית המוערכת של נקיטת האמצעים הסבירים להגנת הסייבר לפי פסקה (1), ביחס למשאבים ולמאפייני הפעילות של הארגון. כך למשל, במקרה שבו קיים אמצעי שעשוי, אומנם, לשפר במידת מה את רמת הגנת הסייבר של הארגון, אך נקיטתו תהיה כרוכה בעלות בלתי סבירה ביחס למשאבים של הארגון וביחס לסיכון הנשקף למאפייני הפעילות של הארגון, יובא הדבר בחשבון בין מכלול השיקולים הנוגעים לעניין. נוסף על כך, יובאו בחשבון אמצעי הגנת הסייבר המקובלים בארגונים דומים והידע המקצועי הנגיש לארגונים כאמור. כמו כן, יובאו בחשבון גודלו של הארגון, אופיו והיקף פעילותו, ואף יינתן משקל מיוחד להיותו של הארגון "עסק זעיר", כהגדרתו בסעיף מוצע זה. זאת, בשים לב לכך שבמכלול השיקולים, בנסיבות מסוימות, עסק זעיר לא יידרש לנקוט אמצעים מסוימים שארגון גדול יותר יידרש לנקוט, בשל משאביו המוגבלים.

(ב) סיכוני הסייבר והנזק שעלול להיגרם לארגון, לציבור, או לצדדים שלישיים, ובכלל זה לקוחות, במקרה של תקיפת סייבר נגד הארגון או באמצעותו, ככל שביכולתו של הארגון לצפות אותם;

(ג) העלות הכלכלית המוערכת של נקיטת אמצעים כאמור בפסקה (1), ביחס למשאבים ולמאפייני הפעילות של הארגון.

(ד) אמצעי הגנת הסייבר המקובלים בארגונים דומים והידע המקצועי הנגיש לארגונים כאמור;

(ה) גודל הארגון, אופיו והיקף פעילותו; לעניין זה, יינתן משקל מיוחד להיותו של הארגון עסק זעיר; לעניין זה, "עסק זעיר" – ארגון שמחזור העסקאות שלו בשנה אינו עולה על 2 מיליון שקלים חדשים.

(ב) (1) בלי לגרוע מהוראות סעיף קטן (א), ארגון חיוני ידאג לקיים רמת הגנת סייבר בסיסית על ידי קיום הדרישות המפורטות בחלק א' לתוספת הרביעית, באמצעות יישום ההוראות הנוגעות לאותן דרישות בתקן אחד שיבחר מתוך התקנים המנויים בחלק ב' לתוספת האמורה, בהתאמות המתחייבות.

(2) מערך הסייבר הלאומי יפרסם באתר האינטרנט שלו הודעה על כל שינוי בהוראת תקן מהתקנים האמורים, הנוגעת לדרישות האמורות בפסקה (1).

(3) ראש הממשלה, לאחר שהובאה לפניו המלצת ראש מערך הסייבר הלאומי, ובאישור ועדת החוץ והביטחון של הכנסת, רשאי, בצו, לשנות את התוספת הרביעית; המלצת ראש מערך הסייבר הלאומי לעניין פסקה זו תגובש בהתייעצות עם ראש הרשות להגנת הפרטיות; לא מסר ראש הרשות להגנת הפרטיות את עמדתו בתוך 45 ימים מיום שפנה אליו ראש מערך הסייבר הלאומי בעניין, יראו בתום אותה תקופה כאילו קוימה חובת ההתייעצות לפי פסקה זו.

דברי הסבר

לסעיף קטן (ב)

לאור חשיבותם של ארגונים חיוניים להמשך שמירה על הרציפות התפקודית, לצד החובה הכללית החלה על ארגונים להבטיח רמת הגנת סייבר ראויה בפעילותם, ובלי לגרוע ממנה, מוצע לעגן, בחלק א' לתוספת הרביעית כנוסחה המוצע (להלן – תוספת רביעית), חובות פרטניות לעניין רמת הגנת סייבר בסיסית שארגונים חיוניים נדרשים לעמוד בהן. על פי המוצע, על ארגון חיוני לעמוד בדרישות אלה, באמצעות יישום ההוראות הנוגעות לאותן דרישות בתקן אחד שייבחר מתוך התקנים המנויים בחלק ב' לאותה תוספת, בהתאמות המתחייבות ותוך הבטחת הלימה לדרישות המפורטות בחלק א' לתוספת האמורה. יישום הדרישות האמורות בהתאם להוראות התקנים המקצועיים המקובלים, המנויים בחלק ב' לאותה תוספת, בהתאמות כאמור, נועד להקל על הארגונים החיוניים ליישם את אותן דרישות באמצעות מתן הכוונה לעניין אופן יישומן.

יובהר כי לא מוצע לקבוע חובה לעמידה מלאה בכל הוראות התקן שנבחר על ידי הארגון החיוני, אם הוראות התקן מתייחסות לדרישות רחבות יותר מדרישות המנויות בחלק א' לתוספת הרביעית. במקרה כזה, יידרש הארגון החיוני לעמוד רק בהוראות הרלוונטיות לאותן דרישות. יצוין כי התקנים המנויים בחלק ב' לתוספת הרביעית הם תקנים הזמינים לעיון הציבור במרשתת.

כדי להנגיש לארגונים החיוניים שינויים בהוראות התקינה שלפיהן עליהם ליישם את הדרישות שבחלק א' לתוספת הרביעית, מוצע לקבוע כי המערך יפרסם באתר האינטרנט שלו כל שינוי בהוראת תקן מהתקנים המנויים בחלק ב' לתוספת האמורה, הנוגעת לדרישות האמורות. נוסף על כך, כדי לסייע לארגונים החיוניים, בכוונת המערך לערוך ולפרסם באתר האינטרנט של המערך טבלה אשר תפנה לסעיפי הבקרות בכל תקן המנוי בחלק ב' לתוספת הרביעית, ביחס לדרישות המפורטות בחלק א' לאותה תוספת, לרבות בעת עדכון התקן כאמור לעיל.

ההוראות המנויות בתוספת הרביעית נועדו להבטיח רמת הגנה בסיסית לארגון חיוני באמצעות יישום דרישות שעניינן, בין השאר, מדיניות לניתוח סיכונים והגנה על נכסי סייבר; דרישות שעניינן היערכות לאירועי סייבר (Cyber Events), ובכלל זה תקיפות סייבר והתמודדות עימן; רציפות תפקודית והמשכיות השירות; הגנת סייבר בשרשרת האספקה; פיתוח מאובטח, תחזוקה של מערכות וטיפול בחשיפות (Exposure) ובפגיעויות (Vulnerabilities); מדיניות ונהלים להערכת התועלת של הפעילות הארגונית להגנת סייבר; היגיינת מחשב בסיסית והדרכות; הצפנה והסתרה של נכסי סייבר; בקרת גישה, ניהול נכסי סייבר והתייחסות לגורם האנושי.

(ג) גורם מאסדר של תחום הגנת הסייבר במגזר כאמור בפסקה (1) להגדרה "מגזר" שבסעיף 1, רשאי, לאחר התייעצות עם ראש מערך הסייבר הלאומי, לקבוע בתקנות דרישות בעניין רמת הגנת הסייבר שיחולו על ארגונים חיוניים באותו מגזר, נוסף על הדרישות המנויות בחלק א' לתוספת הרביעית, וכן רשאי הוא, לאחר התייעצות כאמור, לקבוע דרישות נוספות כאמור בהוראות שהוא מוסמך לתת לפי דין אחר.

(ד) ראש הרשות המוסמכת כאמור בפסקה (2) להגדרה "רשות מוסמכת" שבסעיף 1, רשאי, לאחר התייעצות עם ראש מערך הסייבר הלאומי, לתת, בהנחיות או בנהלים, הוראות לעניין רמת הגנת הסייבר של גופים ממשלתיים, נוסף על הדרישות המנויות בחלק א' לתוספת הרביעית.

(ה) ארגון חיוני ישמור מידע ומסמכים המעידים על עמידתו בדרישות לפי סעיפים קטנים (ב) עד (ד).

(ו) תקנות, הוראות, הנחיות ונהלים לפי סעיפים קטנים (ב) עד (ד) ייקבעו על בסיס כללים ואמות מידה מקצועיים, המיושמים במדינות מפותחות עם שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת, בין השאר בשל תנאי שוק ייחודיים לרבות מגבלות על מתן השירות בידי ארגונים במגזר, מיעוט חלופות למתן השירות במגזר, צרכים תפעוליים ייחודיים של ארגונים במגזר והערכת איומים וסיכונים בתחום הסייבר במגזר.

דברי הסבר

יתרה מכך, כדי לאפשר עדכון של ההוראות המנויות בתוספת הרביעית המוצעת מזמן לזמן ולהמשיך להבטיח הגנת סייבר בסיסית, מוצע להסמיך את ראש הממשלה, לאחר שהובאה לפניו המלצת ראש מערך הסייבר הלאומי שגובשה בהתייעצות עם ראש הרשות להגנת הפרטיות כמפורט בפסקה (3) המוצעת, ובאישור ועדת החוץ והביטחון של הכנסת, לשנות בצו את התוספת הרביעית.

לסעיף קטן (ג)

כדי להשלים ולשפר את רמת הגנת הסייבר של ארגונים חיוניים ולאפשר התאמה מרבית של הסטנדרט המקצועי הנדרש למאפיינים הייחודיים של כל מגזר, מוצע, נוסף על הדרישות המנויות בחלק א' לתוספת הרביעית, להסמיך גורמים מאסדרים, לאחר התייעצות עם ראש מערך הסייבר הלאומי, כגורם המקצועי הלאומי המתכלל את תחום הגנת הסייבר, לקבוע בתקנות, או לתת בהוראות שהם מוסמכים לתת לפי דין (מכוח חקיקה אחרת), דרישות נוספות בעניין רמת הגנת הסייבר שיחולו על ארגונים חיוניים במגזר שהם הגורם המאסדר שלו. יובהר כי הסעיף המוצע אינו מקנה סמכות לגורם מאסדר לקבוע דרישות כאמור בהוראות שאינן תקנות, כגון הוראות מינהל, אלא מבהיר שגורם מאסדר שמוסמך לתת הוראות כאמור, מכוח דין אחר, רשאי לקבוע במסגרתן דרישות כאמור, אך זאת בהתייעצות עם ראש מערך הסייבר.

לסעיף קטן (ד)

באופן דומה לאמור בסעיף קטן (ג) המוצע, מוצע להסמיך את ראש הרשות המוסמכת כאמור בפסקה (2) להגדרה "רשות מוסמכת" המוצעת, כלומר, ראש מערך הדיגיטל, לקבוע, לאחר התייעצות עם ראש מערך הסייבר הלאומי, כגורם המקצועי הלאומי המתכלל את תחום הגנת הסייבר, הוראות נוספות על הדרישות שבחלק א' לתוספת הרביעית, שיחולו לעניין רמת הגנת הסייבר של גופים ממשלתיים. הוראות כאמור ייקבעו בהנחיות או בנהלים.

לסעיף קטן (ה)

כדי לאפשר בקרה על עמידתם של ארגונים חיוניים בדרישות רמת הגנת סייבר כמוצע בסעיף זה, מוצע לחייב ארגון חיוני לשמור מידע ומסמכים המעידים על עמידתו בדרישות לפי סעיפים קטנים (ב) עד (ד) המוצעים, כלומר ברמת ההגנה התואמת את הדרישות לפי התוספת הרביעית, ואם נקבעו תקנות, הוראות, הנחיות או נהלים לפי סעיפים קטנים (ג) או (ד) – לפי אותן הוראות.

לסעיף קטן (ו)

מוצע להתוות את שיקול הדעת של הגורמים המוסמכים לקבוע תקנות, ובכלל זה צווים וכן הוראות, הנחיות ונהלים, לפי סעיפים קטנים (ב) עד (ד) המוצעים כאמור, כך שאלה ייקבעו בהתאם לעקרונות האסדרה הנהוגים ועל בסיס כללים ואמות מידה מקצועיים, המיושמים במדינות מפותחות בעלות שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת, בין השאר בשל תנאי שוק ייחודיים לרבות מגבלות על מתן השירות בידי ארגונים במגזר, מיעוט חלופות למתן השירות במגזר, צרכים תפעוליים ייחודיים של ארגונים במגזר והערכת איומים וסיכונים בתחום הסייבר במגזר.

חוות דעת מקדמית

10. (א) רשות מוסמכת תיתן, לבקשת ארגון חיוני, חוות דעת מקדמית בעניין אופן קיום דרישה המנויה בחלק א' לתוספת הרביעית באמצעות יישום הוראות תקן כמפורט בחלק ב' לאותה תוספת, בהתאמות המתחייבות כאמור בסעיף 9(ב)(1), בידי הארגון (בסעיף זה – חוות דעת מקדמית).

(ב) בקשת ארגון חיוני לקבלת חוות דעת מקדמית תכלול את מטרת הבקשה ואת כל העובדות הנדרשות למתן חוות הדעת, בצירוף המסמכים הנוגעים בדבר; רשות מוסמכת רשאית לדרוש ידיעות ומסמכים נוספים הדרושים לה לצורך מתן חוות הדעת המקדמית.

(ג) חוות דעת מקדמית תינתן בתוך 60 ימים ממועד קבלת בקשת הארגון החיוני, ואם דרשה הרשות המוסמכת ידיעות ומסמכים נוספים לפי סעיף קטן (ב) – ממועד המצאתם, לפי המאוחר; מנהל בכיר ברשות מוסמכת רשאי להאריך את התקופה האמורה, אם מצא כי מתקיימות נסיבות מיוחדות המצדיקות זאת.

(ד) הרשות המוסמכת תעביר את חוות הדעת המקדמית למערך הסייבר הלאומי, ורשאית היא, בהסכמת הארגון, לפרסם חוות דעת מקדמית הכוללת פרטים שיש בהם כדי לזהות את הארגון החיוני, ואם לא ניתנה לכך הסכמת הארגון החיוני – לפרסם את חוות הדעת המקדמית בלא פרטים שיש בהם כדי לזהות את הארגון החיוני.

הוראות דחופות למניעת סיכון סייבר משמעותי בארגון חיוני

11. (א) מצא ראש מערך הסייבר הלאומי כי מתקיים סיכון סייבר שיש בו כדי לאפשר תקיפת סייבר חמורה כהגדרתה בסעיף 13, נגד ארגונים חיוניים שונים או באמצעותם, אם לא יינקטו בדחיפות אמצעים להתמודדות עימו, רשאי הוא, באישור ראש הממשלה, להורות בכתב לארגון חיוני שביחס אליו עלול להתממש הסיכון, לנקוט אמצעים כאמור במועד שעליו יורה.

דברי הסבר

סעיף 10 במטרה לייצר ודאות בעבור הארגונים החיוניים באשר לעמידתם בדרישות הגנת הסייבר הבסיסיות המחייבות לפי חלק א' לתוספת הרביעית, באמצעות יישום הוראות תקן כמפורט בחלק ב' לאותה תוספת בהתאמות המתחייבות, מוצע לקבוע הסדר שמאפשר לאותם ארגונים לבקש לקבל מהרשות המוסמכת הנוגעת לעניין, חוות דעת מקדמית לעניין זה. כדי לאפשר לרשות המוסמכת לגבש את חוות הדעת המקדמית על בסיס כלל המידע הנדרש לצורך כך, מוצע לקבוע כי בקשת ארגון חיוני לקבלת חוות דעת מקדמית תכלול את מטרת הבקשה ואת כל העובדות הנדרשות למתן חוות הדעת, בצירוף המסמכים הנוגעים בדבר. נוסף על כך, מוצע לאפשר לרשות מוסמכת שקיבלה בקשה כאמור לדרוש ידיעות ומסמכים נוספים הדרושים לה לצורך מתן חוות הדעת המקדמית.

עוד מוצע לקבוע שחוות הדעת המקדמית תינתן בתוך 60 ימים ממועד קבלת בקשת הארגון החיוני, ואם דרשה הרשות המוסמכת ידיעות ומסמכים נוספים כאמור לפי סעיף קטן (ב) המוצע – בתוך 60 ימים מהמועד שבו הומצאו לה, לפי המאוחר.

כמו כן, מוצע להסמיך מנהל בכיר ברשות מוסמכת להאריך את התקופה למתן חוות דעת מקדמית, אם מצא כי מתקיימות נסיבות מיוחדות המצדיקות זאת. על פי המוצע, הרשות המוסמכת תעביר את חוות הדעת המקדמית למערך הסייבר הלאומי, ורשאית היא, בהסכמת הארגון, לפרסם חוות דעת מקדמית הכוללת פרטים שיש בהם כדי לזהות את הארגון החיוני. אם לא ניתנה לכך הסכמת הארגון החיוני, תוכל הרשות המוסמכת לפרסם את חוות הדעת המקדמית בלא פרטים שמאפשרים לזהותו. הכול, כדי לסייע לארגונים חיוניים אחרים באותו מגזר לבחון את עמידתם בדרישות.

סעיף 11 לסעיף קטן (א)

מתוך הראייה הלאומית המתכללת של מערך הסייבר הלאומי בתחום הגנת הסייבר, לנוכח רמת האיומים הגבוהה במרחב הסייבר הישראלי, מוצע להקנות לראש מערך הסייבר הלאומי, באישור ראש הממשלה, סמכות להורות בכתב לארגון חיוני לנקוט אמצעים להתמודדות עם סיכון סייבר או למניעתו, ולקבוע מועד לנקיטתם. ראש המערך יוכל להפעיל סמכות זאת אם מצא כי מתקיים סיכון סייבר שיש בו כדי לאפשר תקיפת סייבר חמורה כהגדרתה בסעיף 13 לחוק המוצע, נגד ארגונים חיוניים שונים או באמצעותם, אם לא יינקטו בדחיפות אמצעים להתמודדות עימו, היינו סיכון סייבר משמעותי. במסגרת הפעלת הסמכות, יהיה ראש מערך הסייבר הלאומי רשאי לתת הוראות כאמור לארגון חיוני שביחס אליו עלול להתממש הסיכון. סעיף זה נועד לאפשר לראש מערך הסייבר הלאומי, במקרים חריגים, לתת הוראות לארגונים חיוניים כדי שהם יתמודדו באופן דחוף עם סיכוני סייבר משמעותיים במסגרת פעילותם להגנת הסייבר בארגון, כגון הוראות לטיפול בפגיעויות חמורות העלולות לגרום לסיכון משמעותי במשק.

(ב) ראש מערך הסייבר הלאומי ייתן הוראה כאמור בסעיף קטן (א), לאחר שקיים ככל האפשר בנסיבות העניין התייעצות עם הרשות המוסמכת הנוגעת לעניין, ולאחר ששקל את השפעתה האפשרית על פעילות הארגון החיוני ועל צד שלישי, ובכלל זה על הזכות לפרטיות, וכן את העלות הכלכלית המוערכת של יישום ההוראה והשפעתה האפשרית על הרציפות התפקודית של הארגון החיוני, למיטב ידיעתו, ואם הארגון החיוני מסר הערכה לעניין זה – בהתחשב בהערכה שמסר, ומצא כי אין במתן ההוראה כדי לפגוע במידה העולה על הנדרש בנסיבות העניין.

(ג) הוראה כאמור בסעיף קטן (א) תועבר לארגון החיוני באמצעות היחידה המגזרית, אלא אם כן התקיימו נסיבות מיוחדות המצדיקות אחרת.

(ד) (1) ארגון חיוני שקיבל הוראה לפי סעיף זה, רשאי, בהקדם האפשרי ולא יאוחר מתום 48 שעות ממועד קבלת ההוראה, להשיג עליה לפני מנהל בכיר במערך, אם מתקיים אחד מאלה:

(א) לטענת הארגון החיוני סיכון הסייבר שבעניינו ניתנה ההוראה אינו קיים לגביו, או שקיים סיכון כאמור אך אין בו כדי לאפשר תקיפת סייבר חמורה נגד הארגון החיוני או באמצעותו;

(ב) הארגון החיוני פירט אמצעים חלופיים להתמודדות עם סיכון הסייבר שבעניינו ניתנה ההוראה.

(2) השגה לפי פסקה (1) (בסעיף זה – השגה) תוגש בכתב בפירוט כל הנתונים ובצירוף כל המסמכים הנדרשים להחלטה בה.

דברי הסבר

לסעיף קטן (ב)

כדי להבטיח שימוש מידתי ומאוזן בסמכות הקבועה בסעיף קטן (א) המוצע, מוצע לקבוע תנאים ברורים להפעלתה. כך, למשל, מוצע לקבוע כי החלטה על מתן הוראות דחופות למניעת סיכון כאמור דורשת את אישור ראש הממשלה. יתרה מכך, מוצע לקבוע כי ההוראות האמורות יינתנו רק לאחר שראש מערך הסייבר הלאומי קיים, ככל האפשר בנסיבות העניין, התייעצות עם הרשות המוסמכת הנוגעת לעניין. נוסף על כך, מוצע לקבוע כי ראש מערך הסייבר הלאומי ייתן הוראה כאמור רק לאחר שמצא כי אין בה כדי לפגוע במידה העולה על הנדרש בנסיבות העניין, וזאת לאחר ששקל את השפעתה האפשרית על פעילות הארגון החיוני ועל צד שלישי, לרבות הזכות לפרטיות, את העלות הכלכלית המוערכת של יישום ההוראה ואת השפעתה האפשרית על הרציפות התפקודית של הארגון החיוני, למיטב ידיעתו, ואם הארגון החיוני מסר לראש מערך הסייבר הלאומי הערכה כלכלית לעניין זה – בהתחשב בהערכה שמסר.

לסעיף קטן (ג)

מוצע לקבוע כי הוראה לנקוט אמצעים להתמודדות עם סיכון סייבר, כאמור לעיל, תועבר לארגון החיוני באמצעות היחידה המגזרית, אלא אם כן התקיימו נסיבות מיוחדות המצדיקות שהדבר ייעשה בדרך אחרת.

לסעיף קטן (ד)

מוצע לאפשר לארגון חיוני שקיבל הוראה לפי סעיף מוצע זה, להשיג עליה לפני מנהל בכיר במערך, בלוח זמנים ומטעמים כמפורט בסעיף קטן (ד) כנוסחו המוצע. הטעמים המוצעים נוגעים לעצם קיומו של הסיכון או לאופיו, או לקיומם של אמצעים חלופים להתמודדות עם הסיכון.

על פי המוצע, ההשגה תוגש בכתב תוך פירוט כל הנתונים וצירוף כל המסמכים הנדרשים להחלטה בה; החלטה בהשגה תינתן בהקדם האפשרי ולא יאוחר מ־48 שעות ממועד הגשתה, אך מוצע לאפשר למנהל בכיר במערך לדחות את המועד לנתינתה מטעמים מיוחדים; ולבסוף, מוצע כי ההחלטה בהשגה תינתן לאחר התייעצות עם מנהל בכיר ברשות המוסמכת הנוגעת לעניין, ותימסר בכתב ובצירוף נימוקים, הן לארגון החיוני והן לרשות המוסמכת.

עוד מוצע לקבוע כי אם החליט מנהל בכיר במערך לקבל את ההשגה מהטעם שקיימים אמצעים חלופיים להתמודדות עם הסיכון, שהארגון החיוני פירט בהשגה שהגיש, יראו כאילו ניתנה לארגון החיוני הוראה לנקוט את אותם אמצעים חלופיים. כמו כן, מוצע להבהיר כי עצם הגשת ההשגה אינו מעכב את ביצוע ההוראה שלגביה היא הוגשה, אלא אם כן החליט המנהל הבכיר במערך אחרת.

(3) החלטה בהשגה תינתן בהקדם האפשרי ולא יאוחר מ־48 שעות ממועד הגשתה, אלא אם כן דחה מנהל בכיר במערך את המועד לנתינתה, מטעמים מיוחדים; ההחלטה בהשגה תינתן לאחר התייעצות עם מנהל בכיר ברשות המוסמכת, תהיה מנומקת ותימסר בכתב לארגון החיוני ולרשות המוסמכת; התקבלה השגה לפי פסקה (1)(ב), כולה או חלקה, יראו כאילו ניתנה לארגון החיוני הוראה לפי סעיף קטן (א) לנקוט את האמצעים החלופיים שפירט כאמור באותה פסקה, בהתאם להחלטה בהשגה.

(4) אין בהגשת השגה כדי לעכב את ביצוע ההוראה שלגביה הוגשה, אלא אם כן החליט המנהל הבכיר במערך אחרת.

(ה) ארגון חיוני ישמור מידע ומסמכים המעידים על עמידתו בהוראות לפי סעיף זה.

חובת דיווח על תקיפת סייבר משמעותית נגד ארגון חיוני

12. (א) נודע לארגון חיוני שמתרחשת, בפועל, תקיפת סייבר נגדו שמתקיים לגביה אחד מאלה (בסעיף זה – תקיפת סייבר משמעותית), ידווח על כך למנהל בכיר במערך ולמנהל בכיר ברשות המוסמכת, בהתאם להוראות סעיפים קטנים (ב) ו־(ג):

(1) היא פוגעת או שיש חשש ממשי שתפגע באופן משמעותי בזמינות, ברציפות או במהימנות השירות של הארגון החיוני, בהתחשב בין השאר באלה:

(א) מספר או סוג המשתמשים בשירות שעלולים להיות מושפעים מהתקיפה;

(ב) סוג הפגיעה והיקפה;

(ג) משך הפגיעה;

(2) התקיפה עלולה להביא לפגיעה בנכס מידע משמעותי או לגישה של גורם שאינו מורשה לנכס כאמור, ובכלל זה בדרך של פגיעה בתהליך הזדהות או שינויו, או הוצאתו שלא כדין של מידע לרבות בדרך של העתקתו על ידי גורם כאמור;

דברי הסבר

להשלמת הדברים, יצוין כי בסעיף 21 לחוק המוצע, מוצע להחיל את ההסדר המעוגן בסעיף זה גם ביחס לארגון חיוני למערכת הביטחון כהגדרתו המוצעת, ובכלל זה להקנות את הסמכות הנתונה בו לראש המערך (והסמכות הנתונה למנהל בכיר במערך בכל הנוגע להשגה), גם לראש מלמ"ב ולמנהל בכיר במלמ"ב, הכול כמפורט בסעיף 21 לחוק המוצע.

לסעיף קטן (ה)

מוצע להטיל על ארגון חיוני חובה לשמור מידע ומסמכים המעידים על עמידתו בהוראות לפי סעיף מוצע זה.

סעיף 12 כל אדם, וכן כל ארגון, רשאי למסור הודעה למערך הסייבר הלאומי בעניין תקיפת סייבר. באשר לתקיפות כאמור נגד ארגונים חיוניים או באמצעותם, הרי קבלת דיווח על תקיפות כאמור שהן תקיפות משמעותיות היא חיונית במסגרת מאמצי ההגנה על המשק.

לסעיף קטן (א)

בשים לב לאמור לעיל, מוצע לקבוע שארגון חיוני יהיה חייב למסור דיווח על תקיפת סייבר משמעותית נגדו הידועה לו והמתרחשת בפועל. הדיווח יימסר למנהל בכיר במערך הסייבר הלאומי ולמנהל בכיר ברשות המוסמכת לעניין פעילות בתחום הגנת הסייבר במגזר שבו פועל הארגון. יובהר שבהתאם להסדר המוצע, הארגון החיוני יגיש דיווח אחד, שיוגש במקביל לרשות המוסמכת ולמערך הסייבר הלאומי.

מוצע להגדיר "תקיפת סייבר משמעותית" שבשלה תקום חובת הדיווח לפי סעיף זה כתקיפה שמתקיים לגביה אחד משלושה תנאים, המנויים בפסקאות (1) עד (3) של סעיף קטן (א), שעניינם מהות וחומרת התקיפה.

יובהר כי בעוד ההחלטה בשאלה אם תקיפה היא "תקיפת סייבר חמורה" כהגדרתה בסעיף 13 לחוק המוצע כרוכה בבחינת שיקולים שאת חלקם לרשות מינהלית יש יכולת לשקול, הרי "תקיפת סייבר משמעותית" מוגדרת כך שארגון חיוני יכול להפעיל את שיקול דעתו ולבחון אם מדובר בתקיפה כאמור שחלה עליו חובה לדווח עליה בהתאם לסעיף מוצע זה. עוד יצוין כי בכוונת מערך הסייבר הלאומי לפרסם גילוי דעת בדבר דוגמאות לתקיפות סייבר משמעותיות שיש לדווח עליהן לפי סעיף מוצע זה, ודוגמאות לעניינים שיש לכלול בדיווח לפי הסעיף האמור, ושאם לא יפורטו, יהיה ניתן להטיל על הארגון החיוני עיצום בשל אי־מסירתם.

(3) יש חשש ממשי שהיא אינה מוגבלת לארגון החיוני הנתקף.

(ב) לשם מילוי חובתו בהתאם לסעיף זה יפעל ארגון חיוני באחת הדרכים שבפסקאות (1) או (2) להלן, בציון הדרך שבה בחר לפעול:

(1) יגיש את הדיווחים בהתאם למפורט להלן:

(א) יגיש, באופן מיידי, דיווח הכולל את הפרטים שלהלן, אם הם ידועים לו, וכל מידע אחר שיש בו כדי לסייע להערכת חומרתה של תקיפת הסייבר והשלכותיה:

(1) פרטי הארגון והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;

(2) מועד תחילת תקיפת הסייבר ומועד גילויה;

(3) מידע לגבי מאפייני תקיפת הסייבר והשפעתה על הארגון;

(4) מידע הנוגע לאפשרות שתקיפת הסייבר תפגע ישירות ובאופן ממשי בארגון אחר;

(ב) יגיש, בסמוך לאחר סיום הטיפול בתקיפת הסייבר, דיווח הכולל את הפרטים שלהלן (להלן – דיווח מסכם):

(1) תיאור מפורט על אודות תקיפת הסייבר, לרבות חומרתה והשלכותיה;

(2) סוג תקיפת הסייבר והגורמים שהיו מקור להתרחשותה, לפי מיטב ידיעתו של הארגון;

דברי הסבר

לסעיף קטן (ב)

מוצע לפרט את הדרכים שבהן ארגון חיוני יכול לקיים את חובת הדיווח לפי סעיף מוצע זה. על פי המוצע, יידרש הארגון לפעול באחת מהדרכים שלהלן, בציון הדרך שנבחרה:

1. בדרך הראשונה על הארגון להגיש, באופן מיידי, דיווח הכולל את הפרטים המוצעים בסעיף, אם הם ידועים לו וכל מידע אחר שיש בו כדי לסייע להערכת חומרתה של תקיפת הסייבר והשלכותיה, ובכלל האמור: פרטי הארגון והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו (כגון שם איש קשר בארגון, מספר טלפון, כתובת למשלוח הודעות, כתובת דואר אלקטרוני ומספר ח"פ (אם קיים)); מועד תחילת תקיפת הסייבר ומועד גילויה; מידע לגבי מאפייני תקיפת הסייבר והשפעתה על הארגון; ומידע הנוגע לאפשרות שתקיפת הסייבר תפגע ישירות ובאופן ממשי בארגון אחר.

נוסף על כך, במסגרת דיווח בדרך זו, על הארגון להגיש, בסמוך לאחר סיום הטיפול בתקיפת הסייבר, דיווח מסכם שנועד, בין השאר, לאפשר למערך הסייבר הלאומי ולרשות המוסמכת, לוודא שהאינטרסים הציבוריים שעלולים להפגע כתוצאה מתקיפת סייבר משמעותית מוגנים, וכן להבטיח שהמערך והרשות המוסמכת מחזיקים בתמונת מצב מלאה ככל האפשר של רמת ההגנה במשק ובמגזר, לפי העניין. בהתאם למוצע, הדיווח המסכם יכלול פרטים אלה: תיאור מפורט על אודות תקיפת הסייבר, לרבות חומרתה והשלכותיה; סוג תקיפת הסייבר והגורמים שהיו מקור להתרחשותה, לפי מיטב ידיעתו של הארגון; אופן הטיפול בתקיפת הסייבר, לרבות פירוט בדבר אמצעים שננקטו או שעדיין ננקטים לשם כך, אך למעט סוד מסחרי הנוגע ישירות לאופן הטיפול בתקיפת הסייבר ולאמצעים כאמור. יובהר בזה כי קיומו של סוד מסחרי כאמור אינו פוטר את הארגון החיוני מהעברת המידע, אלא שהארגון יידרש להעברת המידע באופן שאינו פוגע בסוד המסחרי.

2. בדרך השנייה על הארגון החיוני להגיש בלא דיחוי ולא יאוחר מחלוף 24 שעות מהמועד שבו נודע לו על תקיפת הסייבר, דיווח ראשוני בדבר התקיפה, הכולל מידע שיש בו כדי לסייע בהערכת חומרת התקיפה והשלכותיה, אם הוא ידוע לו, וכן את פרטי הארגון והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו (כמפורט לעיל). לאחר מכן, יידרש הארגון להגיש בלא דיחוי ולא יאוחר מחלוף 72 שעות מהמועד שבו נודע לו על תקיפת הסייבר, דיווח נוסף הכולל עדכון לגבי המידע שנמסר בדיווח הראשוני, הערכה ראשונית בדבר חומרת התקיפה והשלכותיה, ומידע הנוגע למאפייני תקיפת הסייבר ולמזהי התקיפה, והכול אם המידע האמור ידוע לו. כמו כן, הארגון יידרש להגיש, לפי דרישה מאת עובד מוסמך מגזרי או עובד מוסמך במערך, במועד שיקבע העובד המוסמך האמור, דיווח ביניים הכולל עדכון לגבי המידע שנמסר. נוסף על כך, לא יאוחר מחלוף 30 ימים מהמועד שבו הגיש הארגון החיוני את הדיווח הנוסף, הוא יידרש להגיש דיווח מסכם הכולל את הפרטים האמורים בפסקה (1)(ב) של סעיף קטן (ב) המוצע. ואולם אם לא הסתיים הטיפול בתקיפת הסייבר בחלוף 30 ימים

(3) אופן הטיפול בתקיפת הסייבר, לרבות פירוט בדבר אמצעים שננקטו או שעדיין ננקטים לשם כך, למעט סוד מסחרי הנוגע ישירות לאופן הטיפול בתקיפת הסייבר ולאמצעים כאמור;

(2) יגיש את הדיווחים בהתאם למפורט להלן:

(א) יגיש, בלא דיחוי ולא יאוחר מחלוף 24 שעות מהמועד שבו נודע לארגון החיוני על תקיפת הסייבר, דיווח ראשוני עליה הכולל מידע שיש בו כדי לסייע בהערכת חומרת התקיפה והשלכותיה, אם הוא ידוע לו, וכן את פרטי הארגון והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;

(ב) יגיש, בלא דיחוי ולא יאוחר מחלוף 72 שעות מהמועד שבו נודע לארגון החיוני על תקיפת הסייבר, דיווח הכולל עדכון לגבי המידע שנמסר בדיווח הראשוני כאמור בפסקת משנה (א), הערכה ראשונית בדבר חומרת התקיפה והשלכותיה, ומידע הנוגע למאפייני תקיפת הסייבר ולמזהי התקיפה, והכול אם המידע האמור ידוע לו;

(ג) יגיש, לפי דרישה מאת העובד המוסמך המגזרי או העובד המוסמך במערך הסייבר הלאומי, במועד שיקבע העובד המוסמך, דיווח ביניים הכולל עדכון לגבי המידע שנמסר לפי פסקאות משנה (א) או (ב);

(ד) יגיש, לא יאוחר מחלוף 30 ימים מהמועד שבו הגיש את הדיווח לפי פסקת משנה (ב), דיווח מסכם הכולל את הפרטים האמורים בפסקה (1)(ב);

(ה) על אף האמור בפסקת משנה (ד), אם לא הסתיים הטיפול בתקיפת הסייבר במועד הדיווח כאמור באותה פסקת משנה, יגיש הארגון, באותו מועד, דיווח על התקדמות הטיפול בתקיפת הסייבר, הכולל את הפרטים לפי אותה פסקת משנה, אם הם ידועים לו; הסתיים הטיפול בתקיפת הסייבר, יגיש הארגון, לא יאוחר מ־30 ימים לאחר סיום הטיפול בתקיפה, דיווח מסכם כאמור באותה פסקת משנה;

(ג) (1) דיווח לפי סעיף זה יוגש למנהל בכיר במערך ולמנהל בכיר ברשות המוסמכת, בדיווח אחד, באמצעות המערך, באופן מקוון באתר האינטרנט של המערך או בהודעה טלפונית ל־CERT, ואם פרסם ראש מערך הסייבר הלאומי באתר האינטרנט של המערך דרך נוספת להגשת דיווח כאמור – יכול שיוגש גם בדרך שפורסמה כאמור.

דברי הסבר

מהדיווח הנוסף, יגיש הארגון דיווח על התקדמות הטיפול בתקיפת הסייבר, הכולל את כל הפרטים הנדרשים לדיווח מסכם, אם הם ידועים לו. משהסתיים הטיפול בתקיפת הסייבר, יגיש הארגון, לא יאוחר מ־30 ימים לאחר סיום הטיפול בתקיפה, דיווח מסכם הכולל את הפרטים האמורים בפסקה (1)(ב) האמורה.

לסעיף קטן (ג)

כדי להקל על ארגונים חיוניים ולהבטיח שיידרשו להגיש דיווח אחד בלבד, מוצע לקבוע כי הדיווח לפי סעיף מוצע זה יוגש למנהל בכיר במערך ולמנהל בכיר ברשות המוסמכת, בדיווח אחד, באמצעות המערך, באופן מקוון באתר האינטרנט של המערך או בהודעה טלפונית ל־CERT, וכמו כן יכול שיוגש בדרך אחרת שהורה עליה ראש מערך הסייבר הלאומי ופורסמה באתר האינטרנט של המערך. לאחר ההגשה, הדיווח יועבר לרשות המוסמכת באופן אוטומטי או באמצעות שליחה פרטנית על ידי מערך הסייבר הלאומי. לצד זאת, כדי לאפשר התאמה מרבית לאופן ההתנהלות של רשויות מוסמכות עם המגזרים שהן פועלות מולם, מוצע לאפשר לגורם מאסדר או לשר הממונה על מערך הדיגיטל (שהוא הרשות המוסמכת לעניין פעילות משרדי הממשלה) לקבוע שהדיווח האמור יוגש בדיווח אחד באמצעות הרשות המוסמכת, בדרך שיקבע הגורם המאסדר או השר הממונה כאמור, ובלבד שייקבע בתקנות כאמור שהרשות המוסמכת תעביר את הדיווח למנהל בכיר במערך מייד עם קבלתו.

(2) על אף הוראות פסקה (1), גורם מאסדר או השר הממונה על הרשות המוסמכת כאמור בפסקה (2) להגדרה "רשות מוסמכת" שבסעיף 1, רשאי לקבוע כי הדיווח יוגש למנהלים האמורים בפסקה (1), בדיווח אחד, באמצעות הרשות המוסמכת כפי שיקבע, ובלבד שיקבע שהרשות המוסמכת תעביר את הדיווח למנהל בכיר במערך מייד עם קבלתו; גורם מאסדר או השר הממונה כאמור יידע את המערך מבעוד מועד על כוונתו לקבוע כאמור בסעיף קטן זה; קבע גורם מאסדר או השר הממונה כאמור תקנות לפי פסקה זו, יפרסם הודעה על כך באתר האינטרנט של הרשות המוסמכת.

סימן ג': סמכויות לשם התמודדות עם תקיפת סייבר חמורה

סימן ד' – הגדרה

13. בסימן זה, "תקיפת סייבר חמורה" – תקיפת סייבר שיש חשש ממשי כי מתקיים לגביה אחד או יותר מאלה:

(1) היא פוגעת ברציפות התפקודית של ארגון חיוני, ובכלל זה בתהליך חיוני בארגון;

(2) היא פוגעת בזמינות, ברציפות או במהימנות של השירות שארגון חיוני מספק;

(3) היא מאפשרת לגורם שאינו מורשה לכך גישה לנכס מידע משמעותי של ארגון חיוני;

(4) היא מבוצעת נגד ארגון חיוני או באמצעותו והיא בעלת מאפיינים המעידים על חומרה מיוחדת, לרבות מיתאר התקיפה או זהות התוקף, ומתקיים לגביה אחד מאלה:

(א) היא עלולה לפגוע בביטחון המדינה או בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור;

(ב) קיים חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לארגון הנתקף.

דברי הסבר

עוד מוצע לקבוע כי הגורם המאסדר או השר הממונה על מערך הדיגיטל יידע את המערך מבעוד מועד על כוונתו לקבוע דרך דיווח אחרת כאמור, ואם קבע הוראות כאמור לעניין דרך הדיווח, יפרסם על כך הודעה באתר האינטרנט של הרשות המוסמכת.

סימן ג': סמכויות לשם התמודדות עם תקיפת סייבר חמורה

כללי לשם הבטחת התמודדות הולמת עם תקיפות סייבר חמורות כלפי ארגון חיוני או ספק שירותים דיגיטליים ושירותי אחסון, או באמצעות ארגון או ספק כאמור, בהתחשב בנזק הפוטנציאלי החמור שעלול להיגרם כתוצאה מתקיפה כאמור, מוצע, לצד החובות המוטלות על אותם ארגונים, להסדיר את הסמכויות שיוקנו לגופי המדינה השונים כלפי אותם ארגונים, ואת הפעולות שגורמים אלה יוכלו לבצע, לצורך איתור, מניעה או בלימה של תקיפות סייבר חמורות.

יצוין כי סעיפים דומים במהותם נחקקו במסגרת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), התשפ"ד–2023 (להלן – הוראת השעה), ביחס למגזר השירותים הדיגיטליים ושירותי האחסון, והביאו לשיפור ניכר בהגנת הסייבר של המשק הישראלי. ההסדר המוצע בסימן זה נועד, בהתבסס בין השאר על הניסיון המצטבר ביישום הוראת השעה, לעגן הסדרים דומים ביחס לארגונים חיוניים וכן ביחס לארגונים במגזר השירותים הדיגיטליים ושירותי האחסון גם אם אינם ארגונים חיוניים.

סעיף 13 מוצע לקבוע שתקיפת סייבר חמורה לעניין חוק זה, היא תקיפת סייבר שיש חשש ממשי כי מתקיימים לגביה אחד או יותר מהמאפיינים שלהלן, שהם מאפיינים המקנים לתקיפה ממד מיוחד של חומרה:

1. היא פוגעת ברציפות התפקודית של ארגון חיוני, ובכלל זה בתהליך חיוני בארגון.

2. היא פוגעת בזמינות, ברציפות או במהימנות השירות שארגון חיוני מספק.

3. היא מאפשרת לגורם שאינו מורשה לכך גישה לנכס מידע משמעותי של ארגון חיוני.

4. היא מבוצעת נגד ארגון חיוני או באמצעותו והיא בעלת מאפיינים המעידים על חומרה מיוחדת, לרבות מתאר התקיפה או זהות התוקף, וכמו כן היא עלולה לפגוע בביטחון המדינה או בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור; או שקיים חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לארגון הנתקף.

מתן הוראות לארגון חיוני במגזר המנוי בתוספת השלישית להתמודדות עם תקיפת סייבר חמורה

14. (א) מנהל בכיר ברשות מוסמכת כאמור בפסקה (1) להגדרה "רשות מוסמכת" שבסעיף 1 (בסעיף זה – רשות מוסמכת), רשאי לקבוע, ככל האפשר בנסיבות העניין בהתייעצות עם המערך, כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה נגד ארגון חיוני במגזר שהרשות מוסמכת לעניין פעילות בו בתחום הגנת הסייבר, או תקיפה כאמור הנעשית באמצעות הארגון החיוני, הדורשת את מעורבותו.

(ב) היה למנהל בכיר ברשות מוסמכת יסוד סביר להניח כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר שמתקיים לגביה האמור בסעיף קטן (א), רשאי הוא, בעצמו או באמצעות עובד מוסמך מגזרי, לדרוש מהארגון החיוני להציג לו כל ידיעה או מסמך, לרבות פלט, כדי להבטיח או להקל את ביצועו של אותו סעיף קטן.

דברי הסבר

סעיף 14 כללי

סעיף מוצע זה נועד לאפשר לרשות המוסמכת, בנסיבות מסוימות, לתת הוראות לארגון חיוני במגזר המנוי בתוספת הראשונה לחוק המוצע, לשם התמודדות עם תקיפת סייבר שמתרחשת או שיש חשש ממשי שעומדת להתרחש, ושמנהל בכיר ברשות המוסמכת מצא שהיא תקיפת סייבר חמורה כהגדרתה בסעיף 13, הדורשת את מעורבותו. הנחת המוצא היא שארגון חיוני יתמודד כנדרש עם תקיפת סייבר חמורה, אך יחד עם זאת, לנוכח ההשלכות האפשריות של תקיפה כזו, מוצע לאפשר לרשות מוסמכת לתת הוראות מחייבות לארגון חיוני בנסיבות שבהן אותו ארגון אינו מתמודד באופן הולם עם תקיפת סייבר חמורה. תכליתן של הוראות אלה היא לוודא שהארגון החיוני פועל כנדרש לאיתור התקיפה, מניעתה או בלימתה, וזאת כדי לצמצם את נזקי התקיפה, ועל ידי כך להגן על האינטרס הציבורי העלול להיפגע כתוצאה מתקיפת הסייבר החמורה. הסעיף המוצע בא לקבוע הליך מינהלי סדור שיופעל באופן מדורג בכמה שלבים, ושמגולם בו איזון בין הצורך להגן על ארגונים, ובכך – על האינטרס הציבורי, מפני תקיפת סייבר חמורה לבין הצורך להגן על אינטרסים נוספים של הארגון המותקף ועל זכויות של צדדים שלישיים, דוגמת עובדי הארגון, ובעלי עניין נוספים.

לסעיף קטן (א)

מוצע להסמיך מנהל בכיר ברשות מוסמכת כאמור בפסקה (1) להגדרה "רשות מוסמכת" שבסעיף 1 לחוק המוצע, לקבוע, בהתייעצות עם מערך הסייבר הלאומי, אלא אם כן מתקיימות נסיבות שאינן מאפשרות את קיום ההתייעצות, כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה, כהגדרתה בסעיף 13 המוצע, נגד או באמצעות ארגון חיוני במגזר שהרשות המוסמכת פועלת לגביו, הדורשת את מעורבותו. יובהר כי לא בכל מצב שבו מתקיימת תקיפת סייבר חמורה תידרש מעורבות הרשות המוסמכת. הציפייה היא כי ארגון חיוני יתמודד עם תקיפות סייבר חמורות באופן הולם, ולכן אם נראה שהארגון מודע לתקיפת הסייבר החמורה ומתמודד עימה באופן הולם, לא תידרש בהכרח קביעה כאמור.

לסעיף קטן (ב)

כדי להקל על מימוש הסמכות המוצעת לעיל, ובכלל זה לדאוג לכך שלפני המנהל הבכיר יהיו הנתונים הנדרשים לצורך הקביעה אם תקיפה מסוימת היא תקיפת סייבר חמורה, מוצע לקבוע שאם היה למנהל בכיר ברשות מוסמכת יסוד סביר להניח כי תקיפת סייבר שמתרחשת או שקיים חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה כהגדרתה בסעיף 13, נגד ארגון חיוני במגזר שהרשות המוסמכת פועלת לגביו, או שהיא תקיפה כאמור הנעשית באמצעות הארגון החיוני, ונדרשת מעורבות מצידו לשם התמודדות איתה, הוא יהיה רשאי, בעצמו או באמצעות עובד מוסמך מגזרי, לדרוש מהארגון החיוני להציג לו כל ידיעה או מסמך, לרבות פלט, הנדרשים כדי להקל על הקביעה אם התקיפה האמורה היא תקיפת סייבר חמורה.

יובהר כי הפנייה של רשות מוסמכת לארגון לצורך דרישת ידיעות ומסמכים מכוח סעיף מוצע זה תבוצע באופן מצומצם והדרגתי ככל האפשר, בשים לב לנתונים הקיימים בידי הרשות ולמידע הנדרש לה לבחינת חומרת התקיפה. כך לדוגמה, אם לצורך החלטה בשאלה אם התקיפה הנבחנת היא תקיפת סייבר חמורה, נדרש למנהל המוסמך מידע בנוגע לאפשרות השפעת התקיפה על ארגון אחר, לצורך הערכת הסיכון הנגזר מן התקיפה, הרי דרישת המידע הראשונית תתמקד במידע הנוגע לכך; כמו כן, במקרה שבו קיים ספק באשר למאפיינים הטכנולוגיים של התקיפה לשם הבנת חומרתה, תתמקד הפנייה, ככל האפשר, בדרישה ממוקדת לקבלת המאפיינים הטכנולוגיים הנדרשים לצורך הבחינה האמורה.

(ג) הודיע עובד מוסמך מגזרי לארגון חיוני, לאחר שהזדהה לפניו, על קביעה כאמור בסעיף קטן (א), יחולו הוראות אלה:

(1) העובד המוסמך המגזרי יפרט לפני הארגון החיוני את התשתית העובדתית והמקצועית לקביעה כאמור, אם אין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים;

(2) העובד המוסמך המגזרי ייתן לארגון החיוני הזדמנות לפעול באופן הולם לאיתור התקיפה, מניעתה או בלימתה, בתוך פרק זמן סביר שיימסר לארגון, והכול בהתחשב במאפייני תקיפת הסייבר;

(3) הארגון החיוני יעדכן את העובד המוסמך המגזרי בדבר הפעולות שביצע לאיתור התקיפה, מניעתה או בלימתה בתוך פרק זמן סביר כאמור בפסקה (2);

(4) מצא העובד המוסמך המגזרי כי הארגון החיוני לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה, כאמור בפסקה (2), רשאי הוא, אם מצא שהדבר נדרש לשם איתור התקיפה, מניעתה או בלימתה, ולאחר שהודיע לארגון החיוני על כוונתו לתת לו הוראות לפי פסקה זו ונתן לו הזדמנות להשמיע טענותיו, לתת לו, ככל האפשר בנסיבות העניין בהתייעצות עם מערך הסייבר הלאומי, הוראות, בכתב או בעל פה, שיבצע הארגון, ובכלל זה הוראות לביצוע פעולות להגנת סייבר בחומר מחשב או הוראות למסירת ידיעה או מסמך הנוגעים לאיתור התקיפה, מניעתה או בלימתה, לרבות העתק של חומר מחשב, לידי העובד; במתן הוראות לפי פסקה זו –

דברי הסבר

לסעיף קטן (ג)

על פי המוצע, תנאי להפעלת הסמכות למתן הוראות להתמודדות עם תקיפת סייבר חמורה לפי הסעיף המוצע, הוא מתן הודעה בידי עובד מוסמך מגזרי, לארגון חיוני, על קביעת מנהל בכיר כאמור בסעיף קטן (א), ולאחר שהודיע כאמור יחל הליך מדורג, כמפורט להלן:

1. תחילה, יפרט העובד המוסמך המגזרי לפני הארגון החיוני את התשתית העובדתית והמקצועית לקביעה כי מדובר בתקיפה חמורה, אם אין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים.

2. לאחר מתן ההודעה כאמור, העובד המוסמך ייתן לארגון החיוני הזדמנות לפעול באופן הולם לאיתור התקיפה, מניעתה, ובכלל זה מניעתה מבעוד מועד או מניעת הישנותה, או בלימתה, הכול בתוך פרק זמן סביר שיקבע העובד המוסמך המגזרי ויימסר לארגון החיוני על ידו; פרק הזמן כאמור ייקבע בהתחשב, בין השאר, במאפייני תקיפת הסייבר.

3. בהמשך לכך, הארגון החיוני יעדכן את העובד המוסמך המגזרי, בתוך פרק הזמן שקבע לכך העובד האמור, בדבר הפעולות שביצע למטרות הנזכרות לעיל.

4. אם העובד המוסמך המגזרי הגיע למסקנה שהארגון החיוני לא פעל באופן הולם לאיתור תקיפת הסייבר החמורה, מניעתה או בלימתה, הוא יהיה רשאי, אם מצא שהדבר נדרש לאיתור התקיפה, מניעתה או בלימתה, להודיע לארגון החיוני על כוונתו לתת לו הוראות מחייבות, ולארגון תינתן הזדמנות להשמיע את טענותיו לעניין הכוונה לתת לו הוראות כאמור. לעניין זה, יודגש כי לא יינתנו הוראות מכוח סעיף קטן מוצע זה לארגון חיוני אשר טיפל באופן הולם באיתור התקיפה, מניעתה או בלימתה. לאחר שמיעת טענות הארגון החיוני, יוכל העובד המוסמך המגזרי, ככל האפשר בנסיבות העניין בהתייעצות עם מערך הסייבר הלאומי כגורם הלאומי המתכלל, לתת לארגון הוראות, בכתב או בעל פה, וזאת ככל שהדבר נדרש לצורך איתור התקיפה, מניעתה או בלימתה. מובהר כי גם בשלב מתקדם זה בהליך מתן ההוראות, החוק המוצע אינו מסמיך את העובד המוסמך המגזרי לבצע בעצמו פעולות במחשביו של הארגון, וההוראות שייתן העובד יבוצעו על ידי הארגון.

על פי המוצע, במסגרת הפעלת סמכותו לפי סעיף זה, יוכל העובד המוסמך לתת לארגון החיוני, בין השאר, הוראות לביצוע פעולות להגנת סייבר בחומר מחשב כהגדרתן המוצעת בסעיף 1 לחוק המוצע, היינו להורות לארגון לתת הוראות למחשב בשפת קריאת מחשב לשם הגנת סייבר. בתוך כך, יוכל העובד המוסמך להורות לארגון החיוני לבצע סריקה, עיבוד, הסרה של חומר מחשב הנוגע לתקיפת סייבר, התקנת סוג תוכנה שפעולתו מוגבלת לרשת הארגון בלבד, חסימה או ניתוק של מחשב או יצירת עותק של חומר מחשב. כמו כן, יוכל העובד המוסמך המגזרי לתת סוגי הוראות נוספים מכוח סעיף מוצע זה, ובכלל זה הוראה למסור לידיו ידיעה או מסמך הנוגעים לאיתור התקיפה, לרבות עותק של חומר מחשב.

(א) ישקול העובד המוסמך המגזרי את השפעתן האפשרית על פעילות הארגון החיוני ועל צד שלישי, ובכלל זה על הזכות לפרטיות, וכן את העלות הכלכלית המוערכת של יישום ההוראות והשפעתן האפשרית על הרציפות התפקודית של הארגון, למיטב ידיעתו של העובד, ואם הארגון החיוני מסר הערכה לעניין זה – בהתחשב בהערכה שמסר;

(ב) יורה העובד המוסמך המגזרי לנקוט אמצעי שפגיעתו פחותה לאיתור התקיפה, מניעתה או בלימתה;

(ג) יפרט העובד המוסמך המגזרי את המועד האחרון לביצוע ההוראה;

(5) נתן עובד מוסמך מגזרי לארגון החיוני הוראה לפי פסקה (4), יפעל הארגון בהתאם לה עד המועד האחרון שנקבע לביצועה כאמור בפסקה (4)(ג), וידווח על אופן ביצועה לעובד המוסמך המגזרי עד המועד האמור.

(ד) (1) מסר עובד מוסמך מגזרי לארגון חיוני הודעה כאמור בסעיף קטן (ג), ימסור הארגון, בלא דיחוי, עדכון בדבר תקיפת הסייבר החמורה לכל ארגון העלול להיפגע ממנה ישירות ובאופן ממשי, וידווח על כך בכתב לעובד המוסמך המגזרי, והכול אלא אם כן הורה העובד המוסמך המגזרי, בהתייעצות עם מערך הסייבר הלאומי, אחרת.

(2) מנהל בכיר ברשות המוסמכת רשאי, לפי בקשה בכתב מאת ארגון חיוני, ובהתייעצות עם מערך הסייבר הלאומי, לפטור את הארגון החיוני מחובת היידוע כאמור בפסקה (1) או לדחות את מועד היידוע, אם שוכנע כי קיימות נסיבות חריגות המצדיקות זאת.

דברי הסבר

יובהר כי בהתאם להנחיית היועצת המשפטית לממשלה מספר 1.2500, שעניינה "כללים מנחים לגיבוש הסדרים דיגיטליים" מיום י"א בתשרי התש"ף (10 אוקטובר 2019), "הסדר דיגיטלי לא יעדיף – ככל הניתן – אמצעי טכנולוגי אחד על פני אמצעי טכנולוגי אחר, אם שניהם מגשימים את השימושים והמטרות של אותו ההסדר". בהתאם לכך, מוצע לקבוע שהעובד המוסמך המגזרי יהיה רשאי, במסגרת הפעלת סמכותו לפי סעיף זה, להורות על התקנת תוכנה מסוג מסוים ולא על התקנת תוכנה מסוימת, מקום שבו יש יותר מתוכנה אחת המגשימה את אותם השימושים והמטרות. זאת ועוד, בהתאם להגדרה המוצעת למונח "פעולה להגנת סייבר בחומר מחשב", מתן הוראה מחייבת על ידי עובד מוסמך מגזרי לפי חוק מוצע זה, להתקנת תוכנה, תתייחס לסוג תוכנה שפעולתו מוגבלת לרשת של הארגון החיוני, בלבד.

מוצע להתוות את שיקול דעתו של העובד המוסמך המגזרי בהפעלת סמכות לפי סעיף 14 לחוק המוצע, כך שבמתן הוראות לפי סעיף זה הוא יידרש לשקול את השפעתן האפשרית של ההוראות על פעילות הארגון החיוני ועל צד שלישי, ובכלל זה על הזכות לפרטיות, וכן את העלות הכלכלית המוערכת של יישום ההוראות ואת השפעתן האפשרית על הרציפות התפקודית של הארגון, למיטב ידיעתו של העובד, ואם הארגון החיוני מסר הערכה כלכלית לעניין זה – בהתחשב בהערכה שמסר.

כמו כן, כדי להדגיש את חובת העובד המוסמך המגזרי לפעול במידתיות, מוצע לקבוע שהוא יורה לנקוט אמצעי שפגיעתו פחותה לאיתור התקיפה, מניעתה או בלימתה. יובהר בהקשר זה שבמרבית המקרים המידע המתקבל בהקשר של התמודדות עם תקיפת סייבר הוא מידע טכנולוגי שאינו מכיל מידע אישי כהגדרתו בחוק הגנת הפרטיות, התשמ"א–1981 (להלן – מידע אישי, חוק הגנת הפרטיות).

נוסף על כך, מוצע לקבוע שבעת מתן ההוראה, העובד המוסמך המגזרי יפרט את המועד האחרון לביצועה, והארגון יידרש לפעול בהתאם לה עד למועד שצוין ולדווח על אופן ביצועה לעובד המוסמך המגזרי.

לסעיף קטן (ד)

בשל הצורך למנוע התפשטות תקיפות סייבר חמורות ולצמצם את השלכותיהן, מוצע לקבוע כי אם מסר עובד מוסמך מגזרי לארגון חיוני הודעה על תקיפה חמורה, בהתאם לסעיף קטן (ג) המוצע, הארגון יידרש למסור, בלא דיחוי, עדכון בדבר תקיפת הסייבר החמורה לכל ארגון העלול להיפגע ממנה ישירות ובאופן ממשי, ולדווח על העדכון שמסר כאמור, בכתב, לעובד המוסמך המגזרי, והכול אלא אם כן הורה העובד המוסמך המגזרי, בהתייעצות עם מערך הסייבר הלאומי, אחרת.

נוסף על כך, מוצע שאם מתקיימות נסיבות חריגות המצדיקות זאת, יוכל מנהל בכיר ברשות מוסמכת, לפי בקשה בכתב מאת הארגון החיוני, ולאחר התייעצות עם מערך הסייבר הלאומי, לפטור את הארגון החיוני מהחובה למסור עדכון כאמור, או לדחותה.

מתן הוראות לארגון חיוני שהוא גוף ממשלתי להתמודדות עם תקיפת סייבר חמורה

15. (א) קבע מנהל בכיר ברשות מוסמכת כאמור בפסקה (2) להגדרה "רשות מוסמכת", כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה נגד גוף ממשלתי או תקיפה כאמור הנעשית באמצעות גוף ממשלתי, הדורשת את מעורבותו, והודיע על כך עובד מוסמך מגזרי לגוף הממשלתי, יפעל הגוף הממשלתי להתמודדות עם התקיפה בהתאם להוראות שייתן לו העובד המוסמך המגזרי, בהתייעצות עם המערך.

(ב) במתן הוראות לפי סעיף קטן (א) ישקול העובד המוסמך המגזרי את השפעתן האפשרית על פעילות הגוף הממשלתי ועל צד שלישי, ובכלל זה על הזכות לפרטיות, וכן את העלות הכלכלית המוערכת של יישום ההוראות והשפעתן האפשרית על הרציפות התפקודית של הגוף, למיטב ידיעתו של העובד, ואם הגוף הממשלתי מסר הערכה לעניין זה – בהתחשב בהערכה שמסר, ויורה לנקוט אמצעי שפגיעתו פחותה לאיתור התקיפה, מניעתה או בלימתה.

(ג) הסמכות הנתונה למנהל בכיר ברשות מוסמכת ולעובד מוסמך מגזרי לפי סעיף 14(ב) תהיה נתונה למנהל בכיר ברשות מוסמכת כאמור בסעיף קטן (א) ולעובד מוסמך מגזרי גם לעניין סעיף זה.

מתן הוראות להתמודדות עם תקיפת סייבר חמורה שנקבעה בידי מנהל בכיר במערך

16. (א) הסמכויות הנתונות למנהל בכיר ברשות מוסמכת ולעובד מוסמך מגזרי כלפי ארגון חיוני לפי סעיפים 14 ו־15 יהיו נתונות גם למנהל בכיר במערך ולעובד מוסמך במערך, כמפורט להלן, ויחולו לעניין זה ההוראות לפי אותם סעיפים, בשינויים המחויבים:

דברי הסבר

סעיף 15 לסעיף קטן (א)

מוצע לקבוע הסדר דומה להסדר המוצע בסעיף 14 לחוק המוצע, לעניין תקיפת סייבר חמורה נגד גוף ממשלתי או באמצעותו, בהתאמות הנדרשות. יובהר שביחס לגופים ממשלתיים, בשל אופיים הייחודי והציפייה המוגברת מהם לפעול באופן מיידי לטיפול בתקיפות סייבר חמורות בהתאם להנחיות הרשות המוסמכת, לא מוצע בסעיף זה הליך מדורג כפי שמוצע לקיים טרם מתן הוראות לארגונים חיוניים שאינם גופים ממשלתיים, כאמור בסעיף 14 לחוק המוצע.

על פי המוצע, יוכל מנהל בכיר ברשות המוסמכת (שהיא, לגבי הגופים הממשלתיים – מערך הדיגיטל הלאומי), לקבוע שתקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש היא תקיפת סייבר חמורה כהגדרתה בסעיף 13 המוצע, נגד גוף ממשלתי או באמצעותו, הדורשת את מעורבותו. לאחר שהודיע על כך העובד המוסמך המגזרי לגוף הממשלתי, הוא יוכל לתת לו הוראות להתמודדות עם התקיפה, בהתייעצות עם מערך הסייבר הלאומי כגורם המקצועי הלאומי המתכלל בתחום הגנת הסייבר, והגוף הממשלתי יפעל בהתאם לאותן הוראות.

לסעיף קטן (ב)

מוצע להתוות את שיקול הדעת של העובד המוסמך המגזרי ולקבוע כי במתן הוראות כאמור בסעיף קטן (א) המוצע, הוא ישקול את השיקולים המנויים בסעיף קטן (ב) המוצע.

לסעיף קטן (ג)

מוצע להקנות למנהל בכיר ברשות מוסמכת ולעובד מוסמך מגזרי כאמור, כלומר למנהל בכיר ולעובד מוסמך במערך הדיגיטל, את הסמכות לפי סעיף 14(ב) לחוק המוצע, שעניינה דרישת ידיעות ומסמכים מגוף ממשלתי, בנסיבות המנויות באותו סעיף.

סעיף 16 הצעת חוק זו באה לעגן, בין השאר, כללים הנוגעים להתמודדות של ארגון חיוני עם תקיפת סייבר חמורה, וזאת ככל שנדרש בליווי היחידה המגזרית ברשות המוסמכת הנוגעת לעניין. במקביל, בשים לב לכך שמערך הסייבר הלאומי הוא הגוף הלאומי בעל ראיית הרוחב המחזיק בכלים נוספים להתמודדות עם תקיפות סייבר חמורות, נקודת המוצא בראייה לאומית היא שבנסיבות מסוימות נדרשת מעורבות ישירה של מערך הסייבר הלאומי בליווי ההתמודדות של הארגון עם תקיפות סייבר חמורות. לפיכך, מוצע לקבוע בסעיף זה את הנסיבות שבהתקיימן יוכל המערך להתערב וללוות ארגון חיוני שמבוצעת נגדו או באמצעותו תקיפת סייבר חמורה.

לסעיף קטן (א)

מוצע להקנות למנהל בכיר במערך את הסמכות הנתונה למנהל בכיר ברשות מוסמכת לפי סעיפים 14 ו־15 לחוק המוצע, לקבוע כי תקיפת סייבר נגד ארגון חיוני כאמור בהם היא תקיפת סייבר חמורה כהגדרתה בסעיף 13, הדורשת את מעורבותו, וכן להקנות לעובד מוסמך במערך את הסמכויות הנתונות בסעיפים 14 ו־15 האמורים לעובד מוסמך מגזרי. הוראות הסעיפים האמורים יחולו על

(1) כלפי ארגון חיוני;

(2) כלפי ספק שירותים דיגיטליים ושירותי אחסון, ויקראו את ההגדרה "תקיפת סייבר חמורה" שבסעיף 13, לעניין ספק כאמור, בשינויים המחויבים.

(ב) על אף האמור בסעיף קטן (א), עובד מוסמך במערך רשאי להפעיל סמכויות הנתונות לעובד מוסמך מגזרי לפי סעיפים 14 או 15 כלפי ארגון חיוני, רק אם קבע ראש מערך הסייבר הלאומי על פי פנייה מאת רשות מוסמכת שיש מקום לסייע לה בהפעלת הסמכויות לפי אותם סעיפים, או אם קבע, לאחר שקיים ככל האפשר בנסיבות העניין התייעצות עם הרשות המוסמכת, שקיים חשש ממשי כי תקיפת סייבר חמורה נגד הארגון החיוני או באמצעותו תתפשט במהירות לארגונים רבים, תתפשט ליותר ממגזר אחד או תפגע בביטחון המדינה או בביטחון הציבור; בסעיף קטן זה, "ארגון חיוני" – למעט ארגון חיוני ממגזר שמערך הסייבר הלאומי הוא הרשות המוסמכת לעניין פעילות בתחום הגנת הסייבר של ארגונים הפועלים בו.

(ג) קבע ראש מערך הסייבר הלאומי כאמור בסעיף קטן (ב), יידע את הרשות המוסמכת בדבר קביעתו, והסמכויות לעניין תקיפת הסייבר יופעלו כלפי הארגון החיוני על פי הוראה מאת עובד מוסמך במערך, בלבד, וזאת ככל האפשר בנסיבות העניין באמצעות הרשות המוסמכת.

תיעוד

17. עובד מוסמך מגזרי או עובד מוסמך במערך יתעד בכתב את ההוראות שניתנו לארגון לפי סעיפים 14, 15 או 16 וימסור לארגון נוסח כתוב של ההוראות שכולל מידע בלתי מסווג בלבד, בהקדם האפשרי לאחר מתן ההוראות.

דברי הסבר

פי המוצע, בשינויים המחויבים, לעניין הפעלת הסמכויות לפי סעיף מוצע זה.

על פי המוצע, סמכויות אלה יוקנו לגורמים הנזכרים כלפי ארגונים חיוניים וכן כלפי ספקי שירותים דיגיטליים ושירותי אחסון אף אם אינם ארגון חיוני. ביחס למגזר השירותים הדיגיטליים ושירותי האחסון, שכאמור לעיל, מערך הסייבר הלאומי הוא הרשות המוסמכת לגביו, מוצע כי הסמכות למתן הוראות להתמודדות עם תקיפת סייבר חמורה תהיה נתונה לעניין כלל הארגונים במגזר ולא רק ביחס לארגונים חיוניים במגזר זה. הסדר זה נדרש בשל המאפיינים הייחודיים של המגזר האמור, ובהם: החיבוריות הגבוהה של ספקי שירותי אחסון וספקי שירותים דיגיטליים שעלולה להיות מנוצלת בידי תוקפים לגרימת נזק רחב היקף, ופוטנציאל הנזק למשק הגלום בתקיפת סייבר חמורה נגד ארגונים במגזר זה גם אם אינם ארגונים חיוניים. יודגש כי כיום, מוקנית סמכות דומה למערך הסייבר הלאומי מכוח הוראת השעה ביחס למגזר השירותים הדיגיטליים ושירותי האחסון, והניסיון מיישומה מלמד כי הסמכות חיונית להגנת הסייבר במגזר זה לנוכח המאפיינים המתוארים לעיל.

לסעיף קטן (ב)

מוצע לקבוע ביחס לארגונים חיוניים שאינם שייכים למגזר שבו מערך הסייבר הלאומי הוא הרשות המוסמכת, כי עובד מוסמך במערך יוכל להפעיל כלפיהם סמכות לפי סעיפים 14 או 15 לחוק המוצע, רק אם מתקיימת אחת מהנסיבות המנויות בסעיף קטן (ב), וזן:

א. אם רשות מוסמכת פנתה לראש מערך הסייבר הלאומי בבקשה לסיוע בהפעלת סמכויותיה כלפי ארגון חיוני לפי סעיפים 14 או 15 האמורים, וראש המערך מצא כי יש מקום להיענות לפנייתה. פנייה כאמור עשויה לנבוע, למשל, מהצורך להסתייע ביכולות המצויות בידי מערך הסייבר הלאומי במסגרת התמודדות עם התקיפה, אשר אינן מצויות בידי הרשות המוסמכת.

ב. אם ראש המערך קבע, לאחר שקיים ככל האפשר בנסיבות העניין התייעצות עם הרשות המוסמכת, שקיים חשש ממשי כי תקיפת סייבר חמורה נגד הארגון החיוני או באמצעותו תתפשט במהירות לארגונים רבים, תתפשט ליותר ממגזר אחד או תפגע בביטחון המדינה או בביטחון הציבור.

לסעיף קטן (ג)

כדי להבטיח תיאום וסינכרון מול הארגון החיוני, מוצע לקבוע כי מרגע שראש מערך הסייבר הלאומי הפעיל את סמכותו לפי סעיף קטן (ב) המוצע, וקבע כי מתקיימות הנסיבות כאמור בו להפעלת סמכויות עובד מוסמך במערך כלפי ארגון חיוני, הוא יידע את הרשות המוסמכת בדבר קביעתו, והסמכויות לעניין תקיפת הסייבר יופעלו כלפי הארגון החיוני על פי הוראה מאת עובד מוסמך במערך, בלבד, וזאת ככל האפשר בנסיבות העניין באמצעות הרשות המוסמכת, שיש עדיפות לכך שהיא זו שתהיה בקשר ישיר עם הארגון החיוני.

סעיף 17 מוצע לקבוע במפורש שעובד מוסמך מגזרי או עובד מוסמך במערך יתעד בכתב את ההוראות שניתנו לארגון לצורך התמודדות עם תקיפת סייבר חמורה

מתן הוראות להתמודדות עם תקיפת סייבר חמורה שנקבעה בידי צה"ל או השירות

18. (א) ראש חטיבת הגנה בסייבר בצה"ל, ובהיעדרו – ממלא מקומו, רשאי לקבוע כי תקיפת סייבר שמתרחשת או שיש חשש ממשי שהיא עומדת להתרחש, היא תקיפת סייבר חמורה נגד ארגון חיוני, ארגון חיוני למערכת הביטחון או ספק שירותים דיגיטליים או שירותי אחסון, או באמצעות ארגון כאמור, הדורשת מעורבות של המערך או מלמ"ב לפי סימן זה או סימן ד', בהתאמה, אם מצא כי יש חשש ממשי שיש בה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל.

(ב) ראש שירות הביטחון הכללי או עובד בכיר בשירות הביטחון הכללי (בפרק זה – השירות), בדרגת ראש חטיבה לפחות, שראש השירות הסמיכו לעניין חוק זה (בחוק זה – מנהל בכיר בשירות), ובהיעדרו – ממלא מקומו, רשאי לקבוע כי תקיפת סייבר שמתרחשת או שקיים חשש ממשי שהיא עומדת להתרחש היא תקיפת סייבר חמורה נגד ארגון כאמור בסעיף קטן (א) או באמצעותו, הדורשת מעורבות של המערך או מלמ"ב לפי סימן זה או סימן ד', בהתאמה, אם מצא כי הדבר נדרש לשם מילוי תפקידי השירות כאמור בסעיף 7(ב)(1) ו־(2) לחוק שירות הביטחון הכללי.

(ג) קבע ראש חטיבת ההגנה בסייבר בצה"ל או מנהל בכיר בשירות, כאמור בסעיפים קטנים (א) או (ב), יראו את הקביעה כקביעת מנהל בכיר במערך לפי סעיף 16(א) ויחולו הוראות סעיף 16(א) ו־(ג), בשינויים המחויבים; ואולם, הייתה הקביעה כאמור לעניין ארגון חיוני למערכת הביטחון, יראו אותה כקביעה של מנהל בכיר במלמ"ב לפי סעיף 14(א) כפי שהוחל בסעיף 21(א)(2).

דברי הסבר

לפי סעיפים 14, 15 או 16 לחוק המוצע. עוד מוצע כי אותו עובד ימסור לארגון נוסח כתוב של ההוראות שכולל מידע בלתי מסווג בלבד, בהקדם האפשרי לאחר מתן ההוראות.

סעיף 18 מתוך הבנת הסיכון וכדי לתת מענה לאומי כולל, מוצע לקבוע נסיבות מתוחמות שבהן תינתן סמכות לבעלי תפקידים בכירים בצבא הגנה לישראל (להלן – צה"ל) או בשירות הביטחון הכללי (להלן – השירות) לקבוע שתקיפת סייבר נגד ארגונים חיוניים מסוימים המנויים בסעיף היא תקיפת סייבר חמורה, וזאת כאשר הם הגורמים שבידיהם התשתית העובדתית הנדרשת להערכת חומרת התקיפה והשלכותיה האפשריות כמוצע בסעיף. יובהר כי מדובר בסמכות קביעה בלבד, שלא נגזרות ממנה סמכויות לביצוע פעולות או למתן הוראות על ידי צה"ל או השירות. כלומר, אם אותם בעלי תפקידים בכירים יקבעו שתקיפת סייבר מסוימת היא תקיפת סייבר חמורה, הסמכויות למתן הוראות להתמודדות איתה יוקנו לפי המוצע למערך הסייבר הלאומי, ולעניין ארגונים חיוניים למערכת הביטחון כהגדרתם המוצעת – למלמ"ב, בהתאם לסמכויות שמוצע להקנות להם לעניין זה לפי החוק המוצע, וכמפורט להלן.

לסעיף קטן (א)

מוצע להסמיך את ראש חטיבת ההגנה בסייבר בצה"ל, ובהיעדרו – את ממלא מקומו, לקבוע שתקיפת סייבר שמתרחשת או שיש חשש ממשי שהיא עומדת להתרחש היא תקיפת סייבר חמורה, כהגדרתה בסעיף 13 לחוק המוצע, נגד ארגון חיוני, ארגון חיוני למערכת הביטחון או ספק שירותים דיגיטליים או שירותי אחסון, או באמצעות ארגון כאמור, הדורשת מעורבות של מערך הסייבר הלאומי לפי סימן זה או מעורבות של מלמ"ב לפי סימן ד' המוצע, וזאת אם מצא כי קיים חשש ממשי שיש בתקיפה האמורה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל.

לסעיף קטן (ב)

מוצע להסמיך את ראש השירות או עובד בכיר בשירות, בדרגת ראש חטיבה לפחות, שראש השירות הסמיכו לעניין חוק זה (להלן – מנהל בכיר בשירות), ובהיעדרו – את ממלא מקומו, לקבוע כי תקיפת סייבר שמתרחשת או שיש חשש ממשי שהיא עומדת להתרחש היא תקיפת סייבר חמורה נגד ארגון כאמור בסעיף קטן (א) המוצע או תקיפה כאמור הנעשית באמצעותו, הדורשת מעורבות של מערך הסייבר הלאומי או של מלמ"ב לפי סימן מוצע זה או סימן ד' המוצע, וזאת אם מצא כי הדבר נדרש לשם מילוי תפקידי השירות כאמור בסעיף 7(ב)(1) ו־(2) לחוק שירות הביטחון הכללי, התשס"ב–2002 (להלן – חוק שירות הביטחון הכללי).

לסעיף קטן (ג)

מוצע כי קביעה שניתנה לפי סעיפים קטנים (א) ו־(ב) לסעיף מוצע זה, תיחשב לקביעה של מנהל בכיר במערך לפי סעיף 16(א) לחוק המוצע, ויחולו הוראות סעיף 16(א) ו־(ג) לחוק המוצע, בשינויים המחויבים, בלא צורך בתהליך הקבוע בסעיף 16(ב) לחוק המוצע. ואולם אם הייתה הקביעה האמורה בעניין תקיפת סייבר חמורה נגד ארגון חיוני למערכת הביטחון או באמצעותו, יראו אותה כקביעה של מנהל בכיר במלמ"ב לפי סעיף 14(א) לחוק המוצע, כלומר, הסמכות לתת הוראות תהיה מוקנית

סימן ד׳: הוראות מיוחדות לעניין ארגון חיוני למערכת הביטחון

סימן ד׳ בפרק ה׳ – הגדרות

19. בסימן זה –

"מלמ"ב" – הממונה על הביטחון במערכת הביטחון;

"מערכת הביטחון" – צה"ל, משרד הביטחון, מלמ"ב ומפעלי מערכת הביטחון כמשמעותם בסעיף 20 לחוק להסדרת הביטחון בגופים ציבוריים.

קביעת ארגון חיוני למערכת הביטחון

20. (א) שר הביטחון, לפי המלצת ראש מלמ"ב, רשאי לקבוע שארגון הוא ארגון חיוני למערכת הביטחון, אם מצא, לאחר שניתנה לארגון הזדמנות להשמיע את עמדתו, כי מתקיימים כל אלה:

(1) הוא אינו גוף מונחה;

(2) מתקיים לגביו אחד מאלה:

(א) קיימת התקשרות בתוקף בין הארגון לבין גוף הנמנה עם מערכת הביטחון, שמכוחה הארגון מספק למערכת הביטחון מוצרים, שירותים, ידע או טכנולוגיות שהם חיוניים לפעילות ביטחונית או מבצעית של גוף הנמנה עם מערכת הביטחון, ושפגיעה בזמינותם או תפקודם בשל תקיפת סייבר עלולה לגרום לפגיעה משמעותית בביטחון המדינה או ברציפות התפקוד של גוף הנמנה עם מערכת הביטחון;

(ב) הייתה התקשרות בין הארגון לבין גוף הנמנה עם מערכת הביטחון, שטרם חלפו חמש שנים ממועד סיומה, ומכוחה הארגון מחזיק מידע על מוצרים, שירותים, ידע או טכנולוגיות כאמור בפסקת משנה (א), שמתקיים לגביהם האמור בסיפה של אותה פסקת משנה.

דברי הסבר

למלמ"ב. כפי שיפורט להלן, הסמכות לקבוע כאמור ביחס לארגונים חיוניים למערכת הביטחון נתונה לראש מלמ"ב מכוח סעיף 21(א)(2) לחוק המוצע.

סימן ד׳: הוראות מיוחדות לעניין ארגון חיוני למערכת הביטחון

סעיף 19 בסעיף זה מוצעות הגדרות למונחים שנעשה בהם שימוש בסימן מוצע זה. במסגרת זו, מוצע להגדיר את "מערכת הביטחון", ככוללת את צה"ל, משרד הביטחון, מלמ"ב ומפעלי מערכת הביטחון כמשמעותם בסעיף 20 לחוק להסדרת הביטחון.

סעיף 20 ותוספת חמישית בשל צרכים ייחודיים של הגנת סייבר הקיימים לעיתים בחלק מהארגונים שיש להם, או שהייתה להם, התקשרות עם גופים במערכת הביטחון, מוצע לקבוע תהליך סדור להגדרת ארגון כארגון חיוני למערכת הביטחון לפי החוק המוצע, בהתחשב בתבחינים ובגדרים המוצעים לעניין זה. על פי המוצע, הרשות המוסמכת לגבי ארגונים אלה לעניין חוק זה תהיה מלמ"ב.

לסעיף קטן (א)

מוצע לקבוע כי הסמכות לקבוע שארגון הוא ארגון חיוני למערכת הביטחון תהיה נתונה לשר הביטחון, לפי המלצת ראש מלמ"ב, והוא יקבע כאמור אם מצא, לאחר שניתנה לארגון הזדמנות להשמיע את עמדתו, כי הארגון אינו גוף מונחה וכן מתקיימים לגביו אחד משני תנאים, כמפורט להלן.

התנאי הראשון, המנוי בפסקה (2)(א), הוא שקיימת התקשרות בתוקף בין הארגון לבין גוף הנמנה עם מערכת הביטחון, שמכוחה הארגון מספק למערכת הביטחון מוצרים, שירותים, ידע או טכנולוגיות שהם חיוניים לפעילות ביטחונית או מבצעית של הגוף האמור, ושפגיעה בזמינותם או תפקודם בשל תקיפת סייבר עלולה לגרום לפגיעה משמעותית בביטחון המדינה או ברציפות התפקוד של גוף הנמנה עם מערכת הביטחון.

התנאי השני, המנוי בפסקה (2)(ב), הוא שהייתה בעבר התקשרות בין הארגון לבין גוף הנמנה עם מערכת הביטחון, שטרם חלפו חמש שנים ממועד סיומה, ומכוחה הארגון מחזיק מידע על מוצרים, שירותים, ידע או טכנולוגיות כאמור בפסקה (2)(א), שמתקיים לגביהם האמור בסיפה של אותה פסקת משנה.

לסעיף קטן (ב)

מוצע לקבוע ששר הביטחון יוכל לקבוע שארגון ממגזר המנוי בתוספת הראשונה לחוק המוצע, הוא ארגון חיוני למערכת הביטחון, רק אם ניתנה לכך הסכמת הגורם המאסדר של המגזר שבו פועל הארגון, ואם מדובר בארגון חיוני –

(ב) שר הביטחון רשאי לקבוע כאמור בסעיף קטן (א) לגבי ארגון ממגזר המנוי בפסקה (1) להגדרה "מגזר" שבסעיף 1, אם ניתנה לכך הסכמת הגורם המאסדר של המגזר שבו פועל הארגון, ולעניין ארגון כאמור שהוא ארגון חיוני – גם אם מצא כי אין די בהגדרתו כארגון חיוני לצורך מתן מענה לסיכון האמור בסעיף קטן (א)(2)(א) סיפה או (ב) סיפה; לא השיב הגורם המאסדר לפניית שר הביטחון בעניין בתוך 30 ימים, יראו אותו כמי שהסכים לקביעת הארגון כארגון חיוני למערכת הביטחון.

(ג) המלצת ראש מלמ"ב כאמור בסעיף קטן (א) תינתן לאחר התייעצות עם ראש המטה הכללי של צה"ל ולאחר שקיבל את הסכמת ראש מערך הסייבר הלאומי; לא נתן ראש מערך הסייבר הלאומי את הסכמתו להמלצה, רשאי ראש מלמ"ב להביא את העניין לדיון לפני שר הביטחון וראש הממשלה שיכריעו במחלוקת.

(ד) קבע שר הביטחון לפי סעיף זה כי ארגון הוא ארגון חיוני למערכת הביטחון, יודיע על כך מלמ"ב לארגון, למערך הסייבר הלאומי, לצה"ל, ולעניין ארגון כאמור בסעיף קטן (ב) – גם לגורם המאסדר של המגזר שבו פועל הארגון, בתוך 14 ימים ממועד הקביעה; קביעת שר הביטחון תיכנס לתוקף במועד מסירת ההודעה על הקביעה לארגון, ותעמוד בתוקף עד המועד שלהלן לפי העניין, אלא אם כן קבע שר הביטחון קודם לכן, ביוזמתו או לפי בקשה מאת הארגון, שאותו ארגון לא ייחשב עוד לארגון חיוני למערכת הביטחון:

(1) לעניין ארגון שמתקיים לגביו האמור בסעיף קטן (א)(2)(א) – מועד סיום ההתקשרות של הארגון עם הגוף הנמנה עם מערכת הביטחון;

(2) לעניין ארגון שמתקיים לגביו האמור בסעיף קטן (א)(2)(ב) – תום 5 שנים ממועד סיום ההתקשרות של הארגון עם הגוף הנמנה עם מערכת הביטחון.

(ה) קבע שר הביטחון שארגון שנקבע כארגון חיוני למערכת הביטחון לפי סעיף זה לא ייחשב עוד לארגון כאמור, יודיע על כך מלמ"ב לגורמים האמורים בסעיף קטן (ד) רישה, במועד האמור בו, וקביעתו תיכנס לתוקף במועד מסירת ההודעה כאמור לארגון.

דברי הסבר

רק אם מצא שאין די בהגדרתו כארגון חיוני לצורך מענה לסיכון המתואר לעיל לפגיעה משמעותית בביטחון המדינה או ברציפות התפקוד של גוף הנמנה עם מערכת הביטחון. במקביל, מוצע לקבוע שאם הגורם המאסדר לא השיב לפניית שר הביטחון בעניין בתוך 30 ימים, יראו אותו כמי שהסכים לקביעת הארגון כארגון חיוני למערכת הביטחון.

לסעיף קטן (ג)

כדי להבטיח שהגדרת ארגון כארגון חיוני למערכת הביטחון תתבצע לאחר בחינת שיקולים רוחביים, מוצע לקבוע שהמלצת ראש מלמ"ב לפי סעיף קטן (א) המוצע, תינתן לאחר שקיים התייעצות עם ראש המטה הכללי של צה"ל ולאחר שקיבל את הסכמת ראש מערך הסייבר הלאומי.

כמו כן מוצע לקבוע כי אם ראש מערך הסייבר הלאומי לא הסכים לקביעת שר הביטחון, יוכל ראש מלמ"ב להביא את הסוגיה לדיון לפני שר הביטחון וראש הממשלה שיכריעו במחלוקת.

לסעיף קטן (ד)

מוצע לקבוע כי אם קבע שר הביטחון לפי סעיף מוצע זה, שארגון הוא ארגון חיוני למערכת הביטחון, הוא יודיע על כך למלמ"ב, לארגון, למערך הסייבר הלאומי, לצה"ל ולגורם המאסדר הנוגע לעניין, אם ישנו, בתוך 14 ימים ממועד הקביעה.

כמו כן, מוצע לקבוע כי קביעת שר הביטחון תיכנס לתוקף במועד מסירת ההודעה על הקביעה לארגון, ותעמוד בתוקף עד המועד שלהלן לפי העניין, אלא אם כן קבע שר הביטחון קודם לכן, ביוזמתו או לפי בקשת הארגון, שאותו ארגון לא ייחשב עוד לארגון חיוני למערכת הביטחון:

1. לעניין ארגון שקיימת התקשרות בתוקף בינו לבין גוף הנמנה עם מערכת הביטחון, כאמור בסעיף קטן (א)(2)(א) המוצע – עד מועד סיום ההתקשרות.

2. לעניין ארגון שהייתה בעבר התקשרות בינו לבין גוף הנמנה עם מערכת הביטחון כאמור בסעיף קטן (א)(2)(ב) המוצע – עד תום 5 שנים ממועד סיום ההתקשרות.

לסעיף קטן (ה)

על פי המוצע, אם קבע שר הביטחון שארגון שנקבע כארגון חיוני למערכת הביטחון לא ייחשב עוד לארגון כאמור, מלמ"ב יידרש להודיע על כך לארגון, למערך הסייבר הלאומי, לצה"ל ולגורם מאסדר נדרש לפי סעיף מוצע זה, אם ישנו, וקביעתו תיכנס לתוקף במועד מסירת ההודעה לארגון.

(ו) קבע שר הביטחון לפי סעיף זה שארגון הוא ארגון חיוני למערכת הביטחון, לא יראו ארגון כאמור לעניין חוק זה כארגון חיוני כמשמעותו בסעיף 8, כל עוד קביעת שר הביטחון עומדת בתוקף.

(ז) מספר הארגונים שייקבעו כארגון חיוני למערכת הביטחון לפי סעיף זה לא יעלה על המספר הקבוע בתוספת החמישית; שר הביטחון, בהסכמת ראש הממשלה, רשאי, בצו, על פי המלצה משותפת של ראש מערך הסייבר הלאומי וראש מלמ"ב, לתקן את התוספת החמישית.

(ח) רשימת הארגונים החיוניים למערכת הביטחון שנקבעו לפי סעיף זה לא תפורסם לציבור.

תחולת הוראות מהחוק לעניין ארגון חיוני למערכת הביטחון

21. (א) נקבע ארגון כארגון חיוני למערכת הביטחון לפי סעיף 20, יחולו לגביו הוראות פרק זה החלות לעניין ארגון חיוני למעט סעיף 16, וכן יחולו הוראות פרק ו' וסעיפים 46 ו־51, והכול בשינויים המחויבים, ובשינויים אלה:

(1) סמכות הנתונה לגורם מאסדר תהיה נתונה לשר הביטחון;

(2) סמכות הנתונה למנהל הרשות המוסמכת, למנהל בכיר ברשות מוסמכת ולעובד מוסמך מגזרי, תהיה נתונה לראש מלמ"ב, למנהל בכיר במלמ"ב ולעובד מוסמך במלמ"ב, בהתאמה;

(3) בסעיף 6(ב), במקום "עובדי הרשות" יקראו "עובדי מלמ"ב";

(4) בסעיף 7, במקום פסקה (1) יקראו:

"(1) הוא לא הורשע בעבירה שמפאת מהותה, חומרתה או נסיבותיה אין הוא ראוי, לדעת ראש מלמ"ב או מי שהוא הסמיכו לכך, לשמש עובד מוסמך במלמ"ב, לא הוגש נגדו כתב אישום בעבירה כאמור ולא מתנהלת לגביו חקירה בשל חשד לביצוע עבירה כאמור;";

דברי הסבר

לסעיף קטן (ו)

מוצע לקבוע שארגון שנקבע שהוא ארגון חיוני למערכת הביטחון, לא ייחשב לארגון חיוני כמשמעותו בסעיף 8 לחוק המוצע, כל עוד קביעה זו עומדת בתוקפה.

לסעיף קטן (ז)

במקביל לעיגון שיטת קביעת הארגונים החיוניים למערכת הביטחון לפי ההסדר המוצע לעיל, ובהתאם לתפיסה שבבסיס החוק המוצע והרצון לשמר את המודל המבוזר, כמו גם בהתאם לעמדות המקצועיות באשר להיקף הארגונים המרבי הנדרש בהקשר זה, מוצע לקבוע כי מספר הארגונים שיהיה ניתן לקבוע כארגונים חיוניים למערכת הביטחון לפי החוק לא יעלה על המספר הקבוע בתוספת החמישית, לצד מתן סמכות לשר הביטחון, בהסכמת ראש הממשלה, לשנות את התוספת בצו, על פי המלצה משותפת של ראש מערך הסייבר הלאומי וראש מלמ"ב, אם ימצאו כי הדבר נדרש.

לסעיף קטן (ח)

מוצע לקבוע שרשימת הארגונים החיוניים למערכת הביטחון לא תפורסם לציבור.

סעיף 21 לסעיף קטן (א)

בהמשך להסדר המוצע לעניין קביעת ארגון כארגון חיוני למערכת הביטחון, מוצע לקבוע שאם נקבע ארגון כחיוני למערכת הביטחון, יחולו לגביו הוראות פרק מוצע זה החלות לעניין ארגון חיוני, בשינויים המחויבים, למעט סעיף 16 לחוק המוצע, שעניינו סמכות מתן ההוראות של מערך הסייבר הלאומי (באמצעות מנהל בכיר במערך ועובד מוסמך במערך) בתקיפת סייבר חמורה, וכן יחולו הוראות פרק ו' לחוק המוצע, אשר מקנה לעובדים מוסמכים מגזריים סמכויות לפיקוח על ביצוע ההוראות לפי החוק המוצע, והוראות סעיפים 46 ו־51 לחוק המוצע, שעניינן בשמירת סודיות ובהסתייעות במומחה חיצוני, והכול בשינויים המחויבים ובשינויים המנויים בסעיף קטן (א).

כך, על פי המוצע, סמכות הנתונה באותן הוראות לגורם מאסדר תהיה נתונה לשר הביטחון, וסמכות הנתונה בהן למנהל הרשות המוסמכת, למנהל בכיר ברשות מוסמכת או לעובד מוסמך מגזרי, תהיה נתונה לראש מלמ"ב, למנהל בכיר במלמ"ב ולעובד מוסמך במלמ"ב, בהתאמה. כמו כן, עובדים מוסמכים במלמ"ב יוסמכו, לפי סעיף 6 לחוק המוצע כפי שהוחל כאמור, מקרב עובדי מלמ"ב, ובדיקת העבר

(5) בסעיף 9(ב)(1), במקום הסיפה החל במילים "בתקן אחד" יקראו "במסמך תאימות "רב מגן", העומד לעיון הארגונים החיוניים למערכת הביטחון במשרדי מלמ"ב, בהתאמות המתחייבות";

(6) הסמכות הנתונה לראש מערך הסייבר הלאומי ולמנהל בכיר במערך לפי סעיף 11, תהיה נתונה גם לראש מלמ"ב ולמנהל בכיר במלמ"ב, בהתאמה; מצא ראש מלמ"ב, לפי סעיף 11(א) כפי שהוחל כאמור, כי מתקיים סיכון סייבר שיש בו כדי לאפשר תקיפת סייבר חמורה כהגדרתה בסעיף 13 נגד ארגונים שונים שהם ארגונים חיוניים למערכת הביטחון, או באמצעותם, אם לא יינקטו בדחיפות אמצעים להתמודדות עימו, רשאי הוא, באישור שר הביטחון, להורות בכתב לארגון חיוני למערכת הביטחון שביחס אליו עלול להתממש הסיכון, לנקוט אמצעים כאמור במועד שעליו יורה, ויחולו הוראות סעיף 11(ב), (ד) ו־(ה), בשינויים המחויבים ובשינויים אלה:

(א) בסעיף קטן (ב), במקום "הרשות המוסמכת הנוגעת לעניין" יקראו "המערך";

(ב) בסעיף קטן (ד)(3), במקום "ברשות המוסמכת" יקראו "במערך" ובמקום "לרשות המוסמכת" יקראו "למערך".

(ב) ההוראות לפי סעיף 9(ב) ו־(ג), כפי שהוחלו בסעיף קטן (א), יחולו לגבי ארגון חיוני למערכת הביטחון החל מתום 6 חודשים ממועד הכניסה לתוקף של קביעתו כארגון כאמור, כאמור בסעיף 20(ה).

(ג) בסעיף זה –

"מנהל בכיר במלמ"ב" – ראש יחידת הסייבר במלמ"ב;

"עובד מוסמך במלמ"ב" – עובד המלמ"ב שראש המלמ"ב הסמיכו לפי סעיף 6(ב) כפי שהוחל בסעיף קטן (א)(3).

דברי הסבר

הפלילי הנדרשת לשם הסמכה כעובד מוסמך במלמ"ב, לפי סעיף 7 לחוק המוצע כפי שהוחל כאמור, תהיה בסמכות ראש מלמ"ב.

כדי לעמוד ברמת הגנת הסייבר הנדרשת מארגונים חיוניים לפי סעיף 9(ב)(1) לחוק המוצע, כפי שהוחל כאמור, יידרש ארגון חיוני למערכת הביטחון לעמוד בדרישות המפורטות בחלק א' לתוספת הרביעית לחוק המוצע, באמצעות יישום ההוראות הנוגעות לאותן דרישות ב"מסמך תאימות רב מגן", שיועמד לעיון הארגונים החיוניים למערכת הביטחון במשרדי מלמ"ב, ולא באחד מהתקנים המנויים בחלק ב' לתוספת הרביעית.

הסמכות הנתונה לראש המערך ולמנהל בכיר במערך לפי סעיף 11 לחוק המוצע, קרי הסמכות לתת הוראות דחופות למניעת סיכון סייבר משמעותי בארגון חיוני ולפעול בהקשר זה, תהיה נתונה גם לראש מלמ"ב ולמנהל בכיר במלמ"ב בהתאמה. ומוצע לקבוע כי אם מצא ראש מלמ"ב לפי סעיף 11(א) לחוק המוצע, כפי שהוחל כאמור, כי מתקיים סיכון סייבר שיש בו כדי לאפשר תקיפת סייבר חמורה כהגדרתה בסעיף 13 לחוק המוצע נגד ארגונים שונים שהם ארגונים חיוניים למערכת הביטחון או באמצעותם, אם לא יינקטו בדחיפות אמצעים להתמודדות עימו, הוא יהיה מוסמך, באישור שר הביטחון, להורות בכתב לארגון חיוני למערכת הביטחון שביחס אליו עלול להתממש הסיכון, לנקוט אמצעים כאמור במועד שעליו יורה, ויחולו הוראות סעיף 11(ב), (ד) ו־(ה) לחוק המוצע, בשינויים המחויבים ובשינויים המנויים בפסקה (4), ועיקרם שההתייעצות לפני מתן ההוראה, כאמור בסעיף 11(ב) האמור, תהיה עם המערך (ולא עם הרשות המוסמכת) וההתייעצות לפני מתן ההחלטה בהשגה, כאמור בסעיף 11(ד)(3) לחוק המוצע, תהיה עם מנהל בכיר במערך.

לסעיף קטן (ב)

מוצע כי ההוראות לפי סעיף 9(ב) ו־(ג) לחוק המוצע, כפי שהוחלו בסעיף קטן (א) לסעיף המוצע, יחולו לגבי ארגון חיוני למערכת הביטחון החל מתום 6 חודשים ממועד הכניסה לתוקף של קביעתו כארגון כאמור, כאמור בסעיף 20(ה) לחוק המוצע, וזאת כדי לאפשר לארגונים תקופת היערכות בנסיבות העניין.

מובהר כי בהתאם למוצע לא יחולו שינויים נוספים, ובכלל האמור תחול חובת הדיווח על תקיפה משמעותית גם למערך הסייבר הלאומי, כמו גם חובת התייעצות עם המערך בהתאם לסעיפי החוק השונים. עוד מובהר, למען הסר ספק, כי על פי המוצע לא יחולו לעניין מלמ"ב הוראות סעיף 5 לחוק המוצע, ובהתאם לכך, לא תוקם במלמ"ב יחידה מגזרית.

סימן ה': הוראות מיוחדות לעניין משרדי ממשלה מסוימים

הוראות מיוחדות לעניין משרד ראש הממשלה ומשרד החוץ

22. (א) הוראות פרק זה החלות לעניין ארגון חיוני, למעט סעיף 16, יחולו לעניין משרד ראש הממשלה ומשרד החוץ, למעט יחידות הסמך שלהם, וכן יחולו הוראות פרק ו' וסעיפים 46 ו־51, והכול בשינויים המחויבים ובשינויים אלה:

(1) סמכות הנתונה לגורם מאסדר תהיה נתונה לראש הממשלה;

(2) סמכות הנתונה למנהל הרשות המוסמכת, למנהל בכיר ברשות מוסמכת, ולעובד מוסמך מגזרי, תהיה נתונה לראש השירות או למנהל בכיר בשירות, לעובד השירות בדרגת ראש מחלקה שראש השירות הסמיכו לכך, ולעובד מוסמך בשירות, בהתאמה;

(3) בסעיף 6(ב), במקום "עובדי הרשות" יקראו "עובדי שירות הביטחון הכללי";

(4) בסעיף 7, פסקה (1) – לא תיקרא.

(ב) בסעיף זה, "עובד מוסמך בשירות" – עובד שירות הביטחון הכללי שראש השירות או מנהל בכיר בשירות הסמיכו לפי סעיף 6(ב) כפי שהוחל בסעיף קטן (א)(2).

פרק ו': סמכויות פיקוח

דרישת ידיעות ומסמכים

23. לשם פיקוח על ביצוע ההוראות לפי חוק זה, רשאי עובד מוסמך מגזרי לדרוש מכל אדם הנוגע בדבר למסור או להציג לו כל ידיעה או מסמך לרבות עותק מחומר מחשב, שיש בהם כדי להבטיח את ביצוען של ההוראות לפי חוק זה.

דברי הסבר

סימן ה': הוראות מיוחדות לעניין משרדי ממשלה מסוימים

סעיף 22 לסעיף קטן (א)

כאמור לעיל, מוצע לקבוע את משרדי הממשלה כארגונים חיוניים לפי החוק המוצע. במקביל, לנוכח רגישות המערכות והמידע של משרד החוץ ומשרד ראש הממשלה (בלא יחידות הסמך שלהם), המונחים כבר כיום בתחומי הגנת סייבר שונים בידי השירות, מוצע לקבוע שהרשות המוסמכת לגביהם לעניין החוק המוצע תהיה השירות, ובהתאם יחולו הוראות פרק ה' המוצע החלות לעניין ארגון חיוני, למעט סעיף 16 לחוק המוצע שעניינו סמכות מתן ההוראות של מערך הסייבר הלאומי בתקיפה חמורה, וכן יחולו הוראות פרק ו' וסעיפים 46 ו־51 לחוק המוצע לעניין שמירת סודיות, הגבלת שימוש ומחיקה והסתייעות במומחה חיצוני, והכול בשינויים המחויבים ובשינויים המפורטים בסעיף קטן (א) לסעיף המוצע.

כך, על פי המוצע, סמכות הנתונה לגורם מאסדר לפי ההוראות הנזכרות לעיל תהיה נתונה לראש הממשלה; סמכות הנתונה בהן למנהל הרשות המוסמכת, למנהל בכיר ברשות מוסמכת, ולעובד מוסמך מגזרי, תהיה נתונה לראש השירות או למנהל בכיר בשירות, לעובד השירות בדרגת ראש מחלקה בשירות שראש השירות הסמיכו לכך, ולעובד מוסמך בשירות, בהתאמה.

כמו כן, עובדים מוסמכים בשירות יוסמכו, לפי סעיף 6 לחוק המוצע כפי שהוחל כאמור, מקרב עובדי השירות, ואולם קבלת אישור המשטרה (פסקה (1) של סעיף 7 לחוק המוצע) לא תהיה תנאי להסמכה מאחר שהדבר אינו נדרש לגבי עובדי השירות.

מובהר כי בהתאם למוצע, ההוראות הנזכרות לעיל יחולו לעניין משרד החוץ ומשרד ראש הממשלה בלי שינויים נוספים על אלה שנזכרו לעיל, כך שתחול חובה לדווח על תקיפת סייבר משמעותית (לפי סעיף 12 לחוק המוצע) גם למערך הסייבר הלאומי, כמו גם חובת התייעצות עם המערך בהתאם לסעיפי החוק השונים. עוד מובהר, למען הסר ספק, כי בהתאם למוצע לא תוקם בשירות הביטחון הכללי יחידה מגזרית.

פרק ו': סמכויות פיקוח

סעיף 23 כפי שמקובל ביחס לסמכויות פיקוח במשפט הישראלי, מוצע לקבוע כי לשם פיקוח על ביצוע ההוראות לפי החוק המוצע, רשאי עובד מוסמך מגזרי לדרוש מכל אדם הנוגע בדבר למסור או להציג לו כל ידיעה או מסמך, לרבות עותק מחומר מחשב, שיש בהם כדי להבטיח את ביצוען של ההוראות לפי החוק המוצע. זאת לרבות לשם פיקוח על עמידת ארגון חיוני במגזר ברמת ההגנה הנדרשת לפי סעיף 9 לחוק המוצע, לשם פיקוח על עמידת ארגון חיוני בחובת הדיווח על תקיפות סייבר משמעותית נגד ארגון חיוני לפי סעיף 12 לחוק המוצע, או לשם בחינה אם ארגון הוא ארגון חיוני באותו המגזר לפי סעיף 8 המוצע. מעבר לכך, יצוין כי סמכות זו, ככל סמכות, תופעל בהתאם לכללי המשפט המינהלי באופן המידתי הנדרש.

כניסה למקום

24. לשם פיקוח על ביצוע ההוראות לפי סעיפים 9(ב) עד (ה) ו־12, רשאי עובד מוסמך מגזרי להיכנס למקום, ובלבד שלא ייכנס למקום המשמש למגורים, אלא על פי צו של בית משפט.

זיהוי עובד מוסמך מגזרי

25. (א) עובד מוסמך מגזרי לא יעשה שימוש בסמכויות הנתונות לו לפי פרק זה, אלא בעת מילוי תפקידו, ובלבד שיש בידו תעודה החתומה בידי מנהל הרשות המוסמכת, המעידה על תפקידו ועל סמכויותיו של עובד מוסמך מגזרי, שאותה יציג על פי דרישה.

(ב) חובת ההזדהות לפי סעיף קטן (ב) לא תחול אם קיומה עלול לגרום לאחד מאלה:

(1) סיכול ביצוע הסמכות בידי העובד המוסמך המגזרי;

(2) פגיעה בביטחון העובד המוסמך המגזרי או בביטחון אדם אחר.

(ג) חלפה הנסיבה שבשלה לא קיים עובד מוסמך מגזרי את חובת ההזדהות, כאמור בסעיף קטן (ב), יקיים העובד המוסמך את חובתו כאמור, מוקדם ככל האפשר.

פרק ז': אמצעי אכיפה מינהליים

סימן א': הגדרות

פרק ז' – הגדרות

26. בפרק זה –

"ארגון חיוני" – אחד מאלה:

(1) ארגון כאמור בסעיף 8(א)(2) או (3) שאינו ארגון הנמנה עם מגזר המנוי בפרט 7 לתוספת הראשונה;

(2) ארגון חיוני למערכת הביטחון;

דברי הסבר

סעיף 24 מוצע לקבוע כי לשם פיקוח על ביצוע ההוראות לפי סעיפים 9(ב) עד (ה) ו־12 לחוק המוצע, רשאי עובד מוסמך מגזרי להיכנס למקום, ובלבד שלא ייכנס למקום המשמש למגורים אלא על פי צו של בית משפט. כמו כן, יודגש, כי סמכות הכניסה למקום של העובד המוסמך המגזרי אינה כוללת סמכות לבצע פעולות בחומר מחשב.

סעיף 25 לסעיף קטן (א)

כדי להבטיח שימוש מידתי בסמכות, מוצע לקבוע שעובד מוסמך מגזרי לא יעשה שימוש בסמכויות הנתונות לו לפי סימן מוצע זה, אלא בעת מילוי תפקידו ובלבד שיש בידו תעודה החתומה בידי מנהל הרשות המוסמכת המעידה על תפקידו וסמכויותיו של העובד המוסמך המגזרי, שאותה יציג לפי דרישה.

לסעיף קטן (ב)

על אף האמור בסעיף קטן (א) המוצע, מוצע לקבוע שחובת ההזדהות האמורה לא תחול אם קיומה עלול לגרום לסיכול הכניסה למקום על ידי העובד המוסמך המגזרי או אם קיומה עלול לפגוע בביטחון העובד המוסמך המגזרי או בביטחון אדם אחר.

לסעיף קטן (ג)

מוצע לקבוע שעם חלוף הנסיבה האמורה בסעיף קטן (ב) המוצע, שבשלה לא קיים העובד המוסמך המגזרי את חובת ההזדהות, יזדהה העובד המוסמך בהתאם למפורט בסעיף, מוקדם ככל האפשר.

פרק ז': אמצעי אכיפה מינהליים

סימן א': הגדרות

הפרת הוראות החוק על ידי ארגונים חיוניים, ארגונים חיוניים למערכת הביטחון וספקי שירותים דיגיטליים ושירותי אחסון עלולה להביא לפגיעה באינטרסים ציבוריים, דוגמת ביטחון המדינה, ביטחון הציבור ולפגיעה חמורה ברציפות אספקת שירותים חיוניים לציבור. לכן מוצע, בפרק מוצע זה, לקבוע את סמכות הרשויות המוסמכות להטיל עיצומים כלפי ארגון בעקבות הפרה של חובות מרכזיות בחוק.

יובהר כי תכליתה של הסנקציה המינהלית היא הרתעתית־מניעתית. כמו כן היא מניחה כי ביצוע הפרות של עבירות הסדר נעשה לעיתים מתוך שיקולים תועלתניים של המפר, שסבור, למשל, שאי־קיום ההוראה עשוי לחסוך לו הוצאות. מסיבה זו, גובה הסכום של העיצום הכספי נועד למנוע את התמריץ הכלכלי להפר את החוק, קרי לנטרל את קיומה של "ההפרה היעילה". עם זאת, גובה הסכום של העיצום הכספי צריך להיות מידתי ולא לסכן את המשך פעילותו הכלכלית של המפר.

סעיף 26 מוצע כי "ארגון חיוני" יוגדר לעניין פרק זה כארגון חיוני כמשמעותו לפי הוראות סעיף 8(א)(2) או (3) לחוק המוצע, למעט רשויות מקומיות, או כארגון חיוני למערכת הביטחון. יודגש כי בפרק זה הגדרת "ארגון חיוני" לא כוללת גופים ממשלתיים כאמור בסעיף 8(א)(1) לחוק המוצע או כאמור בסעיף 22 לאותו חוק.

"הממונה" – אחד מאלה, לפי העניין:

(1) לעניין ארגון חיוני כאמור בפסקה (1) להגדרה "ארגון חיוני" – עובד בכיר ברשות מוסמכת כאמור בפסקה (1) להגדרה "הרשות המוסמכת" בסעיף 1, שדרגתו ראש אגף לפחות, שמנהל הרשות המוסמכת הסמיכו להטיל עיצום כספי לפי פרק זה;

(2) לעניין ארגון חיוני כאמור בפסקה (2) להגדרה "ארגון חיוני" – מנהל בכיר במלמ"ב כהגדרתו בסעיף 21(ג).

סימן ב': עיצום כספי

עיצום כספי

27. (א) ארגון חיוני שלא קיים דרישה מהדרישות המפורטות בחלק א' לתוספת הרביעית, המנויה בטור א' בחלק א' לתוספת השישית, באמצעות יישום ההוראות הנוגעות לאותה דרישה בתקן שבחר מהתקנים המנויים בחלק ב' לתוספת הרביעית, בניגוד להוראות סעיף 9(ב)(1), ולעניין ארגון חיוני כאמור בפסקה (2) להגדרה "ארגון חיוני" – בניגוד לאותן הוראות כפי שהוחלו בסעיף 21(א)(5), רשאי הממונה להטיל עליו עיצום כספי לפי הוראות פרק זה, בסכום הקבוע בטור ב' בחלק א' לתוספת השישית לצד אותה דרישה.

(ב) ארגון חיוני שלא קיים דרישה שהגורם המאסדר האמון על אסדרת תחום הגנת הסייבר במגזר שבו הוא פועל, קבע בתקנות לפי סעיף 9(ג), המנויה בטור א' בחלק ב' לתוספת השישית לעניין אותו מגזר, רשאי הממונה להטיל עליו עיצום כספי לפי הוראות פרק זה, בסכום הקבוע בטור ב' בחלק ב' לתוספת השישית לצד אותה דרישה.

(ג) הפר ארגון חיוני הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בסכום של 640,000 שקלים חדשים:

(1) לא מילא הוראה שנתן לו ראש מערך הסייבר הלאומי לפי סעיף 11;

דברי הסבר

כמו כן, מוצע להגדיר את "הממונה", כעובד בכיר ברשות מוסמכת הרלוונטית אשר דרגתו ראש אגף לפחות ושהוסמך על ידי מנהל הרשות המוסמכת להטיל עיצומים לפי פרק זה, ולעניין ארגון חיוני למערכת הביטחון – מנהל בכיר במלמ"ב כהגדרתו בסעיף 21(ג) לחוק המוצע. יובהר כי ניתן שהממונה יהיה אותו גורם שכבר מוסמך להטיל עיצומים ברשות המוסמכת מכוח דינים אחרים, אם יש כזה.

סימן ב': עיצום כספי

סעיף 27 ותוספת שישית לסעיף קטן (א)

מוצע להסמיך את הממונה להטיל עיצום כספי על ארגון חיוני כהגדרתו בפרק מוצע זה, אם לא קיים דרישה מהדרישות המנויות בחלק א' לתוספת הרביעית המוצעת ואשר מנויה בטור א' בחלק א' לתוספת השישית המוצעת, באמצעות יישום ההוראות הנוגעות לאותה דרישה בתקן שבחר מהתקנים המנויים בחלק ב' לתוספת הרביעית המוצעת, בניגוד להוראות סעיף 9(ב)(1), ולעניין ארגון חיוני למערכת הביטחון – בניגוד לאותן הוראות כפי שהוחלו בסעיף 21(א)(5), שלפיהן התקן שלפיו תיבחן העמידה בדרישות הוא מסמך תאימות "רב מגן". ביחס לכל דרישה שהופרה כאמור, מוצע כי יהיה ניתן להטיל עיצום כספי בסכום הקבוע בטור ב' בחלק א' לתוספת השישית המוצעת לצד אותה דרישה.

לסעיף קטן (ב)

כמו כן מוצע להסמיך את הממונה להטיל עיצום כספי על ארגון חיוני שלא קיים דרישה שהגורם המאסדר קבע בתקנות לפי סעיף 9(ג) לחוק המוצע, המנויה בטור א' בחלק ב' לתוספת השישית המוצעת לעניין המגזר שהוא אמון בו על אסדרת תחום הגנת הסייבר, בסכום הקבוע בטור ב' בחלק ב' לתוספת השישית המוצעת לצד אותה דרישה, זאת אם תתווסף דרישה כזו לתוספת האמורה לפי סעיף 45 לחוק המוצע.

לסעיף קטן (ג)

מוצע להסמיך את הממונה להטיל על ארגון חיוני עיצום בסך 640,000 שקלים חדשים בגין הפרת הוראה שנתן ראש מערך הסייבר הלאומי לפי סעיף 11 לחוק המוצע, או בשל הפרת חובת הדיווח על תקיפת סייבר משמעותית שחלה על ארגון חיוני לפי סעיף 12 לחוק המוצע, ובכלל זה בשל כך שהארגון לא כלל בדיווח האמור את העניינים המפורטים באותו סעיף מוצע. כמו כן, מוצע להסמיך את הממונה להטיל עיצום באותו סכום בשל הפרת החובה למסור לעובד מוסמך מגזרי, מידע או מסמך שהיה על הארגון החיוני לשמור בהתאם להוראות סעיפים 9(ה) או 11(ה) לחוק המוצע, לפי דרישה שנמסרה לארגון בכתב, במועד או באופן שנקבעו בדרישה, וזאת בניגוד להוראות לפי סעיף 23 לחוק המוצע.

(2) לא דיווח על תקיפת סייבר משמעותית כאמור בסעיף 12, או דיווח על תקיפה כאמור שלא בהתאם להוראות סעיף 12(ב);

(3) לא מסר לעובד מוסמך מגזרי, מידע או מסמך שהיה עליו לשמור בהתאם להוראות סעיפים 9(ה) או 11(ה), לפי דרישה שנמסרה לו בכתב, במועד או באופן שנקבעו בדרישה, בניגוד להוראות לפי סעיף 23.

(ד) ארגון חיוני או ספק שירותים דיגיטליים ושירותי אחסון (להלן בפרק זה – ארגון), שלא מילא הוראה לביצוע פעולות להגנת סייבר בחומר מחשב או הוראה למסירת ידיעה או מסמך, שניתנה לו בכתב, לפי סעיפים 14(ג)(4) או 16, רשאי הממונה להטיל עליו עיצום כספי בסכום של 640,000 שקלים חדשים.

(ה) לא יטיל הממונה ברשות מוסמכת עיצום כספי לפי חוק זה, בשל מעשה המהווה הפרה לפי חוק אחר, שיש לרשות המוסמכת סמכות להטיל בשלו עיצום כספי.

הודעה על כוונת חיוב

28. (א) היה לממונה יסוד סביר להניח כי ארגון הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 27 (בפרק זה – המפר), ובכוונתו להטיל עליו עיצום כספי לפי אותו סעיף, ימסור לו הודעה על הכוונה להטיל עליו עיצום כספי (בפרק זה – הודעה על כוונת חיוב).

(ב) בהודעה על כוונת חיוב יציין הממונה, בין השאר, את אלה:

(1) המעשה או המחדל (בפרק זה – המעשה) המהווה את ההפרה ומועד ביצוע ההפרה;

(2) סכום העיצום הכספי והתקופה לתשלומו;

(3) זכותו של המפר לטעון את טענותיו לפני הממונה לפי הוראות סעיף 29, וכי יראו את ההודעה על כוונת חיוב כדרישת תשלום אם המפר לא יממש את הזכות האמורה, כאמור בסעיף 30(ד);

(4) הסמכות להוסיף על סכום העיצום הכספי בשל הפרה נמשכת או הפרה חוזרת לפי הוראות סעיף 27, ושיעור התוספת.

דברי הסבר

לסעיף קטן (ד)

מוצע להסמיך את הממונה להטיל עיצום כספי בסך 640,000 שקלים חדשים על ארגון חיוני כהגדרתו בפרק מוצע זה או על ספק שירותים דיגיטליים ושירותי אחסון גם אם אינו ארגון חיוני כאמור, בגין אי־מילוי הוראה לביצוע פעולה להגנת סייבר בחומר מחשב או הוראה למסירת ידיעה או מסמך, שניתנה לו בכתב לפי סעיפים 14(ג)(4) או 16 לחוק המוצע. מוצע שעיצום בגין הפרת הוראה כאמור יוכל להיות מוטל על כל ארגון במגזר השירותים הדיגיטליים ושירותי האחסון ולא רק על ארגונים חיוניים במגזר זה, מאחר שהסמכות למתן הוראות להתמודדות עם תקיפות סייבר חמורות חלה כלפי כלל הארגונים במגזר האמור בשל מאפייניו הייחודיים, בדגש על החיבוריות הגבוהה של ארגונים בו לארגונים רבים במשק.

לסעיף קטן (ה)

לחלק מהרשויות המוסמכות מוקנית סמכות להטיל עיצומים על ארגונים על הפרות לפי החוק המוצע, בשל מעשים המהווים הפרה גם מכוח חקיקה אחרת במסגרת האסדרה שמתבצעת על ידם. כדי לייצר ודאות למשק ולמנוע כפל ענישה, מוצע לקבוע שהממונה לא יטיל עיצום כספי לפי החוק המוצע, בשל מעשה המהווה הפרה לפי חוק אחר, שיש לרשות המוסמכת [סמכות להטיל בשלו עיצום כספי.

סעיפים 28 עד 30 בסעיפים אלה מוצע לקבוע את אופן הפעלת הסמכות להטיל עיצום כספי. ההוראות המוצעות הן ההוראות המקובלות בהסדרי החקיקה השונים הכוללים סמכות זו. הוראות מפורטות אלה נועדו להבטיח הגנה על זכויות בסיסיות של ארגון במסגרת הליך מינהלי ראוי, הפעלה שוויונית של הסמכות ביחס לארגונים שונים ושקיפות של פעולת הממונה.

בסעיף 28 מוצע לעגן את השלב הראשון בהפעלת הסמכות כלפי ארגון לפי סעיף 27 המוצע. מוצע כי כאשר יש לממונה יסוד סביר להניח כי ארגון הפר את הוראות החוק וקיימת כוונה להטיל עיצום כספי, תישלח הודעה על כוונת חיוב על ידי הממונה. מטרת הודעה זו להבהיר לארגון מה המעשה או המחדל המהווה את ההפרה, מועד ביצועה, מה סכום העיצום הכספי שצפוי להיות מוטל על המפר בשל ביצוע ההפרה האמורה ומה התקופה שבה נדרש לשלם. כמו כן מוצע שבהודעה תצוין זכותו של המפר לטעון את טענותיו לפני הממונה.

בסעיף 29, מוצע לעגן את זכות הטיעון של הארגון לפני הממונה, כמקובל בהליך מינהלי. מוצע שמפר שנמסרה לו הודעה על כוונת חיוב כאמור, יהיה רשאי לטעון את טענותיו בכתב לפני הממונה, הן לעניין הכוונה

זכות טיעון

29. מפר שנמסרה לו הודעה על כוונת חיוב לפי הוראות סעיף 28, רשאי לטעון את טענותיו, בכתב, לפני הממונה, לעניין הכוונה להטיל עליו עיצום כספי ולעניין סכומו, בתוך 30 ימים ממועד מסירת ההודעה, ורשאי הממונה להאריך את התקופה האמורה בתקופה נוספת מטעמים מיוחדים שיירשמו.

החלטת הממונה ודרישת תשלום

30. (א) הממונה יחליט, לאחר ששקל את הטענות שנטענו לפי סעיף 29, אם להטיל על המפר עיצום כספי, ורשאי הוא להפחית את סכום העיצום הכספי לפי הוראות סעיף 32.

(ב) החליט הממונה לפי הוראות סעיף קטן (א) –

(1) להטיל על המפר עיצום כספי – ימסור לו דרישה בכתב לשלם את העיצום הכספי (בפרק זה – דרישת תשלום), ובה יציין, בין השאר, את סכום העיצום הכספי המעודכן ואת התקופה לתשלומו;

(2) שלא להטיל על הארגון עיצום כספי – ימסור לו הודעה על כך בכתב.

(ג) בדרישת התשלום או בהודעה, לפי סעיף קטן (ב), יפרט הממונה את נימוקי החלטתו.

(ד) לא טען המפר את טענותיו לפי הוראות סעיף 29, בתוך התקופה האמורה באותו סעיף, יראו את ההודעה על כוונת החיוב, בתום אותה תקופה, כדרישת תשלום שנמסרה למפר במועד האמור.

הפרה נמשכת והפרה חוזרת

31. (א) בהפרה נמשכת יתווסף על העיצום הכספי הקבוע לאותה הפרה החלק ה־100 שלו לכל יום שבו נמשכת ההפרה לאחר קבלת הודעה, דרישת תשלום או התראה מינהלית.

(ב) בהפרה חוזרת יתווסף על העיצום הכספי הקבוע לאותה הפרה, סכום השווה לעיצום הכספי כאמור; לעניין זה, "הפרה חוזרת" – הפרת הוראה מהוראות חוק זה, כאמור בסעיף 23, בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על הארגון עיצום כספי או שבשלה הורשע.

סכומים מופחתים

32. (א) הממונה אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים לפי סימן זה, אלא לפי הוראות סעיף קטן (ב).

דברי הסבר

להטיל עליו עיצום כספי והן לגבי סכומו, בתוך 30 ימים מיום שנמסרה לו ההודעה, וכן מוצע שהממונה רשאי יהיה להאריך את התקופה האמורה בתקופה נוספת מטעמים מיוחדים שיירשמו.

בסעיף 30 מוצע לקבוע כי רק לאחר ששקל הממונה את טענות הארגון לפי סעיף 29 המוצע, יחליט אם יש להטיל עיצום כספי ומה גובהו. החליט הממונה להטיל עיצום כספי, ישלח לארגון דרישת תשלום בכתב ובה יציין את סכום העיצום הכספי המעודכן ואת התקופה שבה נדרש לשלמו. החליט הממונה שלא להטיל עיצום כספי, ימסור הודעה על כך לארגון, בכתב.

עוד מוצע בסעיף 30(ד) המוצע, לקבוע שאם ארגון בחר שלא לטעון את טענותיו, בחלוף 30 ימים ממסירת ההודעה הראשונית, יראו בה דרישת תשלום, ויהיה על המפר לשלם את סכום העיצום הכספי המצוין בה.

סעיף 31 לסעיף קטן (א)

חלק מההפרות של החובות הקבועות בחוק מוצע זה הן הפרות נמשכות לפי טבען. לכן, מוצע לקבוע בסעיף קטן (א) שכאשר הפרה היא הפרה נמשכת, יהיה רשאי הממונה להוסיף על העיצום הכספי הקבוע לאותה הפרה, את החלק ה־100 שלו כנגד כל יום שבו נמשכת ההפרה.

לסעיף קטן (ב)

עניינו של סעיף קטן מוצע זה הוא בהפרה חוזרת – הפרת הוראה מהוראות החוק בתוך שנתיים מההפרה הקודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע. ביחס להפרה חוזרת, מוצע לקבוע כי יוטל על המפר כפל העיצום הכספי. העיצום המוטל בשל הפרה חוזרת מבטא את הסלמת האמצעי הננקט ביחס למפר חוזר.

סעיף 32 מוצע להתוות את שיקול הדעת של הממונה בהטלת עיצום כספי ולקבוע שגורם מאסדר, בהתייעצות עם ראש מערך הסייבר הלאומי ובהסכמת שר המשפטים, יהיה רשאי לקבוע בתקנות מקרים, נסיבות ושיקולים שבשלהם יהיה ניתן להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים לפי סימן מוצע זה, ובשיעורים שיקבע (להלן – תקנות ההפחתה).

(ב) גורם מאסדר, בהתייעצות עם ראש מערך הסייבר הלאומי ובהסכמת שר המשפטים, רשאי לקבוע מקרים, נסיבות ושיקולים שבשלהם יהיה ניתן להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים לפי סימן זה, ובשיעורים שיקבע.

סכום מעודכן של העיצום הכספי

33. (א) העיצום הכספי יהיה לפי סכומו המעודכן ביום מסירת דרישת התשלום, ולגבי מפר שלא טען את טענותיו לפני הממונה כאמור בסעיף 30(ד) – ביום מסירת ההודעה על כוונת חיוב; הוגשה עתירה לבית המשפט לעניינים מינהליים או הוגש ערעור על פסק דין בעתירה כאמור, ועוכב תשלומו של העיצום הכספי בידי הממונה או בידי בית המשפט – יהיה העיצום הכספי לפי סכומו המעודכן ביום ההחלטה בעתירה או בערעור, לפי העניין.

(ב) סכום העיצום הכספי לפי פרק זה יתעדכן ב־1 בינואר בכל שנה (בסעיף קטן זה – יום העדכון), בהתאם לשיעור שינוי המדד הידוע ביום העדכון לעומת המדד שהיה ידוע ב־1 בינואר של השנה הקודמת; הסכום האמור יעוגל לסכום הקרוב שהוא מכפלה של 10 שקלים חדשים; לעניין זה, "מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה.

(ג) הממונה יפרסם ברשומות הודעה על סכום העיצום הכספי לפי סעיף קטן (ב).

המועד לתשלום העיצום הכספי

34. על המפר לשלם את העיצום הכספי בתוך 30 ימים מיום מסירת דרישת התשלום כאמור בסעיף 30.

ריבית שקלית ודמי פיגורים

35. לא שילם המפר עיצום כספי במועד, ייווספו על העיצום הכספי, לתקופת הפיגור, ריבית שקלית ודמי פיגורים לפי חוק פסיקת ריבית והצמדה, התשכ"א–1961[9] (בפרק זה – חוק פסיקת ריבית והצמדה).

פריסת תשלום העיצום הכספי

36. (א) הממונה רשאי, לבקשת המפר, להחליט על פריסת התשלום של העיצום הכספי, בהתחשב בסכום העיצום הכספי שהוטל על המפר ובנסיבות מיוחדות אחרות המצדיקות פריסה כאמור, ובלבד שמספר התשלומים לא יעלה על 12 תשלומים חודשיים.

(ב) החליט המנהל על פריסת התשלום לפי סעיף קטן (א), תיווסף על סכום שיש לשלמו, בתקופת הפריסה, ריבית שקלית לפי חוק פסיקת ריבית והצמדה.

(ג) לא שילם המפר תשלום במועדו, יראו את החלטת הממונה על פריסת התשלום כאמור בסעיף קטן (א) כבטלה, יתרת החוב תעמוד לפירעון מיידי ויחולו הוראות סעיף 35.

דברי הסבר

הממונה לא יהיה רשאי להטיל עיצום כספי בסכום נמוך מהסכומים הקבועים לפי סימן מוצע זה, אלא לפי הוראות תקנות ההפחתה. בתקנות ההפחתה, רשאי הגורם המאסדר לקבוע נסיבות ושיקולים שייבחנו, כגון שיקולים המעידים על כך שמדובר בארגון המציית בדרך כלל להוראות החוק או בארגון המשתף פעולה עם העובד המוסמך המגזרי או המנהל הבכיר ברשות המוסמכת, ואשר נכון לנקוט אמצעים למניעת הישנות ההפרה או לתקן את הנזקים שנגרמו בשלה. כמו כן, במסגרת תקנות ההפחתה יהיה ניתן להתחשב במחזור עסקאותיו של הארגון, אם מידע על אודותיו נמסר לממונה על ידי הארגון, ולקבוע אפשרות הפחתה של סכום העיצום הכספי במקרים שבהם קיים חשש להמשך פעילותו הכלכלית של הארגון. זאת, מאחר שמטרת העיצום הכספי, כאמור, היא להשיב את הארגון למשטר ציות בלי לסכן את המשך רציפותו התפקודית.

סעיף 33 מוצע לקבוע את מנגנון ההצמדה של סכום העיצום הכספי.

סעיף 34 מוצע לקבוע שארגון ישלם את העיצום הכספי בתוך 30 ימים מיום מסירת דרישת התשלום כאמור בסעיף 30 לחוק המוצע.

סעיף 35 מוצע לקבוע שאם לא שילם ארגון עיצום כספי במועד, תיווסף על העיצום הכספי, לתקופת הפיגור, ריבית שקלית ודמי פיגורים לפי חוק פסיקת ריבית והצמדה, התשכ"א–1961, עד לתשלומו.

סעיף 36 מוצע לקבוע את סמכות הממונה לפרוס את תשלום העיצום הכספי בהתחשב בסכומו ובנסיבות מיוחדות אחרות שיצדיקו פריסה כאמור, ובלבד שמספר התשלומים לא יעלה על 12 תשלומים חודשיים.

[9] ס"ח התשכ"א, עמ' 192.

גבייה

37. עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה–1995[10].

סימן ג': התראה מינהלית

התראה מינהלית

38. (א) היה לממונה יסוד סביר להניח כי ארגון הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 27, והתקיימו נסיבות שקבע ראש מערך הסייבר הלאומי, בנהלים, באישור היועץ המשפטי לממשלה, רשאי הממונה, במקום להטיל עליו עיצום כספי לפי הוראות סימן ב', למסור לו התראה מינהלית לפי הוראות סימן זה; בסעיף קטן זה, "היועץ המשפטי לממשלה" – לרבות משנה ליועץ המשפטי לממשלה שהיועץ המשפטי לממשלה הסמיכו לעניין זה.

(ב) בהתראה מינהלית יציין הממונה מהו המעשה המהווה את ההפרה ומועד ביצועה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהיה צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין כאמור בסעיף 31, וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 39.

(ג) על אף האמור בסעיף קטן (א), היה לממונה יסוד סביר להניח כי ארגון הפר, לראשונה, הוראה מההוראות לפי חוק זה, כמפורט להלן, ובכוונתו להטיל עליו עיצום כספי לפי הוראות סימן ב', ימסור לו התראה מינהלית לפי הוראות סימן זה במקום להטיל עליו עיצום כספי כאמור:

(1) הפר את ההוראה שבפרט (1)(ו) לתוספת הרביעית, כמפורט בפרט 6 לתוספת השישית;

דברי הסבר

סעיף 37 מוצע לקבוע, כי עיצום כספי ייגבה לאוצר המדינה ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה–1995.

סימן ג': התראה מינהלית

סעיף 38 לסעיף קטן (א)

סעיף מוצע זה מבקש לעגן את האפשרות לעשות שימוש בכלי אכיפה חלופי – ההתראה המינהלית. זהו כלי אכיפה המקל עם הארגון המפר, ומחליף במקרים מסוימים הטלה של עיצום כספי. כלי אכיפה זה הוא כלי המיועד לעודד ציות של ארגונים לפי החוק ולאפשר התמודדות עם הפרות עתידיות, על ידי מתן תמריץ שלילי לביצוע הפרות ותמריץ חיובי לציות. ההתראה המינהלית מאפשרת לארגון הזדמנות לתקן את ההפרה, בלא תשלום העיצום הכספי. זאת, אף על פי שהתשתית העובדתית שלפני הממונה מעידה כי הייתה הפרה של הוראות החוק. מנקודת מבטו של הממונה, מנגנון ההתראה מאפשר לו להבהיר את דרישותיו לארגונים, בטרם יטיל עליהם עיצום כספי. ההתראה המינהלית מאפשרת להבהיר גם לארגון המפר וגם לציבור הארגונים הרלוונטיים במגזר כי ההתנהגות שבשלה נשלחה ההתראה היא הפרה של הוראות החוק.

יובהר כי השימוש בכלי זה מתאים רק להפרות שאין בהן חומרה יתרה. הפרות חמורות מחייבות הפגנת מדיניות רגולציה תקיפה ולכן, ככלל, נדרש יהיה להטיל עיצומים ולא יהיה ניתן להסתפק בהתראה. ככלל, גם במצב שבו המפר מפר את ההוראה שלא בפעם הראשונה, השימוש בכלי אכיפה זה אינו מתאים. כדי להבטיח שקיפות ושוויוניות באכיפה ולהגביר את הוודאות, מוצע להבנות את שיקול הדעת של הממונה בהפעלת הסמכות ולקבוע מהם המקרים המתאימים למשלוח התראה, בנהלים שיקבע ראש מערך הסייבר הלאומי באישור היועץ המשפטי לממשלה או משנה ליועץ המשפטי לממשלה שהוא הסמיך לכך.

לסעיף קטן (ב)

מוצע לקבוע שבמתן התראה מינהלית יציין הממונה מהו המעשה המהווה את ההפרה ומועד ביצועה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה, יהיה צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין, כאמור בסעיף 31 לחוק המוצע, וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 39 המוצע.

לסעיף קטן (ג)

מוצע לקבוע כי ביחס להפרה בפעם הראשונה של דרישות מסוימות המפורטות בתוספת הרביעית לעניין רמת הגנת סייבר בסיסית בארגון חיוני, אשר בעניינן ייתכן שתעלה אי־בהירות באשר לאופן יישומן, תמיד תימסר התראה מינהלית טרם תימסר הודעה על כוונת חיוב וטרם יוטל עיצום כספי לפי סעיף 27 לחוק המוצע.

[10] ס"ח התשנ"ה, עמ' 170.

(2) הפר את ההוראה שבפרט (1)(ח) לתוספת הרביעית, כמפורט בפרט 8 לתוספת השישית;

(3) הפר את ההוראה שבפרט (3)(ג) לתוספת הרביעית, כמפורט בפרט 27 לתוספת השישית;

(4) הפר את ההוראה שבפרט (5)(ב) לתוספת הרביעית, כמפורט בפרט 36 לתוספת השישית;

(5) הפר את ההוראה שבפרט (7)(א) לתוספת הרביעית, כמפורט בפרט 44 לתוספת השישית;

(6) הפר את ההוראה שבפרט (8)(ד) לתוספת הרביעית, כמפורט בפרט 50 לתוספת השישית.

בקשה לביטול התראה מינהלית

39. (א) נמסרה למפר התראה מינהלית כאמור בסעיף 38, רשאי הוא לפנות לממונה, בכתב, בתוך 30 ימים, בבקשה לבטל את ההתראה בשל כל אחד מטעמים אלה:

(1) המפר לא ביצע את ההפרה;

(2) המעשה שביצע הארגון המפר, המפורט בהתראה, אינו מהווה הפרה של הוראות חוק זה.

(ב) הממונה רשאי להאריך את התקופה האמורה בסעיף קטן (א), מטעמים מיוחדים שיירשמו.

(ג) קיבל הממונה בקשה לביטול התראה מינהלית לפי הוראות סעיף קטן (א), רשאי הוא לבטל את ההתראה או לדחות את הבקשה ולהשאיר את ההתראה על כנה; החלטת הממונה תינתן בכתב, ותימסר למפר בצירוף נימוקים.

דברי הסבר

סעיף 39 לסעיף קטן (א)

אף על פי שמשלוח ההתראה אינו מלווה בסנקציה מיידית, דוגמת הטלת העיצום הכספי, לנוכח העובדה שיש בהתראה קביעה בדבר ביצועה של הפרה ומשמעויות עתידיות לגבי הפרות נוספות, בסעיף 39(א) לחוק המוצע, מוצע לקבוע שארגון יהיה רשאי לבקש לבטל את ההתראה האמורה באמצעות הגשת בקשה בשל אחד מהטעמים האלה:

1. הארגון לא ביצע את ההפרה.

2. המעשה שביצע הארגון המפר, המפורט בהתראה, אינו מהווה הפרה של הוראות החוק המוצע.

לסעיף קטן (ב)

מוצע לקבוע כי הממונה רשאי להאריך את התקופה האמורה בסעיף קטן (א) המוצע מטעמים מיוחדים שיירשמו.

לסעיף קטן (ג)

מוצע לקבוע, בהמשך להגשת הבקשה לביטול ההתראה המינהלית, כי הממונה רשאי לבטל את ההתראה או לדחות את הבקשה ולהותיר את ההתראה על כנה. החלטת הממונה תינתן לארגון בכתב בצירוף נימוקי ההחלטה.

יובהר, כי אם הארגון לא הגיש בקשה לביטול ההתראה לפי סעיף זה בתוך 30 ימים מקבלת התראה מינהלית, בעת ביצוע הפרה נוספת (שבשלה יוטל עיצום כספי מוגבר), יהיה הארגון מנוע מלטעון כי לא ביצע את ההפרה הראשונה. תחימת אפשרות העלאת הטענות לשלב משלוח ההתראה בלבד נועדה ליצור סופיות להליכים, וכן ודאות ומתן תוקף להתראה ככזו שאמורה להניע את המפר לציית לחוק המוצע.

לעניין זה יובהר כי מכיוון שבהתראה מינהלית מוותר הממונה על העיצום הכספי בשל ההפרה, סכום העיצום הכספי שיוטל במקרה זה הוא בשל הימשכות ההפרה, ואינו כולל את סכום העיצום הכספי בשל ההפרה הראשונית שבשלה ניתנה ההתראה. ההודעה על כוונת חיוב בשל הפרה מתמשכת או חוזרת שימסור הממונה לארגון במקרה זה תהיה כאמור בסעיף 31 המוצע, בשינויים המחויבים. כך למשל, ההודעה תכלול פרטים הנוגעים להפרה הנמשכת, ובין השאר נתונים לעניין התמשכות ההפרה או פרטים הנוגעים להפרה החוזרת ולסכום העיצום הכספי המוטל בגין ההפרה.

הפרה נמשכת והפרה חוזרת לאחר התראה

40. (א) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר המשיך להפר את ההוראה שבשלה נמסרה לו ההתראה, יראו את ההפרה כאמור כהפרה נמשכת לעניין סעיף 31, והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה הנמשכת, בהתאם להוראות סעיף 28, בשינויים המחויבים.

(ב) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר חזר והפר את ההוראה שבשלה נמסרה לו ההתראה, בתוך שנתיים מיום מסירת ההתראה, יראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 31(ב), והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה החוזרת, בהתאם להוראות סעיף 28, בשינויים המחויבים.

סימן ד': שונות

עיצום כספי בשל הפרה של הוראות לפי חוק זה ולפי חוק אחר

41. על מעשה אחד המהווה הפרה של הוראות לפי חוק זה המנויות בסעיף 27 וכן מהווה הפרה לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד.

עיכוב ביצוע והחזר

42. (א) אין בהגשת עתירה לבית משפט לעניינים מינהליים על החלטת הממונה לפי פרק זה, כדי לעכב את ביצוע ההחלטה, אלא אם כן הסכים לכך הממונה או שבית המשפט הורה על כך.

(ב) החליט בית המשפט, לאחר ששולם העיצום הכספי, לקבל עתירה כאמור בסעיף קטן (א) או ערעור על פסק דין בעתירה כאמור והורה בית המשפט על החזרת סכום העיצום הכספי ששולם או על הפחתת העיצום הכספי, יוחזר הסכום ששולם או כל חלק ממנו אשר הופחת, לפי העניין, בתוספת הפרשי הצמדה וריבית, לפי חוק פסיקת ריבית והצמדה מיום תשלומו או הפקדתו עד יום החזרתו.

פרסום

43. (א) הטיל הממונה עיצום כספי לפי פרק זה, יפרסם באתר האינטרנט של רשות מוסמכת את הפרטים שלהלן, בדרך שתבטיח שקיפות לגבי הפעלת שיקול דעתו בקבלת ההחלטה להטיל עיצום כספי:

(1) דבר הטלת העיצום הכספי;

דברי הסבר

סעיף 40 מוצע לקבוע כי אם נמסרה למפר התראה מינהלית והמפר המשיך להפר את ההוראה שבשלה נמסרה לו ההתראה, יראו את ההפרה כהפרה נמשכת, והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה הנמשכת, בהתאם להוראות סעיף 28 לחוק המוצע, בשינויים המחויבים. כמו כן, מוצע לקבוע כי אם נמסרה למפר התראה מינהלית והמפר חזר והפר את ההוראה שבשלה נמסרה לו ההתראה, בתוך שנתיים מיום מסירת ההתראה, יראו את ההפרה הנוספת כהפרה חוזרת והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה החוזרת, בהתאם להוראות סעיף 28 לחוק המוצע, בשינויים המחויבים.

סימן ד': שונות

סעיף 41 מוצע לקבוע שעל מעשה אחד המהווה הפרה של הוראות החוק לפי ההפרות המנויות בפרק מוצע זה, אשר מהווה הפרה גם לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד, וזאת כדי ליצור ודאות וסופיות דיונית.

סעיף 42 מוצע לקבוע שאין בהגשת עתירה לבית משפט לעניינים מינהליים על החלטת הממונה לפי פרק מוצע זה, כדי לעכב את ביצוע החלטתו, אלא אם כן הסכים לכך הממונה או שבית המשפט שאליו הוגשה העתירה הורה על כך. כמו כן מוצע לקבוע הוראות לעניין החזרת הסכום ששולם בנסיבות שבהן החליט כאמור בית המשפט, לאחר ששולם העיצום הכספי.

סעיף 43 לסעיף קטן (א)

מוצע לחייב את הממונה לפרסם את החלטותיו בדבר הטלת העיצום הכספי. תכלית חובת הפרסום היא הבטחת שקיפות לגבי הפעלת שיקול דעתו של הממונה, אשר בידיו מסורה סמכות רבת עוצמה. באמצעות הפרסום מובטחת בקרה ציבורית על כך שהשימוש בסמכות להטיל עיצום כספי הוא שוויוני וענייני. חובת הפרסום חלה על ההחלטות בדבר הטלת העיצומים הכספיים, מהות ההפרה שבשלה הוטל העיצום הכספי ונסיבות ההפרה, סכומי העיצומים הכספיים שהוטלו, הנסיבות והשיעורים שבהם הם הופחתו, אם הופחתו, פרטים על אודות הארגון המפר הנוגעים לעניין ושם הארגון המפר. מידע זה יאפשר בחינה רוחבית מושכלת של הטלת העיצומים הכספיים ויאפשר לארגון לדעת כי העיצום הכספי המוטל במקרה שלו תואם את המדיניות הכללית הנוגעת להפעלת הסמכות האמורה.

(2) מהות ההפרה שבשלה הוטל העיצום הכספי ונסיבות ההפרה;

(3) סכום העיצום הכספי שהוטל;

(4) אם הופחת העיצום הכספי – הנסיבות שבשלהן הופחת סכום העיצום ושיעורי ההפחתה;

(5) פרטים על אודות הארגון המפר, הנוגעים לעניין;

(6) שם הארגון המפר.

(ב) הוגשה עתירה לבית משפט לעניינים מינהליים על החלטת הממונה להטיל עיצום כספי או הוגש ערעור על החלטה בעתירה כאמור, יפרסם הממונה, לפי סעיף קטן (א) גם את דבר הגשת העתירה או הערעור ואת תוצאותיהם.

(ג) על אף האמור בסעיף זה, רשאי הממונה, בהתייעצות עם מערך הסייבר הלאומי, לדחות את הפרסום בתקופות נוספות של 30 ימים כל אחת, אם מצא כי הוא עלול לפגוע בהגנת הסייבר הלאומית או בהגנת הסייבר של הארגון המפר; הממונה לא יפרסם פרטים שהם בגדר מידע שרשות ציבורית מנועה מלמסור לפי סעיף 9(א) לחוק חופש המידע, התשנ"ח–1998[11], וכן רשאי הוא שלא לפרסם פרטים לפי סעיף זה, שהם בגדר מידע שרשות ציבורית אינה חייבת למסור לפי סעיף 9(ב) לחוק האמור.

(ד) פרסום לפי סעיף זה יהיה לתקופה של ארבע שנים.

(ה) מנהל הרשות המוסמכת רשאי לקבוע דרכים נוספות לפרסום הפרטים האמורים בסעיף זה.

שמירת אחריות פלילית

44. (א) תשלום עיצום כספי או מסירת התראה מינהלית, לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה המנויות בפרק ח', המהווה עבירה.

(ב) מסר הממונה למפר הודעה על כוונת חיוב או התראה מינהלית, בשל הפרה המהווה גם עבירה, לא יוגש נגדו כתב אישום בשל אותה הפרה, אלא אם כן התגלו עובדות חדשות המצדיקות זאת; התגלו עובדות חדשות כאמור והוגש נגד המפר כתב אישום לאחר שהמפר שילם עיצום כספי, יוחזר לו הסכום ששולם בתוספת ריבית שקלית לפי חוק פסיקת ריבית והצמדה מיום תשלום הסכום עד יום החזרתו.

דברי הסבר

לסעיף קטן (ב)

מוצע לקבוע כי אם הוגשה עתירה לבתי משפט לעניינים מינהליים על החלטת הממונה להטיל עיצום כספי או הוגש ערעור על החלטה בעתירה כאמור, יפרסם הממונה, לפי סעיף קטן (א) המוצע גם את דבר הגשת העתירה או הערעור ואת תוצאותיהם.

לסעיף קטן (ג)

מוצע לקבוע כי הממונה יהיה רשאי, בהתייעצות עם מערך הסייבר הלאומי, לדחות את הפרסום בתקופות נוספות של 30 ימים כל אחת, אם מצא כי הוא עלול לפגוע בהגנת הסייבר הלאומית או בהגנת הסייבר של הארגון המפר. עוד מוצע לקבוע שהממונה לא יפרסם פרטים שהם בגדר מידע שרשות ציבורית מנועה מלמסור לפי סעיף 9(א) לחוק חופש המידע, התשנ"ח–1998, וכן רשאי הוא שלא לפרסם פרטים לפי סעיף זה, שהם בגדר מידע שרשות ציבורית אינה חייבת למסור לפי סעיף 9(ב) לחוק האמור.

עוד מוצע בסעיף קטן (ד) להגביל את תקופת הפרסום לארבע שנים ובסעיף קטן (ה) לקבוע כי מנהל הרשות המוסמכת רשאי לקבוע דרכים נוספות לפרסום הפרטים האמורים בסעיף המוצע.

סעיף 44 לסעיף קטן (א)

מוצע לקבוע שתשלום עיצום כספי או מסירת התראה מינהלית לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם, לרבות ארגון, בשל הפרת הוראה מהוראות לפי פרק ח' לחוק מוצע זה.

לסעיף קטן (ב)

מוצע לקבוע כי אם מסר הממונה למפר הודעה על כוונת חיוב או התראה מינהלית בשל הפרה המהווה גם עבירה, לא יוגש נגדו כתב אישום בשל אותה הפרה, אלא אם כן התגלו עובדות חדשות המצדיקות זאת.

[11] ס"ח התשנ"ח, עמ' 226.

(ג) הוגש נגד אדם כתב אישום בשל עבירה המהווה הפרה, לא ינקוט נגדו הממונה הליכים לפי פרק זה בשל ההפרה.

שינוי התוספת השישית

45. (א) ראש הממשלה, לאחר שהובאה לפניו המלצת ראש מערך הסייבר הלאומי, בהסכמת שר המשפטים, רשאי, בצו, לשנות את חלק א' לתוספת השישית, ובלבד שסכום העיצום הכספי שייקבע בטור ב' בחלק א' לאותה תוספת, לא יעלה על 640,000 שקלים חדשים.

(ב) גורם מאסדר שקבע בתקנות לפי סעיף 9(ג) דרישות נוספות כאמור באותו סעיף, החלות לעניין ארגונים חיוניים במגזר שבו הוא אמון על אסדרת תחום הגנת הסייבר, רשאי, בצו, בהתייעצות עם ראש מערך הסייבר הלאומי, בהסכמת שר המשפטים, ובאישור ועדת החוץ והביטחון של הכנסת, להוסיף לחלק ב' לתוספת השישית, דרישות שנקבעו כאמור, בציון המגזר שלגביו הן חלות, ובלבד שסכום העיצום הכספי שיקבע בטור ב' בחלק ב' לאותה תוספת, לצד הדרישות שנוספו כאמור, לא יעלה על 640,000 שקלים חדשים.

פרק ח': סודיות ועונשין

שמירת סודיות, הגבלת שימוש ומחיקה

46. (א) אדם שהגיע לידיו לפי חוק זה מידע אישי, ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לשם ביצוע חוק זה, לשם הפעלת סמכות לפי דין שעניינה הגנת סייבר, או לפי צו של בית משפט.

(ב) מידע אישי שהתקבל לפי חוק זה יישמר בהיקף המזערי הנדרש, ויימחק לאחר שנתיים לכל היותר מעת קבלתו, אלא אם כן קבע עובד מוסמך מגזרי או עובד מוסמך במערך כי הוא חיוני לזיהוי מאפייני תקיפת סייבר או להתמודדות עם תקיפת סייבר שמתרחשת או שיש חשש שעומדת להתרחש, או שהוא נדרש להליכים לפי פרק זה או פרק ז', וכל עוד הוא חיוני או נדרש כאמור.

דברי הסבר

לסעיף קטן (ג)

מוצע לקבוע שאם הוגש כתב אישום נגד אדם (לרבות ארגון) בשל עבירה המהווה הפרה, לא ינקוט נגדו הממונה הליכים לפי פרק מוצע זה בשל ההפרה.

סעיף 45 לסעיף קטן (א)

מוצע לקבוע שראש הממשלה, לאחר שהובאה לפניו המלצת ראש מערך הסייבר הלאומי, בהסכמת שר המשפטים, רשאי, בצו, לשנות את חלק א' לתוספת השישית, ובלבד שסכום העיצום הכספי שייקבע בטור ב' בחלק א' לאותה תוספת לא יעלה על 640,000 שקלים חדשים.

לסעיף קטן (ב)

מוצע לקבוע שגורם מאסדר אשר קבע תקנות לעניין דרישות רמת הגנה נוספות לארגון חיוני בהתאם לסעיף 9(ג) לחוק המוצע, רשאי בצו, בהתייעצות עם ראש מערך הסייבר הלאומי, בהסכמת שר המשפטים ובאישור ועדת החוץ והביטחון בכנסת, להוסיף לחלק ב' לתוספת השישית, לעניין המגזר שהוא אמון על אסדרתו, דרישות נוספות שיהיה אפשר להטיל בשל הפרתן עיצום כספי, תוך קביעת סכום העיצום בטור ב' לצידן, ובלבד שסכום העיצום הכספי שיקבע כאמור לצד הדרישות שנוספו לא יעלה על 640,000 שקלים חדשים.

פרק ח': סודיות ועונשין

סעיף 46 לסעיף קטן (א)

כדי להגן על הזכות לפרטיות של אדם שמידע אישי לגביו הגיע לידי אדם אחר לפי החוק המוצע, מוצע לקבוע שאם אדם קיבל מידע אישי שהתקבל לפי החוק המוצע, הוא ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לשם ביצוע החוק המוצע, לשם הפעלת סמכות לפי דין שעניינה הגנת סייבר, או לפי צו של בית משפט. יצוין שהגנת סייבר כוללת, לרבות בהקשר של סעיף מוצע זה, אבטחת מידע.

לסעיף קטן (ב)

מוצע לקבוע שמידע אישי שהתקבל לפי חוק זה יישמר בהיקף המזערי הנדרש, ויימחק לאחר שנתיים לכל היותר מעת קבלתו, אלא אם כן קבע עובד מוסמך מגזרי או עובד מוסמך במערך הסייבר הלאומי כי הוא חיוני לזיהוי מאפייני תקיפת סייבר או להתמודדות עם תקיפת סייבר שמתרחשת או שיש חשש שעומדת להתרחש או שהוא נדרש להליכי הטלת עיצומים לפי פרק זה או פרק ז' לחוק המוצע, וכל עוד הוא חיוני או נדרש כאמור.

(ג) פרסום פומבי של זהות ארגון שהתקבלה לפי חוק זה, יהיה באישור מנהל בכיר במערך או מנהל בכיר ברשות מוסמכת לאחר שנתן לארגון הזדמנות להשמיע את טענותיו.

(ד) אדם שגילה מידע אישי שהתקבל לפי חוק זה, עשה שימוש במידע אישי כאמור או שמר מידע כאמור, בניגוד להוראות סעיף זה, דינו – מאסר שלוש שנים.

עונשין

47. (א) ארגון העושה אחד מאלה, דינו – מאסר שנתיים או קנס כאמור בסעיף 61(א)(4) לחוק העונשין:

(1) לא נקט אמצעים כפי שהורה ראש מערך הסייבר הלאומי או ראש מלמ"ב לפי סעיף 11 או לפי הסעיף האמור כפי שהוחל בסעיף 21(א)(6), בהתאמה;

(2) לא מילא הוראה שנתן לו עובד מוסמך מגזרי, בניגוד להוראות סעיפים 14(ג)(4) ו־(5) או 15(א), או לא מילא הוראה שנתן לו עובד מוסמך במערך לפי אותם סעיפים, בניגוד להוראות סעיף 16(א);

(3) לא מילא הוראה שנתן לו עובד מוסמך במלמ"ב, בניגוד להוראות סעיף 14(ג)(4) ו־(5) כפי שהוחל בסעיף 21.

(ב) הייתה העבירה כאמור בסעיף קטן (א) עבירה נמשכת, רשאי בית המשפט להטיל קנס נוסף, בשיעור הקבוע בסעיף 61(ג) לחוק העונשין, לכל יום שבו נמשכת העבירה.

אחריות נושא משרה בתאגיד

48. (א) נושא משרה בארגון שהוא תאגיד (בסעיף זה – תאגיד) חייב לפקח ולעשות כל שניתן למניעת עבירות לפי סעיף 47(א) בידי תאגיד או בידי עובד מעובדיו; המפר הוראה זו, דינו – קנס כאמור בסעיף 61(א)(3) לחוק העונשין; לעניין סעיף זה, "נושא משרה" – מנהל פעיל בתאגיד, שותף למעט שותף מוגבל, או פקיד האחראי מטעם התאגיד על התחום שבו בוצעה העבירה.

דברי הסבר

לסעיף קטן (ג)

מוצע לקבוע שפעולה יזומה של רשות מוסמכת, לרבות פעולה כאמור של מלמ"ב או של השירות המבוצעת מכוח סעיפים 21 ו־22 לחוק המוצע, בהתאמה, או פעולה כאמור של המערך – לפרסום פומבי של זהות ארגון, לרבות ארגון חיוני או ספק שירותים דיגיטליים או שירותי אחסון, שהתקבלה לפי החוק המוצע, תהיה באישור מנהל בכיר במערך הסייבר הלאומי או מנהל בכיר ברשות מוסמכת, במלמ"ב או בשירות, בהתאמה, לאחר שגורם זה נתן לארגון הזדמנות להשמיע את טענותיו.

לסעיף קטן (ד)

מוצע לקבוע עבירה שדינה שלוש שנות מאסר על אדם שגילה מידע אישי שהתקבל מארגון לפי החוק המוצע, עשה שימוש במידע אישי שהתקבל מארגון לפי החוק המוצע או שמר מידע כאמור, בניגוד להוראות סעיף מוצע זה.

סעיף 47 לנוכח הפגיעה האפשרית באינטרס הציבורי כתוצאה מהפרה של הוראות החוק המוצע, מוצע להטיל אחריות פלילית על ארגון שלא קיים הוראה שתכליתה הגנה על הציבור מפני תקיפות סייבר.

לסעיף קטן (א)

מוצע לקבוע עבירה שדינה מאסר שנתיים או קנס כאמור בסעיף 61(א)(4) לחוק העונשין, על ארגון שלא נקט אמצעים להתמודדות עם סיכון משמעותי במשק או למניעתו, אשר נדרשים באופן דחוף, כפי שהורה ראש מערך הסייבר הלאומי לפי סעיף 11 המוצע או שהורה ראש מלמ"ב לפי סעיף 11 המוצע כפי שהוחל בסעיף 21(א)(6) בהתאמה. כמו כן מוצע להטיל אחריות פלילית בעבירה כאמור על ארגון שלא מילא הוראה להתמודדות עם תקיפת סייבר חמורה שנתן לו עובד מוסמך מגזרי בניגוד להוראות סעיפים 14(ג)(4) ו־(5) או 15(א) לחוק המוצע, ועל ארגון שלא מילא הוראה שנתן לו עובד מוסמך במערך הסייבר הלאומי, לפי אותם סעיפים, בניגוד להוראות סעיף 16(א) לחוק המוצע, או שלא מילא הוראה שנתן לו עובד מוסמך במלמ"ב בניגוד להוראות סעיף 14(ג)(4) ו־(5) לחוק המוצע כפי שהוחל בסעיף 21 המוצע.

לסעיף קטן (ב)

מוצע לקבוע שאם מדובר בעבירה נמשכת, נוסף על העונש האמור, בית המשפט יהיה רשאי להטיל קנס נוסף, בשיעור הקבוע בסעיף 61(ג) לחוק העונשין, לכל יום שבו נמשכת העבירה.

סעיף 48 מוצע לקבוע שנושא משרה בארגון שהוא תאגיד, כלומר מנהל פעיל בתאגיד, שותף למעט שותף מוגבל, או פקיד האחראי מטעם התאגיד על התחום שבו בוצעה העבירה, חייב לפקח ולעשות כל שניתן למניעת עבירות לפי סעיף 47(א) לחוק המוצע בידי התאגיד או בידי עובד מעובדיו, ואם הפר הוראה זו, יוטל עליו קנס כאמור בסעיף 61(א)(3) לחוק העונשין.

(ב) נעברה עבירה לפי סעיף 47(א) בידי תאגיד או בידי עובד מעובדיו, חזקה היא כי נושא משרה בתאגיד הפר את חובתו לפי סעיף קטן (א), אלא אם כן הוכיח כי עשה כל שניתן כדי למלא את חובתו.

פרק ט': הוראות שונות

מתן סיוע בידי המערך לארגון המעוניין בכך

49. (א) במסגרת סיוע בהגנת סייבר שנותן מערך הסייבר הלאומי, רשאי עובד המערך, כדי לסייע לארגון המעוניין בכך, לבצע פעולות סיוע בהגנת סייבר הכרוכות בקבלת מידע אישי, אם מתקיימים כל אלה:

(1) עובד המערך הסביר לנציג הארגון את כל אלה:

(א) הטעם המקצועי לסיוע;

(ב) הפעולות שיתבצעו כחלק מהסיוע;

(ג) האפשרות של הארגון שלא לקבל את הסיוע;

(2) לארגון יש מדיניות בנוגע לגישה למידע אישי ולעיבודו, ובמסגרתה הובהר כי קיימת אפשרות להעברת מידע אישי לגורם מחוץ לארגון לצורכי הגנת סייבר; ואולם אם נדרש מתן סיוע דחוף לארגון שאין לו מדיניות כאמור, רשאי עובד המערך לבצע פעולות סיוע כאמור אם הארגון התחייב לפניו ליידע את עובדיו על קבלת הסיוע ולפרסם מדיניות כאמור בסמוך ככל האפשר לאחר קבלת הסיוע.

(ב) במסגרת פעולות סיוע בהגנת סייבר המבוצעות לפי סעיף קטן (א) –

(1) לא יעובד מידע אישי אלא במידה הנדרשת לשם הגנת סייבר, בשים לב לרגישות המידע ובאופן שיצמצם ככל האפשר את הסיכון לפגיעה בפרטיות;

דברי הסבר

כמו כן, מוצע לקבוע חזקה ולפיה אם נעברה עבירה לפי סעיף 47(א) בידי תאגיד או בידי עובד מעובדיו, נושא משרה בתאגיד הפר את חובתו לפקח ולמנוע עבירות כאמור אלא אם כן הוכיח כי עשה כל שניתן כדי למלא את חובתו.

פרק ט': הוראות שונות

סעיף 49 מערך הסייבר הלאומי מסייע, בהקשרים ובתנאים שונים, לאנשים ולגופים שונים במטרה, בין השאר, להעלות את רמת ההגנה שלהם ולמנוע, לאתר או להתמודד עם תקיפות סייבר. סיוע זה מאפשר לקדם הגנה לאומית טובה יותר על המשק הישראלי בכללותו.

מטרת הסעיף המוצע היא להגדיר את התנאים הנדרשים למתן סיוע בהגנת סייבר של עובד מערך הסייבר הלאומי או מי מטעמו לארגון המעוניין בכך, אם אותו סיוע כאמור כרוך בקבלת מידע אישי כהגדרתו בחוק הגנת הפרטיות. הסיוע האמור יכול להינתן בעקבות פניית מערך הסייבר הלאומי לארגון או לבקשת הארגון.

יודגש כי במרבית המקרים, פעולות הסיוע של מערך הסייבר הלאומי אינן כרוכות בקבלת מידע אישי ופעולות מסוג זה אינן מוסדרות בחוק. לעניין זה יובהר כי גם במקרים שבהם סיוע מאת מערך הסייבר הלאומי עלול להיות כרוך בחשיפה למידע אישי, מדובר בתוצר נלווה לפעולת הסיוע שכן זוהי אינה מטרת הפעולה. עוד יובהר, כי אין בהוראות סעיף מוצע זה כדי להגביל מתן סיוע בנסיבות אחרות, אם אותו סיוע אינו כרוך בקבלת מידע אישי או אם מדובר בסיוע הניתן לאדם ולא לארגון.

נוסף על כך, יובהר כי מתן הסיוע כרוך בהשקעת משאבים ציבוריים, ולכן מתן הסיוע האמור בסעיף מוצע זה לא יינתן לכל ארגון, אלא יינתן בכפוף לשיקול דעת מערך הסייבר הלאומי ובהתאם לגדרי המוצע בסעיף.

כמו כן, מוצע לקבוע שמתן סיוע בהגנת הסייבר לפי סעיף מוצע זה יינתן לארגון הנמנה עם מגזר המנוי בתוספת הראשונה, על ידי המערך, לאחר התייעצות עם הרשות המוסמכת הנוגעת לעניין לגבי עצם מתן הסיוע.

יובהר כי הסעיף המוצע לא יחול לגבי גופים ממשלתיים, מאחר שפעולות המבוצעות עימם ובעבורם הן במסגרת פעילות משולבת של מערך הסייבר הלאומי עם גוף ממשלתי אחר, ואין מדובר בפעולות סיוע.

נוסף על כך, מוצע להגדיר מה ייחשב ל"פעולת סיוע בהגנת סייבר" לעניין סעיף מוצע זה (סעיף קטן (ו)). על פי המוצע, מדובר בפעולות לצורך סיוע במניעת תקיפת סייבר, איתור תקיפת סייבר או התמודדות עימה, לרבות פעולות הכרוכות בקבלת מידע בעל ערך לשם הגנת סייבר, באופן חד־פעמי או מתמשך או בקבלת גישה למחשב או לחומר

(2) ייעשה שימוש בטכנולוגיות ובשיטות פעולה באופן שיצמצם ככל האפשר חשיפה של אדם למידע אישי, ובכלל זה –

(א) מידע העלול לכלול מידע אישי לא יעובד על ידי אדם, אלא אם כן קבע מנהל מוסמך כי אופי פעולת הסיוע מחייב עיבוד על ידי אדם, בין השאר לצורך התמודדות עם תקיפת סייבר שמתרחשת או שיש חשש שעומדת להתרחש או לצורך ביצוע מבדק חדירות למערכות הארגון;

(ב) עיבוד על ידי אדם כאמור בפסקת משנה (א) –

(1) יבוצע בידי מי שעבר הכשרה לעניין הגנה על מידע אישי כפי שקבע ראש מערך הסייבר הלאומי, ובידו הרשאת גישה למידע;

(2) יתועד באופן שיאפשר פיקוח ובקרה על אופן ביצוע העיבוד, על מועד ביצועו ועל זהות מבצע העיבוד; המערך ישמור את התיעוד שבוצע לפי פסקת משנה זו למשך 3 שנים לפחות;

(3) פעולת סיוע בהגנת סייבר שהיא פעולה להגנת סייבר בחומר מחשב, תבוצע באמצעות נציג הארגון, אלא אם כן אישר ראש מערך הסייבר הלאומי, מטעמים מיוחדים, על פי בקשה בכתב מאת הארגון, כי הפעולה תבוצע בידי עובד המערך; אישר כאמור, תבוצע הפעולה בנוכחות נציג הארגון.

דברי הסבר

מחשב. יובהר שסיוע בהגנת סייבר אפשר שיינתן לא רק במסגרת התמודדות עם תקיפת סייבר פעילה אלא גם לשם מניעתה, לרבות סיוע בפעולות להעלאת חוסן בשגרה, בנסיבות שבהן הוחלט לתת סיוע כאמור.

עוד מוצע להגדיר את הארגונים שמערך הסייבר הלאומי יוכל לתת להם סיוע בהגנת סייבר תוך קבלת מידע אישי לפי סעיף מוצע זה. על פי המוצע, נדרש שמדובר בארגון אשר ראש מערך הסייבר הלאומי קבע כי קיים אינטרס לאומי לסייע לו בהגנת סייבר לפי סעיף מוצע זה, או ארגון שמתרחשת או שיש חשש שמתרחשת תקיפת סייבר נגדו או באמצעותו, ושמנהל בכיר במערך קבע כי קיים אינטרס לאומי לסייע לו בהגנת סייבר לפי סעיף מוצע זה אגב אותה תקיפת סייבר.

בסעיף קטן (א), מוצע לקבוע שורה של תנאים שבהתקיימם יוכל עובד המערך לבצע פעולות סיוע בהגנת סייבר הכרוכות בקבלת מידע אישי, כדי לסייע לארגון המעוניין בכך, כמפורט להלן:

1. תחילה, נדרש שעובד המערך יסביר לנציג הארגון את הטעם המקצועי לסיוע, הפעולות שיתבצעו כחלק מהסיוע והאפשרות של הארגון שלא לקבל את הסיוע (פסקה (1)). יובהר כי ארגון שהסכים לקבל סיוע בהגנת הסייבר לפי הסעיף המוצע, רשאי בכל עת להודיע בכתב למערך הסייבר הלאומי שאינו מעוניין עוד בסיוע – כולו או חלקו, והסיוע יופסק בהקדם האפשרי (סעיף קטן (ו)).

2. כדי לצמצם את הפגיעה האפשרית בזכויות, מוצע לקבוע שסיוע לפי סעיף זה יינתן לארגון בעל מדיניות בנוגע לגישה למידע אישי ולעיבודו, שבמסגרתה הובהרה האפשרות להעביר מידע אישי לגורם מחוץ לארגון לצורכי הגנת הסייבר. ואולם בנסיבות שבהן נדרש סיוע דחוף לארגון שאין לו מדיניות כאמור, יוכל עובד מערך הסייבר לבצע את פעולות הסיוע אם הארגון התחייב לפניו ליידע את עובדיו בדבר קבלת הסיוע וכן לפרסם מדיניות כאמור בסמוך ככל האפשר לאחר קבלת הסיוע (פסקה (2)). בהקשר זה יובהר שבחלק מהמקרים, מטעמים הנוגעים לביטחון הציבור, לא ניתן לחשוף לקהל הרחב את מתן הסיוע הדחוף עד למועד מאוחר לקבלתו על ידי הארגון.

אף על פי שכאמור, החשיפה למידע אישי היא תהליך נלווה לפעולות הסיוע להגנת סייבר שאינה במוקד הסיוע האמור, וכדי להבטיח הגנה מרבית על הזכות לפרטיות, מוצע, בסעיף קטן (ב), לקבוע שלא יעובד מידע אישי בהתאם לסעיף מוצע זה אלא במידה הנדרשת לשם הגנת סייבר, בשים לב לרגישות המידע ובאופן שיצמצם ככל האפשר את הסיכון לפגיעה בפרטיות.

עוד מוצע לקבוע שעובד מערך הסייבר הלאומי יעשה במסגרת סיוע לפי סעיף מוצע זה שימוש בטכנולוגיות ובשיטות פעולה באופן שיצמצם ככל האפשר חשיפה של אדם למידע אישי. בכלל זה, מידע העלול לכלול מידע אישי לא יעובד על ידי אדם אלא אם כן קבע מנהל מוסמך כי אופי פעולת הסיוע מחייבת עיבוד על ידי אדם, בין השאר לצורך התמודדות עם תקיפת סייבר או ביצוע מבדק חדירות למערכות הארגון.

נוסף על כך, מוצע לקבוע כי עיבוד על ידי אדם במקרים כאמור בפסקת משנה (א) יבוצע בידי מי שעבר הכשרה לעניין הגנה על מידע אישי כפי שקבע ראש מערך הסייבר הלאומי ובידו הרשאת גישה למידע, ויתועד באופן שיאפשר פיקוח ובקרה על אופן ביצוע העיבוד, על מועד ביצועו ועל זהות מבצע העיבוד. המערך ישמור את התיעוד שבוצע לפי פסקת משנה זו למשך 3 שנים לפחות.

(ג) ארגון שקיבל סיוע בהגנת סייבר לפי הוראות סעיף זה רשאי בכל עת להודיע בכתב למערך הסייבר הלאומי שאינו מעוניין עוד בהמשך פעולות הסיוע בהגנת סייבר; הודיע כאמור, יופסקו פעולות הסיוע בהקדם האפשרי.

(ד) לשם קבלת סיוע בהגנת סייבר לפי סעיף זה רשאי ארגון למסור מידע אישי למערך הסייבר הלאומי.

(ה) מערך הסייבר הלאומי יבצע פעולות סיוע בהגנת הסייבר, לפי סעיף זה, במסגרת סיוע לארגון הנמנה עם מגזר כאמור בפסקה (1) להגדרה "מגזר" שבסעיף 1, לאחר התייעצות עם הרשות המוסמכת.

(ו) פעולות סיוע בהגנת סייבר לפי סעיף זה יכול שיבוצעו, במסגרת סיוע בהגנת סייבר שניתן לארגון הנמנה עם מגזר כאמור בסעיף קטן (ה), גם על ידי הרשות המוסמכת, במסגרת הפעלת SOC מגזרי, ויחולו על פעולות הסיוע כאמור הוראות סעיף זה, בשינויים המחויבים ובשינוי זה: סמכות הנתונה לראש מערך הסייבר הלאומי לפי סעיף זה תהיה נתונה למנהל הרשות המוסמכת.

(ז) בסעיף זה –

"ארגון" – כל אחד מאלה:

(1) ארגון שראש מערך הסייבר הלאומי אישר כי קיים אינטרס לאומי לתת לו סיוע בהגנת סייבר לפי סעיף זה;

(2) ארגון שמתרחשת או שיש חשש שמתרחשת תקיפת סייבר נגדו או באמצעותו, ומנהל בכיר במערך קבע כי קיים אינטרס לאומי לסייע לו בהגנת סייבר לפי סעיף זה אגב אותה תקיפת סייבר;

"עיבוד" – כהגדרתו בחוק הגנת הפרטיות;

"פעולות סיוע בהגנת סייבר" – פעולות לצורך סיוע במניעת תקיפת סייבר, איתור תקיפת סייבר או התמודדות עם תקיפת סייבר, לרבות פעולות הכרוכות בקבלת מידע בעל ערך לשם הגנת סייבר, באופן חד־פעמי או מתמשך, או בקבלת גישה למחשב או לחומר מחשב.

דברי הסבר

עוד מוצע שבכלל, פעולה בחומר מחשב במסגרת סיוע וולונטרי לפי סעיף מוצע זה, תתבצע על ידי נציג הארגון. יודגש כי ככלל, ביצוע פעולות על העתק חומר מחשב שנמסר מהארגון באופן וולנטרי במסגרת סיוע לפי סעיף זה פוגענית פחות מביצוע פעולות במחשבי הארגון עצמם, ועל כן אפשר שפעולה בהעתק חומר מחשב כאמור תתבצע על ידי עובד במערך הסייבר הלאומי, בעוד פעולת סיוע שהיא פעולה להגנת סייבר בחומר מחשב לפי סעיף זה, שאינו עותק של מחשב, תתבצע באמצעות נציג הארגון, אלא אם כן אישר ראש המערך, מטעמים מיוחדים, על פי בקשה בכתב מאת הארגון, כי הפעולה תבוצע בידי עובד המערך. על פי המוצע, אם אישר ראש המערך כאמור, תבוצע הפעולה בנוכחות נציג הארגון.

להשלמת התמונה, מוצע להבהיר שארגון יוכל למסור מידע אישי במסגרת קבלת סיוע לפי סעיף זה והדבר לא ייחשב לפגיעה בפרטיות (סעיף קטן (ד)).

נוסף על כך, מוצע, בסעיף קטן (ו), לקבוע שרשות מוסמכת תוכל לתת סיוע לארגון הנמנה עם המגזר שעליו היא אמונה בהתאם לתוספת הראשונה המוצעת, במסגרת הפעלת מרכז שליטה ובקרה מגזרי (SOC מגזרי), כחלק מגיבוש תמונת מצב שוטפת בהיבטי הגנת הסייבר והטיפול באירועי סייבר במגזר. במקרים אלה הוראות הסעיף, לרבות האיזונים והבלמים שנקבעו בו, יחולו בשינויים המחויבים ובשינוי זה: "הסמכות הנתונה לראש מערך הסייבר הלאומי לפי סעיף זה תהיה נתונה למנהל הרשות המוסמכת". למען הסר ספק, יובהר כי הסעיף אינו חל על הפעלת SOC ממשלתי לעניין הגנת הסייבר של משרדי הממשלה עצמם, הכלולה, בין השאר, במסגרת תנאי ההעסקה של עובדי המדינה, וההסדרים בסעיף אינם מתייחסים אליה.

איתור פגיעויות חמורות

50. (א) עובד המערך רשאי, במסגרת ביצוע תפקידיו, לפעול לאיתור פגיעויות חמורות המוכרות למערך ולמתן התרעה עליהן.

(ב) פעולות כאמור בסעיף קטן (א), ייעשו במטרה לאתר את הפגיעויות החמורות בארגונים, באופן שאינו כולל גישה למערכות מחשוב שיש הגבלה על הגישה של הציבור אליהן מרשת האינטרנט או מרשת ציבורית אחרת, ושאין לו השפעה שלילית על מתן שירות בידי ארגון שביחס אליו מאותרת הפגיעות החמורה, בהתמקדות במידע הטכנולוגי בהיקף המזערי הנדרש לשם זיהוי קיומה או העדרה של פגיעות חמורה, בהימנעות ככל האפשר מחשיפה מידע אישי, ובלא איסוף מידע אישי.

הסתייעות במומחה חיצוני

51. (א) לשם הפעלת סמכויות עובד מוסמך מגזרי או עובד מוסמך במערך לפי חוק זה, וכן לשם הפעלת סמכויות עובד לפי סעיפים 49 או 50 (בסעיף זה – עובד מוסמך), רשאי עובד מוסמך להסתייע באדם שאינו עובד המדינה ושבידו אישור שניתן לו לפי הוראות סעיף קטן (ד) (בחוק זה – מומחה חיצוני) בעניינים שנדרשים לגביהם ניסיון, ידע או אמצעים ייחודיים.

(ב) מומחה חיצוני יפעל מטעמו של עובד מוסמך בהתאם להנחייתו ולהוראותיו ובפיקוחו; מומחה חיצוני לא יפעיל סמכות הכרוכה בהפעלה של שיקול הדעת שניתן לפי דין לעובד מוסמך.

(ג) מומחה חיצוני רשאי לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך, ובלבד שכל דרישה תאושר מראש על ידי העובד המוסמך.

דברי הסבר

סעיף 50 תקיפות סייבר רבות כנגד ארגונים מתבצעות תוך ניצול פגיעויות באותם ארגונים. לפיכך, מוצע לעגן בסעיף מוצע זה את הפעילות שמבצע מערך הסייבר הלאומי בהקשר זה, בהתאם לשיקול דעתו, לרבות בשים לב למשאבים ולאמצעים העומדים לרשותו לשם כך, ולהסמיך את עובד המערך, במסגרת ביצוע תפקידיו, לפעול לאיתור פגיעויות חמורות המוכרות למערך באמצעות אינדיקציה טכנולוגית המאפשרת זיהוי פגיעויות ברשתות ובמערכות, ומתן התרעה עליהן, ובכך להעלות את ההגנה של ארגונים במרחב הסייבר הלאומי.

בהקשר זה, מוצע לקבוע שפעילות עובד המערך לאיתור פגיעויות כאמור, תתבצע במטרה לאתר את הפגיעויות בארגונים, באופן שאינו כולל גישה למערכות מחשוב שיש הגבלה על הגישה של הציבור אליהן מרשת האינטרנט או מרשת ציבורית אחרת, ואשר אין לו השפעה שלילית על מתן שירות בידי ארגון שביחס אליו מאותרת הפגיעות החמורה, ותוך התמקדות במידע הטכנולוגי בהיקף המזערי הנדרש לשם זיהוי קיומה או העדרה של הפגיעות החמורה.

פעילות זו מטבעה ממוקדת כאמור במידע טכנולוגי, דוגמת סוג המערכת וגרסתה, אך למען הסר ספק, מוצע להדגיש בסעיף מוצע זה כי הפעילות תבוצע תוך הימנעות ככל האפשר מחשיפה למידע אישי ובלא איסוף מידע אישי, לרבות אחסון, העתקה, העברה או מסירה של מידע אישי.

סעיף 51 לסעיף קטן (א)

מוצע לקבוע שלצורך הפעלת סמכות עובד מוסמך מגזרי או עובד מוסמך במערך לפי החוק המוצע, לרבות כפי שהוחלו בסעיפים 21 ו־22, וכן לשם הפעלת סמכות עובד לפי סעיפים 49 או 50 לחוק המוצע (בדברי ההסבר לסעיף זה – עובד מוסמך), בעניינים שנדרשים לגביהם ניסיון, ידע או אמצעים ייחודיים, יוכל עובד מוסמך להסתייע באדם שאינו עובד מדינה ושבידו אישור שניתן לו לפי הוראות סעיף קטן (ד) המוצע (להלן – מומחה חיצוני).

לסעיף קטן (ב)

כדי להבטיח שגם כאשר סמכויות מופעלות על ידי מומחה חיצוני כאמור, יחולו כלל המגבלות, האיזונים והבלמים הנדרשים, מוצע לקבוע שמומחה חיצוני יפעל מטעמו של עובד מוסמך בהתאם להנחייתו ולהוראותיו ושהעובד המוסמך יפקח על ביצוע הפעולות על ידי המומחה החיצוני. עוד מוצע להבהיר, ששיקול הדעת שניתן לפי דין לעובד מוסמך לא יופעל על ידי המומחה החיצוני.

לסעיף קטן (ג)

מוצע לקבוע שמומחה חיצוני יהיה רשאי לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך, ובלבד שכל דרישה תאושר מראש על ידי העובד המוסמך.

(ד) מומחה חיצוני רשאי, לשם סיוע לעובד מוסמך מגזרי בהפעלת סמכותו לפי סעיף 24, להיכנס למקום גם בלא נוכחות של העובד המוסמך המגזרי, ובלבד שהמקום אינו מקום המשמש למגורים, ושניתנה הסכמה בכתב של מחזיק המקום לכניסת המומחה החיצוני למקום, לאחר שניתן למחזיק המקום הסבר על מטרת הכניסה למקום וכן על זכותו לסרב לכניסת המומחה החיצוני למטרה כאמור או לחזור בו מהסכמתו.

(ה) מנהל בכיר ברשות מוסמכת או מנהל בכיר במערך (בסעיף זה – הגורם המאשר) רשאי לתת למי שמתקיימים בו כל אלה אישור לשמש מומחה חיצוני:

(1) הוא בעל ניסיון, ידע ומומחיות המתאימים לתפקידו;

(2) הוא לא הורשע בעבירה שמפאת מהותה, חומרתה או נסיבותיה הוא אינו ראוי לשמש מומחה חיצוני ולא הוגש נגדו כתב אישום בעבירה כאמור.

(ו) (1) לא ימונה למומחה חיצוני ולא יכהן כמומחה חיצוני מי שבשל כהונתו יימצא באופן תדיר במצב של ניגוד עניינים.

(2) מומחה חיצוני לא יטפל במסגרת תפקידו בנושא שהטיפול בו יגרום לו להימצא במצב של ניגוד עניינים.

(3) נודע למומחה חיצוני כי הוא עלול להימצא במצב של ניגוד עניינים כאמור בפסקאות (1) או (2), יודיע על כך בהקדם לגורם המאשר.

(ז) הרואה את עצמו נפגע מפעולה של מומחה חיצוני, רשאי לפנות בתלונה מנומקת בכתב, לגורם המאשר; הגורם המאשר יבחן את התלונה וישיב לפונה, בכתב, בתוך 45 ימים; הגורם המאשר יעביר העתק מתשובתו למומחה החיצוני.

(ח) דינו של מומחה חיצוני כדין עובדי המדינה לעניין ההוראות הנוגעות לעובדי הציבור בחוק העונשין, וההוראות בחוק שירות הציבור (מתנות), התש"ם–1979[12].

(ט) מגבלות על עיסוקיו של המומחה החיצוני לאחר סיום ההתקשרות עימו ייקבעו בחוזה ההתקשרות עימו, ובכלל זה הוראות לעניין פרק הזמן שבו לא יעבוד המומחה החיצוני אצל גוף שמתחרה בגוף שטיפל בענייניו כמומחה חיצוני ולא ייתן שירות לגוף כאמור או יקבל זכות או טובת הנאה ממנו.

דברי הסבר

לסעיף קטן (ד)

מוצע לקבוע שמומחה חיצוני יהיה רשאי, לשם סיוע לעובד מוסמך מגזרי בהפעלת סמכותו לפי סעיף 24 המוצע, להיכנס למקום גם בלא נוכחות של העובד המוסמך המגזרי, ובלבד שהמקום אינו משמש למגורים ושניתנה הסכמה בכתב של מחזיק המקום לכניסת המומחה החיצוני למקום, לאחר שניתן לו הסבר על אודות מטרת הכניסה ועל אודות זכותו לסרב לכניסת המומחה למטרה כאמור או על אודות זכותו לחזור בו מהסכמתו. יודגש כי אין באמור כדי לגרוע מהאפשרות של המומחה החיצוני להתלוות לעובד מוסמך.

לסעיף קטן (ה)

מוצע לקבוע את התנאים למתן אישור לשמש מומחה חיצוני. על פי המוצע מנהל בכיר ברשות מוסמכת או מנהל בכיר במערך, לפי העניין (בסעיף מוצע זה – הגורם המאשר) יוכלו לתת אישור כאמור רק למי שהוא בעל ניסיון, ידע ומומחיות המתאימים לתפקיד, ושלא הורשע בעבירה שמפאת מהותה, חומרתה או נסיבותיה הוא אינו ראוי לשמש מומחה חיצוני ולא הוגש נגדו כתב אישום בעבירה כאמור.

לסעיף קטן (ו)

מוצע לקבוע תנאים שיבטיחו שהמומחה החיצוני לא יהיה מצוי בניגוד עניינים.

לסעיף קטן (ז)

מוצע לקבוע שהרואה את עצמו נפגע מפעולת מומחה חיצוני יהיה רשאי לפנות בתלונה מנומקת בכתב לגורם המאשר. כמו כן, מוצע לקבוע הסדר לעניין אופן בחינת התלונה בידי הגורם המאשר.

לסעיף קטן (ח)

מוצע לקבוע שדינו של המומחה החיצוני כדין עובדי מדינה לעניין ההוראות הנוגעות לעובדי הציבור בחוק העונשין וההוראות בחוק שירות הציבור (מתנות), התש"ם–1979.

[12] ס"ח התש"ם, עמ' 2.

(י) בסעיף זה –

"בן משפחה" – בן זוג, הורה, הורה הורה, בן או בת ובני זוגם, אח או אחות וילדיהם, חם, חמות, נכד או נכדה, לרבות קרוב כאמור שהוא שלוב (חורג);

"בעל עניין" – כהגדרתו בחוק ניירות ערך, התשכ"ח–1968[13];

"טיפול" – לרבות קבלת החלטה, העלאת נושא לדיון, נוכחות בדיון, השתתפות בדיון או בהצבעה, או עיסוק בנושא מחוץ לדיון;

"ניגוד עניינים" של מומחה חיצוני – ניגוד עניינים בין מילוי תפקידו לבין עניין אישי או תפקיד אחר, שלו או של קרובו;

"קרוב" – כל אחד מאלה:

(1) בן משפחה של מומחה חיצוני;

(2) אדם שלמומחה החיצוני יש עניין במצבו הכלכלי;

(3) תאגיד שמומחה חיצוני, בן משפחתו או אדם כאמור בפסקה (2) הם בעלי עניין בו;

(4) גוף שמומחה חיצוני, בן משפחתו או אדם כאמור בפסקה (2) הם מנהלים או עובדים אחראים בו.

סייג לתחולת חובות ולהפעלת סמכויות לפי החוק

52. (א) (1) ארגון חיוני ממגזר כאמור בפסקה (1) להגדרה מגזר שבסעיף 1, המנוי בתוספת השביעית (בסעיף זה – מגזר הכלול בתוספת השביעית), רשאי להגיש למנהל בכיר ברשות מוסמכת כאמור בפסקה (1) להגדרה "רשות מוסמכת" שבסעיף 1, תצהיר בנוסח שפרסם מנהל הרשות המוסמכת באתר האינטרנט של הרשות, בדבר ביצוע פעולות להגנת סייבר בפעילות הליבה של הארגון בהתאם לאמור בטור א' לתוספת השביעית לעניין אותו מגזר, ואם בטור ב' לתוספת מנוי לצידו מסמך – בצירוף המסמך; הגיש ארגון חיוני תצהיר כאמור, לא יחולו עליו החובות החלות על ארגון חיוני לפי חוק זה למעט החובות לפי סעיפים 9(א) ו־12, ולא יופעלו לגביו סמכויות בקשר לאותן חובות, לתקופה של שנתיים מיום הגשת התצהיר, ורשאי הוא לשוב ולהגיש תצהיר כאמור.

דברי הסבר

לסעיף קטן (ט)

מוצע לקבוע שמגבלות על עיסוקיו של המומחה החיצוני לאחר סיום ההתקשרות עימו ייקבעו במידת הצורך, בחוזה ההתקשרות עמו, ובכלל זה הוראות לעניין פרק הזמן שבו לא יעבוד המומחה חיצוני אצל גוף המתחרה בגוף שטיפל בענייניו כמומחה חיצוני ולא ייתן שירות לגוף כאמור או יקבל זכות או טובת הנאה ממנו.

יודגש כי הסעיף המוצע חל על הסתייעות של עובד במומחה חיצוני לשירות המדינה, ואינו חל, ואף לא נועד למנוע, הסתייעות בין גופי המדינה השונים. כמו כן, לפי הסעיף המוצע, מומחה חיצוני הוא אדם שאינו עובד המדינה. המונח "עובד המדינה" מוגדר בחוק המוצע כהגדרתו בסעיף 7 לפקודת הנזיקין [נוסח חדש], התשכ"ח–1968. הגדרה זו מתייחסת, בין השאר, לכל אדם הממלא מטעם המדינה תפקיד ציבורי על פי חיקוק, לרבות המשרתים בצבא ההגנה לישראל, במשטרת ישראל, בשירות בתי הסוהר ובארגוני הביטחון האחרים של המדינה. בהתאמה, הסתייעות בעובדי המדינה אינה כפופה להוראות הסעיף המוצע ואינה נשללת מכוחו. יובהר כי גם לאחר כניסת החוק לתוקף יוכלו גופי המדינה להעניק זה לזה סיוע הדדי בהפעלת סמכויותיהם לעניין הגנת סייבר לפי הנדרש ובכפוף לכל דין, ובאשר לצה"ל, גם לפי פקודות הצבא.

סעיף 52 ותוספת שביעית

לשם יצירת תמריץ להשקעה מתמשכת בהגנת סייבר בהתאם לסטנדרט בין־לאומי ומקצועי גבוה ולהפחתת נטל האסדרה על ארגונים המוכיחים יכולת הגנת סייבר גבוהה, מוצע לעגן בחוק תשתית שתאפשר לגורם המאסדר להפעיל, במקרים המתאימים במגזר, מנגנון של פטור ממרבית החובות הקבועות בחוק המוצע, שיינתן לארגונים שיוכיחו השקעה מתמשכת בהגנת סייבר כאמור, וזאת, בין

[13] ס"ח התשכ"ח, עמ' 234.

(2) הוראות פסקה (1) יחולו על ארגון חיוני למערכת הביטחון הנמנה עם מגזר הכלול בתוספת השביעית, בשינויים המחויבים, ובשינוי זה: הסמכות הנתונה למנהל בכיר ברשות מוסמכת ולמנהל הרשות המוסמכת תהיה נתונה למנהל בכיר במלמ"ב ולראש מלמ"ב, בהתאמה.

(ב) ספק שירותים דיגיטליים ושירותי אחסון חיוני ארגון חיוני, רשאי להגיש למנהל בכיר ברשות מוסמכת תצהיר בנוסח שפרסם ראש הרשות המוסמכת באתר האינטרנט של הרשות, בדבר יישום הנחיות הגנת סייבר בפעילות הליבה של הארגון, ואם מתקיים האמור בסעיף 14 כפי שהוחל בסעיף 16(א)(2) לגבי תקיפה נגד הספק או באמצעותו – בשירותים שנגדם בוצעה התקיפה, הכול בהתאם לאמור בטור א' לתוספת השביעית לעניין מגזר השירותים הדיגיטליים ושירותי האחסון, ואם בטור ב' לצידו מנוי מסמך – בצירוף המסמך; הגיש הספק תצהיר כאמור, לא יחולו עליו החובות לפי סעיף 14, כפי שהוחל לגביו בסעיף 16(א)(2), ולא יופעלו לגביו סמכויות בקשר לאותן חובות, למשך שנתיים מיום ההגשה, ורשאי הוא לשוב ולהגיש תצהיר כאמור.

(ג) גורם מאסדר, לאחר התייעצות עם ראש מערך הסייבר הלאומי, רשאי להוסיף לטור א' לתוספת השביעית מגזר שהוא אמון על אסדרת תחום הגנת הסייבר בו, והוראות, אם מצא כי ביצוע פעולות להגנת סייבר בהתאם לאותן הוראות בפעילות הליבה של ארגונים חיוניים במגזר, יש בו כדי להבטיח רמת הגנת סייבר מספקת לשם החלת הוראות סעיף זה על ארגונים חיוניים כאמור, בשים לב למאפייני הפעילות הייחודיים להם, ורשאי הוא, לאחר התייעצות כאמור, להוסיף מסמך לטור ב' לתוספת השביעית.

דברי הסבר

השאר, לאחר בחינת המאפיינים הייחודיים של ארגונים במגזר, אופי הפעילות בו, סוגי הארגונים, סיכוני הסייבר ורמת הבשלות למנגנון כאמור במגזר.

לסעיף קטן (א)

מוצע לאפשר לארגון חיוני ממגזר המנוי בתוספת הראשונה לחוק המוצע, אשר מנוי גם בתוספת השביעית לחוק המוצע, להגיש למנהל בכיר ברשות מוסמכת תצהיר בדבר ביצוע פעולות להגנת סייבר בפעילות הליבה של הארגון, בהתאם לאמור בטור א' לתוספת השביעית לעניין המגזר שהוא נמנה עימו, ואם בטור ב' לאותה תוספת מנוי בצידו מסמך – בצירוף המסמך. ארגון חיוני שהגיש תצהיר כאמור, לא יחולו עליו החובות החלות על ארגון חיוני לפי החוק המוצע למעט החובה הכללית לעמוד ברמת הגנה לפי סעיף 9(א) לחוק המוצע והחובה לדווח על תקיפת סייבר משמעותית לפי סעיף 12 לחוק המוצע, ולא יופעלו לגביו סמכויות בקשר לאותן חובות כל עוד התצהיר בתוקף.

התצהיר יוגש בנוסח שפרסם מנהל הרשות המוסמכת באתר האינטרנט של הרשות, ויעמוד בתוקפו לתקופה של שנתיים החל מיום מסירתו, כל עוד לא הוגש תצהיר נוסף.

על פי המוצע, הוראות אלה יחולו גם על ארגון חיוני למערכת הביטחון, אם הוא נמנה עם מגזר הכלול בתוספת השביעית, וזאת בשינויים המחויבים וכן בשינוי זה: הסמכות הנתונה למנהל בכיר ברשות מוסמכת ולמנהל הרשות המוסמכת תהיה נתונה למנהל בכיר במלמ"ב ולראש מלמ"ב, בהתאמה.

לסעיף קטן (ב)

מוצע לקבוע כי גם ספק שירותים דיגיטליים ושירותי אחסון, שאינו ארגון חיוני, יוכל להגיש למנהל בכיר ברשות מוסמכת תצהיר כאמור לעיל לעניין המגזר שבו הוא פועל (מגזר השירותים הדיגיטליים ושירותי האחסון), ואם נקבע לפי סעיף 14 לחוק המוצע כפי שהוחל בסעיף 16(א)(2) לאותו חוק, שמתרחשת או שיש חשש ממשי שעומדת להתרחש תקיפת סייבר חמורה נגד הספק או באמצעותו – תצהיר כאמור בהתייחס לשירותים שנגדם בוצעה התקיפה. הגיש הספק תצהיר כאמור, לא יחולו עליו הוראות סעיף 14 לחוק המוצע, כפי שהוחל לגביו כאמור, כלומר לא יינתנו לו הוראות להתמודדות עם תקיפה חמורה לפי אותו סעיף, ולא יופעלו לגביו סמכויות בקשר לאותן חובות, כל עוד התצהיר בתוקף. התצהיר יעמוד בתוקפו לתקופה של שנתיים החל מיום מסירת התצהיר, כל עוד לא הוגש תצהיר נוסף.

יובהר שהארגון המצהיר נדרש לעמוד בהצהרתו למשך כל תקופת תוקף התצהיר. כמו כן, הגשת תצהיר לא תעצור בדיעבד הליכי פיקוח או הליכים להטלת עיצום כספי, לפי פרקים ו' או ז' לחוק המוצע, שהחלו טרם הגשת התצהיר על ידי הארגון.

בשלב זה מוצע לקבוע בתוספת השביעית, ביחס למגזר השירותים הדיגיטליים ושירותי האחסון, תקנים או שילובים של תקנים, אשר עמידה בהם מקנה הגנת סייבר ברמה הגבוהה הנדרשת לצורך מתן הפטור המוצע מתחולת הוראות החוק המוצע. נוסף על כך, מוצע להקנות,

קבלה אגבית של מידע מתקשורת בין מחשבים

53. קבלת מידע מתקשורת בין מחשבים אגב פעולה להגנת סייבר בחומר מחשב לפי חוק זה, לא תיחשב להאזנת סתר לפי חוק האזנת סתר.

דיווח

54. (א) ראש מערך הסייבר הלאומי יציג לוועדת השרים לענייני ביטחון לאומי ולוועדת החוץ והביטחון של הכנסת, אחת לשנה, דוח על רמת הגנת הסייבר הלאומית ועל הפעולות שנקט המערך לחיזוק החוסן הלאומי בהיבטי הגנת הסייבר ולקידום ההתמודדות עם תקיפות סייבר, בשנה החולפת.

(ב) מערך הסייבר הלאומי ידווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, אחת לשנה, על כל אלה:

(1) מספר הארגונים החיוניים שגורם מאסדר קבע שיראו אותם לעניין חוק זה כארגון חיוני אף על פי שלא מתקיימים בהם התנאים לכך, כאמור בסעיף 8(ב)(1), או מספר הארגונים שגורם מאסדר קבע שלא יראו אותם כארגון חיוני אף על פי שהתקיימו לגביהם התנאים לכך, כאמור בסעיף 8(ב)(2), בחלוקה למגזרים, והנימוק לקביעה כאמור;

(2) מספר ההוראות שניתנו לפי סעיף 11, ולגבי כל הוראה שניתנה כאמור – מהות ההוראה שניתנה וסוג הארגון שלו ניתנה.

(ג) מלמ"ב ידווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, אחת לשנה, על מספר ההוראות שניתנו לפי סעיף 11 כפי שהוחל בסעיף 21, ומהותה של כל הוראה שניתנה כאמור.

(ד) דיווחים לפי סעיף זה יהיו חסויים ופרסומם אסור.

דברי הסבר

בסעיף קטן (ג), סמכות לגורם מאסדר, לאחר התייעצות עם ראש מערך הסייבר הלאומי, להוסיף לתוספת השביעית מגזר המנוי בתוספת הראשונה (ואינו מנוי עדיין בתוספת השביעית), וכן הוראות לעניין אופן ביצוע פעולות להגנת סייבר (ובכלל זה תקנים), ומסמך, אם מצא כי יש בביצוע פעולות להגנת סייבר בפעילות הליבה של ארגונים חיוניים במגזר, בהתאם לאותן הוראות, כדי להבטיח רמת הגנת סייבר מספקת, בשים לב למאפייני הפעילות הייחודיים של ארגונים באותו מגזר.

סעיף 53 מוצע להבהיר שקבלת מידע אגבית מתקשורת בין מחשבים אגב פעולה להגנת סייבר בחומר מחשב לפי חוק זה, לא תיחשב להאזנת סתר לפי חוק האזנת סתר, התשל"ט–1979.

סעיף 54 מוצע לקבוע בסעיף קטן (א) שראש מערך הסייבר הלאומי יציג לוועדת השרים לענייני ביטחון לאומי ולוועדת החוץ והביטחון של הכנסת, אחת לשנה, דוח על רמת הגנת הסייבר הלאומית ועל הפעולות שנקט המערך לחיזוק החוסן הלאומי בהיבטי הגנת הסייבר ולקידום ההתמודדות עם תקיפות סייבר בשנה החולפת.

כדי להבטיח פיקוח פנים־ממשלתי ופיקוח פרלמנטרי על אופן יישום חוק זה, מוצע לקבוע בסעיף קטן (ב), שמערך הסייבר הלאומי ידווח לוועדת החוץ והביטחון של הכנסת וליועץ המשפטי לממשלה, אחת לשנה, על מספר הארגונים החיוניים שגורם מאסדר קבע שיראו אותם לעניין חוק זה כארגון חיוני אף על פי שלא מתקיימים בהם התנאים לכך, כאמור בסעיף 8(ב)(1) לחוק המוצע, או מספר הארגונים שגורם מאסדר קבע שלא יראו אותם כארגון חיוני אף על פי שהתקיימו לגביהם התנאים לכך, כאמור בסעיף 8(ב)(2) לחוק המוצע, בחלוקה למגזרים, והנימוק לקביעה כאמור. דיווח זה יגובש על בסיס הנתונים שיועברו מהרשות המוסמכת לפי הוראות החוק.

נוסף על כך, מוצע כי מערך הסייבר הלאומי ידווח על מספר ההוראות שניתנו לפי סעיף 11 לחוק המוצע ולגבי כל הוראה שניתנה כאמור – מהות ההוראה וסוג הארגון שלו ניתנה.

עוד מוצע כי דיווח דומה לעניין סעיף 11 לחוק המוצע שהופעל בידי ראש מלמ"ב בהתאם להוראות סעיף 21 לחוק המוצע, יימסר על ידי מלמ"ב.

עוד מוצע לקבוע שהדיווחים לפי סעיף זה יהיו חסויים ופרסומם אסור.

פעולות להגנת סייבר לפי חוזה

55. אין בהוראות חוק זה כדי לגרוע מהאפשרות של גוף המנוי בסעיף 2(א) לחוק חובת המכרזים, התשנ"ב–1992[14], או של רשות מקומית, לבצע או לדרוש מאחר לבצע, פעולות שעניינן הגנת סייבר מכוח חוזה כמשמעותו באותו סעיף, לרבות פעולות לשם בקרה על קיום החוזה, ובכלל זה דרישה לקבלת מידע ומסמכים וכניסה למקום.

שמירת דינים

56. (א) הוראות חוק זה באות להוסיף על הוראות כל דין אחר, ובכלל זה חוק שירות הביטחון הכללי, התשס"ב–2002[15], ולא לגרוע מהן.

(ב) בלי לגרוע מהוראות סעיף קטן (א), הוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר שנקבעה בהחלטת הממשלה או בהוראת מינהל, ואולם במקרה של סתירה יגברו הוראות חוק זה.

תיקון התוספת הראשונה והתוספת השנייה

57. (א) ראש הממשלה, לאחר שהובאה לפניו המלצת ראש מערך הסייבר הלאומי, בהתייעצות עם שר האוצר ובאישור ועדת החוץ והביטחון של הכנסת, רשאי, בצו, לשנות את התוספת הראשונה, ובלבד –

(1) ששינוי כאמור של פרט המנוי בה ייעשה גם בהתייעצות עם הגורם המאסדר המנוי באותו פרט;

(2) ששינוי כאמור שעניינו הוספת פרט ובכלל זה תחום פעילות במשק, ייעשה גם בהתייעצות עם הגורם האמון על האסדרה של אותו תחום.

(ב) ראש הממשלה רשאי לשנות את התוספת השנייה, בצו, באופן האמור בסעיף קטן (א) רישה וכן בהתייעצות עם השר הממונה על הרשות המוסמכת המנויה בטור ב' לאותה תוספת.

דברי הסבר

סעיף 55 גופים שונים, ציבוריים ופרטיים, עורכים התקשרויות הכוללות, בין השאר, הוראות בנושא הגנת סייבר. התקשרויות אלה כפופות לדיני החוזים הכלליים ולהוראות כל דין. בשים לב לכך שהחוק המוצע מקנה לגופים שלטוניים מסוימים סמכויות מפורשות לבצע, או לדרוש מאחר לבצע, פעולות שעניינן הגנת סייבר, מוצע להבהיר, למען הסר ספק, כי החוק המוצע אינו גורע מהאפשרות של גופים המחזיקים בסמכויות שלטוניות לבצע, או לדרוש מאחר לבצע, גם פעולות שעניינן הגנת סייבר מכוח חוזים שאותם גופים עורכים. הכוונה לחוזים כאמור בסעיף 2(א) לחוק חובת המכרזים, התשנ"ב–1992 – חוזה לביצוע עסקה בטובין או במקרקעין, או לביצוע עבודה, או לרכישת שירותים.

הבהרה זו מתייחסת לגופים המפעילים סמכויות שלטוניות וכפופים לעיקרון חוקיות המינהל, שלפיו רשות שלטונית רשאית להפעיל סמכויות שלטוניות רק מכוח הסמכה מפורשת בדין. עוד יובהה, כי אין בחוק זה כדי לגרוע מהאפשרות של כל גורם לקבוע בהסכם חובה לעמידה ברמת הגנת סייבר מחמירה מזו הקבועה בחוק המוצע. לצד זאת, כמובן שבמקרה של סתירה בין הדרישות שבחוק המוצע לדרישות שבהסכם (למשל, כאשר הסכם יתיימר לקבוע הוראות מקילות יותר מאלה הקבועות בחוק) – הוראות החוק המוצע יגברו.

סעיף 56 החוק המוצע נועד לשפר את הגנת הסייבר הלאומית, ולשפר את רמת החוסן הלאומית בסייבר של ישראל, בין השאר, באמצעות יצירת רמת הגנה בסיסית אחידה בארגונים חיוניים במגזרים חיוניים שונים. במקביל, אין כוונה לפגוע בהסדרים קיימים הנוגעים לתחום הגנת הסייבר אלא רק להוסיף עליהם. בהתאם, מוצע להבהיר שהוראות החוק המוצע באות להוסיף על הוראות כל דין אחר, ובכלל זה על הוראות חוק שירות הביטחון הכללי ולא לגרוע מהן. בכלל זאת, אין בחוק זה או בהוראות מכוחו כדי לגרוע מחובת ארגון להבטיח בהתאם לכל דין רמת הגנת סייבר ראויה לפעילות הארגון.

עוד מוצע להבהיר שהוראות החוק המוצע באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר שנקבעה בהחלטות ממשלה, ובכלל זאת החלטות ממשלה 2443 ו־2444, והוראת מינהל, ואולם במקרה של סתירה יגברו הוראות החוק המוצע.

סעיף 57 מתוך הבנה שאיומים במרחב הסייבר והסיכונים בעבור המגזרים השונים משתנים, ומתוך הרצון לשמר גמישות והתאמה לצרכים במקרים הנדרשים, מוצע לקבוע שראש הממשלה, לאחר שהובאה לפניו המלצת ראש מערך הסייבר הלאומי, וכן בהיוועצות עם שר האוצר, ובאישור ועדת החוץ והביטחון של הכנסת, יהיה רשאי, בצו, לשנות את התוספת הראשונה והתוספת השנייה לחוק המוצע, היינו לשנות את המגזרים הנכללים בתוספת הראשונה, הרשות המוסמכת בכל מגזר, מנהל הרשות

[14] ס"ח התשנ"ב, עמ' 114.

[15] ס"ח התשס"ב, עמ' 179.

תקנות

58. ראש הממשלה ממונה על ביצועו של חוק זה, והוא רשאי להתקין תקנות לביצועו.

תיקון חוק בתי משפט לעניינים מינהליים

59. בחוק בתי משפט לענינים מינהליים, התש"ס–2000[16], בתוספת הראשונה בסופה יבוא:

"69. החלטה לפי חוק להגנת הסייבר הלאומית, התשפ"ו–2026, למעט החלטת הממשלה."

תיקון חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה)

60. בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), התשפ"ד–2023[17], בסעיף 12, במקום "עד יום כ"ג בשבט התשפ"ז (31 בינואר 2027)" יבוא "עד המועד האמור בסעיף 61(ב) לחוק הגנת הסייבר הלאומית, התשפ"ו–2026".

תחולה ותחילה

61. (א) תחילתו של חוק זה 3 חודשים מיום פרסומו.

(ב) על אף האמור בסעיף קטן (א), תחילתם של סעיפים 9(ב) עד (ו), 12, 14, 16 ו־18, 12 חודשים מיום פרסומו של חוק זה.

דברי הסבר

המוסמכת והגורם המאסדר, או להוסיף על האמור בה. מוצע לקבוע כי שינוי כאמור ביחס לפרט המנוי בתוספת הראשונה ייעשה גם בהתייעצות עם הגורם המאסדר המנוי באותו פרט, וכן כי שינוי כאמור שעניינו הוספת פרט לתוספת הראשונה, ובכלל זה תחום פעילות במשק, ייעשה גם בהתייעצות עם הגורם האמון על האסדרה של אותו התחום. כמו כן מוצע כי שינוי התוספת השנייה, יעשה גם בהתייעצות עם השר הממונה על הרשות המוסמכת המנויה באותה תוספת.

סעיף 58 מוצע לקבוע שראש הממשלה, השר האמון על מערך הסייבר הלאומי, ממונה על ביצועו של חוק זה, והוא רשאי להתקין תקנות לביצועו.

סעיף 59 כדי לאפשר ביקורת שיפוטית ונגישות לערכאות ביחס להחלטות לפי החוק, מוצע לתקן את התוספת הראשונה לחוק בתי משפט לעניינים מינהליים, התש"ס–2000, ולהסמיך את בית המשפט לעניינים מינהליים לדון בעתירות בעניין החלטות לפי החוק המוצע, למעט החלטות ממשלה.

סעיף 60 חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), התשפ"ד–2023, חוקק כהוראת שעה כדי לתת מענה לצורך הדחוף להתמודדות לאומית עם תקיפות סייבר במגזר האמור. הוראות החוק המוצע מבקשות לקבוע סדורות לגבי הגנת הסייבר, לרבות ביחס למגזר השירותים הדיגיטליים ושירותי האחסון. בשים לב לאמור, מוצע לקבוע כי הוראת השעה תעמוד בתוקפה עד למועד הכניסה לתוקף של כלל הוראות החוק הרלוונטיות לאותו מגזר.

סעיף 61 במטרה לתת למשק, ובייחוד לארגונים חיוניים, פרק זמן שיאפשר להם להיערך ולבצע את ההתאמות הנדרשות בארגון לצורך עמידה בהוראות החוק המוצע, מוצע לקבוע לו תחילה נדחית. ככלל, מוצע לקבוע שהחוק המוצע ייכנס לתוקף 3 חודשים לאחר יום פרסומו (סעיף קטן (א)).

עם זאת, לעניין הוראות מסוימות מוצעת דחייה נוספת של הכניסה לתוקף, במקביל לעמידה בתוקף של הוראת השעה. כך, על פי המוצע, הוראות לעניין החובה לעמוד ברמת הגנת סייבר בסיסית לפי סעיף 9(ב) עד (ו) לחוק המוצע, חובת הדיווח על תקיפה משמעותית לפי סעיף 12 לחוק המוצע, והאפשרות למתן הוראות לארגון חיוני או לספק שירותים דיגיטליים לפעול להתמודדות עם תקיפת סייבר חמורה בהתאם לסעיפים 14, 16 ו־18 לחוק המוצע, לרבות אותן הוראות כפי שהוחלו בסעיפים 21 ו־22 לחוק המוצע, ייכנסו לתוקף רק לאחר 12 חודשים מיום פרסומו של החוק המוצע.

[16] ס"ח התש"ס, עמ' 190; התשפ"ו, עמ' 562.

[17] ס"ח התשפ"ד, עמ' 410; התשפ"ו, עמ' 264.

תוספת ראשונה

(סעיף 1, ההגדרות "גורם מאסדר", "מגזר", "מנהל הרשות המוסמכת" ו"רשות מוסמכת")

	טור א' תחום פעילות במשק	טור ב' רשות מוסמכת	טור ג' מנהל הרשות המוסמכת	טור ד' גורם מאסדר
1.	תקשורת	משרד התקשורת	מנכ"ל משרד התקשורת	שר התקשורת
2.	אנרגיה	משרד האנרגיה והתשתיות	מנכ"ל משרד האנרגיה והתשתיות	שר האנרגיה והתשתיות
3.	מים וביוב	הרשות הממשלתית למים ולביוב	מנהל הרשות הממשלתית למים ולביוב	שר האנרגיה והתשתיות
4.	בריאות	משרד הבריאות	מנכ"ל משרד הבריאות	שר הבריאות
5.	כימיקלים, רעלים וחומרים מסוכנים	המשרד להגנת הסביבה	מנכ"ל המשרד להגנת הסביבה	השר להגנת הסביבה
6.	תחבורה	משרד התחבורה והבטיחות בדרכים	מנכ"ל משרד התחבורה והבטיחות בדרכים	שר התחבורה והבטיחות בדרכים
7.	הרשויות המקומיות	משרד הפנים	מנכ"ל משרד הפנים	שר הפנים
8.	מזון ואספקת מוצרים ושירותים חיוניים	משרד הכלכלה והתעשייה	מנכ"ל משרד הכלכלה והתעשייה	שר הכלכלה והתעשייה
9.	שירותים דיגיטליים ושירותי אחסון	מערך הסייבר הלאומי	ראש מערך הסייבר הלאומי	ראש הממשלה
10.	חקלאות	משרד החקלאות וביטחון המזון	מנכ"ל משרד החקלאות וביטחון המזון	שר החקלאות וביטחון המזון

תוספת שנייה

(סעיף 1, ההגדרות "מגזר", "מנהל הרשות המוסמכת" ו"רשות מוסמכת")

	טור א' תחום פעילות	טור ב' רשות מוסמכת	טור ג' מנהל הרשות המוסמכת
1.	פעילות משרדי ממשלה, למעט פעילות הנוגעת למידע מסווג ולמעט פעילות משרד ראש הממשלה ומשרד החוץ ופעילות בתי חולים ממשלתיים; לעניין זה, "משרד ראש הממשלה ומשרד החוץ" – למעט יחידות הסמך שלהם	מערך הדיגיטל הלאומי	ראש מערך הדיגיטל הלאומי

תוספת שלישית

(סעיף 8(א))

טור א׳ מגזר	טור ב׳ תת־מגזר	טור ג׳ התנאי
1. תקשורת		הוא ספק מורשה כהגדרתו בחוק התקשורת (בזק ושידורים), התשמ״ב–1982[18] (בפרט זה – חוק התקשורת), שיש לו לכל הפחות 200,000 מנויים; לעניין זה, ״מנוי״ – כהגדרתו בחוק התקשורת
2. אנרגיה	(1) חשמל	מתקיים לגביו אחד מאלה: (1) הוא ארגון שבבעלותו או בשליטתו הישירה או העקיפה מיתקנים, המשמשים לייצור חשמל, או אגירת חשמל בגודל חיבור לרשת העולה על 100 מגה־ואט AC ויותר; (2) הוא ארגון המנהל או בעל יכולת ניהול מרכזי של מיתקנים לייצור חשמל או אגירת חשמל, בסך חיבור לרשת העולה 100 MW AC ויותר, שולט או בעל יכולת שליטה על פעילות במיתקנים כאמור ומבצע בקרה, או בעל יכולת לבצע בקרה על הפעילות
	(2) גז טבעי	הוא בעל רישיון חלוקה כהגדרתו בחוק משק הגז הטבעי, התשס״ב–2002[19], או בעל רישיון ספק גז טבעי דחוס לפי סעיף 9 לחוק הגז (בטיחות ורישוי), התשמ״ט–1989[20]
	(3) דלק וגפ״מ	מתקיים לגביו אחד מאלה, לפי העניין: (1) לעניין ארגון הפועל בתחום הגפ״מ - הוא ספק גז כהגדרתו בחוק הגז הפחמימני המעובה, התשפ״א–2020[21], אשר רוכש מבתי זיקוק גפ״מ בכמות שנתית של 20,000 טונות או יותר או מייבא גפ״מ בכמות שנתית כאמור; (2) לעניין ארגון הפועל בתחום הדלק – ארגון הרוכש בנזין, סולר וקרוסין במסופי דלק בכמות שנתית של 200,000 קוב או יותר
3. מים וביוב		מתקיים לגביו אחד מאלה: (1) הוא חברה כהגדרתה בחוק תאגידי מים וביוב, התשס״א–2001[22], שיש לה מעל 500,000 צרכנים; (2) הוא מיתקן טיפול בשפכים שהיקף השפכים המטופלים בו עולה על 100 מיליון מטרים מעוקבים בשנה; (3) הוא מיתקן התפלה שכמות המים המותפלים שהוא מפיק עולה על 50 מיליון מטרים מעוקבים בשנה
4. בריאות		מתקיים לגביו אחד מאלה: (1) הוא בית חולים ציבורי כללי כהגדרתו בחוק התחשבנות בין בתי חולים ציבוריים כלליים לקופות חולים (תקצוב לאומי), התשפ״ב–2021[23]; (2) הוא קופת חולים כהגדרתה בחוק ביטוח בריאות ממלכתי, התשנ״ד–1994[24]

[18] ס״ח התשמ״ב, עמ׳ 218.
[19] ס״ח התשס״ב, עמ׳ 55.
[20] ס״ח התשמ״ט, עמ׳ 108.
[21] ס״ח התשפ״א, עמ׳ 146.
[22] ס״ח התשס״א, עמ׳ 454.
[23] ס״ח התשפ״ב, עמ׳ 20.
[24] ס״ח התשנ״ד, עמ׳ 156.

טור א׳ מגזר	טור ב׳ תת־מגזר	טור ג׳ התנאי
5. כימיקלים, רעלים וחומרים מסוכנים		הוא מפעל חיוני, כהגדרתו בחוק שירות עבודה בשעת־חירום, התשכ״ז–1967[25], וכמו כן הוא אחד מאלה: (1) מפעל לטיפול, סילוק או השבה של פסולת מסוכנת לרבות קרקע מזוהמת, כאמור בפרט 5.1 לתוספת השלישית לחוק החומרים המסוכנים, התשנ״ג–1993[26] (בפרט זה – התוספת השלישית); (2) מטמנה, למעט מטמנה לפסולת אינרטית כאמור בפרט 5.4 לתוספת השלישית; (3) הוא עוסק בפעילות של אחסון זמני של פסולת מסוכנת לפני העברתה לטיפול או לסילוק כמפורט בפרטים 5.1, 5.4, 5.6 ו־5.7 למעט אחסון זמני, לפני איסוף, באתר שבו נוצרה, כאמור בפרט 5.5 לתוספת השלישית
6. תחבורה	(1) תחבורה ציבורית יבשתית	מתקיים לגביו אחד מאלה: (1) הוא מפעיל תחבורה ציבורית המסיע יותר מ־14 מיליון נוסעים בשנה או שבבעלותו 1,000 כלי רכב ציבוריים או יותר; (2) הוא בעל היתר להפעלת מסילת ברזל מקומית לפי סימן ה׳ בפרק ד׳1 לפקודת מסילות הברזל [נוסח חדש], התשל״ב–1972[27]; (3) הוא בעל היתר הפעלה של רכב עצמאי כהגדרתו בסעיף 16ד לפקודת התעבורה או מפעיל רכבל כהגדרתו בצו פיקוח על מחירי מצרכים ושירותים (דמי נסיעה ברכבת וברכבל), התשפ״ב–2022[28].
	(2) תחבורה אווירית	מתקיים לגביו אחד מאלה: (1) הוא מפעיל אווירי שבידו רישיון הפעלה אווירית שניתן לפי הפרק השלושה עשר לתקנות הטיס (הפעלת כלי טיס וכללי טיסה), התשמ״ב–1981[29]; (2) הוא מכון בדק הנותן שירותים למפעיל אווירי כאמור בפרט משנה (א); (3) הוא בעל רישיון להפעלת יחידת נת״א כהגדרתה בחוק הטיס, התשע״א–2011[30], הנותנת שירותי נת״א כהגדרתם באותו חוק לכלי טיס בלתי מאוישים
	(3) תחבורה ימית	מתקיים לגביו אחד מאלה: (1) הוא מוביל לישראל וממנה בדרך הים סחורות שמשקלן הכולל מהווה 20% לפחות ממשקל כלל המטענים שמובלים לישראל וממנה בדרך הים במהלך השנה הקלנדרית שקדמה למועד הבדיקה; (2) הוא חברת נמל או תאגיד מורשה כהגדרתם בחוק רשות הספנות והנמלים, התשס״ד–2004[31]

[25] ס״ח התשכ״ז, עמ׳ 86.
[26] ס״ח התשנ״ג, עמ׳ 28.
[27] ק״ת התשע״ב, עמ׳ 1588.
[28] ק״ת התשפ״ב, עמ׳ 2742.
[29] ק״ת התשפ״ה, עמ׳ 354.
[30] ס״ח התשע״א, עמ׳ 830.
[31] ס״ח התשס״ד, עמ׳ 456.

טור א׳ מגזר	טור ב׳ תת־מגזר	טור ג׳ התנאי
	(4) תשתיות לניהול תחבורה	מתקיים לגביו אחד מאלה: (1) הוא חברה ממשלתית או תאגיד שהורשו על ידי הממשלה לניהול דרך או רשת דרכים בין־עירוניות או תאגיד שקיבל זיכיון מהמדינה לניהול דרך או רשת דרכים בין־עירוניות; (2) הוא חברה ממשלתית שהוכרה כזרוע ביצוע של משרד התחבורה; (3) הוא מרכז ניהול תנועה מטרופוליני (ת״א, ירושלים, חיפה, ב״ש)
7. הרשויות המקומיות		רשות מקומית שלה 90,000 תושבים רשומים או יותר
8. מזון ואספקת מוצרים ושירותים חיוניים		מתקיים לגביו אחד מאלה: (1) הוא מחסן חירום ייעודי לאחסון מוצרי מזון חיוניים שקבעה הרשות העליונה למזון הפועלת במינהל החירום במשרד הכלכלה; (2) הוא תאגיד שהוא ספק גדול כהגדרתו בחוק קידום התחרות בענפי המזון והפארם, התשע״ד–2014[32] (להלן – חוק קידום התחרות בענפי המזון), ואשר נתח השוק שלו במכירת מוצרי מזון לצריכה ביתית בישראל שווה או עולה על 4%; (3) הוא תאגיד שהוא קמעונאי גדול כהגדרתו בחוק קידום התחרות בענפי המזון, אשר נתח השוק שלו בקמעונאות מזון לצרכן בישראל שווה או עולה על 4%
9. שירותים דיגיטליים ושירותי אחסון		הוא ספק שירותים דיגיטליים או שירותי אחסון, שמתקיים לגביו אחד מאלה: (1) מתקיימים לגביו כל אלה: (א) הוא מעמיד לרשות אחרים מיתקן רשת המאפשר חיבור גומלין בין שתי רשתות אינטרנט עצמאיות או יותר, לשם העברת תעבורת אינטרנט ביניהן (ספק נקודת חילוף אינטרנט (IXP)); (ב) הוקנתה לו סיומת של כתובת אינטרנט והוא אחראי לניהול אותה סיומת, לרבות רישום שמות מתחם (Domains) והפעלה טכנית של אותה סיומת (מנהל מרשם TLD); (ג) הוא מוסמך להחכיר שמות מתחם (Domains) לציבור הרחב ולנהל את רישומם מול המרשם (רשם שמות מתחם (Domain Registrar). (ד) הוא ספק DNS המספק שירותי ניתוב שמות מתחם לרשת האינטרנט, ובכלל זה שירותי ניתוב רקורסיביים למשתמשים (Recursive DNS) או שירותי ניתוב שמות סמכותיים (Authoritative DNS) בעבור צדדים שלישיים, והוא אינו מפעיל שרתי שמות מתחם שורשיים (Root Domains); (ה) שירות אמון אלקטרוני (Trust Service) שמאפשר יצירה או אימות של רשומות אלקטרוניות, ובכלל זה חתימות אלקטרוניות, חותמות אלקטרוניות, חותמות זמן אלקטרוניות, או תעודות לאימות אתרים, וכן מסירת רשומה אלקטרונית, או שימור חתימות או חותמות אלקטרוניות

[32] ס״ח התשע״ד, עמ׳ 438.

טור א׳ מגזר	טור ב׳ תת־מגזר	טור ג׳ התנאי
		(2) מתקיימים לגביו כל אלה:
		(א) מתקיים לגביו אחד לפחות מהתנאים שלהלן:
		(1) מחזור העסקאות השנתי שלו ממכירות בישראל עולה על 40 מיליון שקלים חדשים;
		(2) הוא מספק למשרדי ממשלה, ליחידות סמך או לגוף מונחה שירותים דיגיטליים או שירותי אחסון מהסוג המנוי בפרט משנה (ב); ובלבד שלספק חשבונות של מינהלן (Administrator) או שהוא בעל הרשאה לגישה מועדפת (Privileged Access) לנכסי הסייבר של המשרד הממשלתי, יחידת הסמך או הגוף המונחה;
		(ב) הוא מספק אחד מאלה לפחות:
		(1) שירות דיגיטלי המאפשר למקבל השירות ניהול עצמאי על פי דרישה (on–demand) וגישה רחבה מרחוק למאגר גמיש וניתן להרחבה (scalabel and elastic) של משאבי מחשוב הניתנים לשיתוף, לרבות כאשר משאבים אלה מפוזרים על פני כמה מיקומים גאוגרפיים (שירות מחשוב ענן (Cloud Computing);
		(2) שירות מרכז נתונים (Data Center) ושירות אירוח (Hosting), הכולל החזקה, הפעלה או ניהול של מיתקן המיועד לאירוח, חיבור ותפעול מרכזי של ציוד, טכנולוגיית מידע ותקשורת או טכנולוגיית רשת, המאפשרים אחסון, עיבוד או העברת נתונים, ובכלל זה שירותי אחסון של אתרי אינטרנט, שירותי אחסון של מדיה וגיבוי פיזי או לוגי, וכן החזקה הפעלה או ניהול של מיתקן המיועד לאספקת חשמל ולבקרת סביבה בהתאם לדרישות התפעוליות של הציוד;
		(3) שירות רשת אספקת תוכן (Content Delivery Network – CDN), המספק, בשם ספקי תוכן ומפעילי שירותים, רשת של שרתים מפוזרים גיאוגרפית לשם הבטחת זמינות גבוהה, נגישות או אספקה מהירה של תוכן ושירותים דיגיטליים למשתמשי אינטרנט;
		(4) שירות מנוהל (MSP) הכולל התקנה, ניהול, תפעול או תחזוקה, באופן פעיל ומתמשך, באתר הלקוח או מרחוק, של מוצרי טכנולוגיית מידע ותקשורת, רשתות, תשתיות מחשוב, יישומים או מערכות מידע אחרות;
		(5) שירות אבטחת סייבר מנוהל (MSSP) הכולל ניהול סיכוני סייבר של הלקוח, כולם או חלקם, לרבות ניטור וזיהוי שוטף של סיכונים כאמור, תגובה להם או ייעוץ שוטף לגביהם, וכן אספקת מודיעין על סיכוני סייבר.
10. חקלאות		הוא קבלן מורשה לשיווק לפי תקנות המועצה לענף הלול (ייצור ושיווק) (כללים בדבר הסמכת קבלנים מורשים לשיווק ביצים, בשר עוף וחומר רביה), התשנ״ה–1994[33], שהגיש את הבקשה להסמכה לפי תקנה 2(1) לתקנות האמורות, המשווק 35 אחוזים או יותר מביצי המאכל המיוצרות בישראל

[33] ק״ת התשנ״ה, עמ׳ 292.

תוספת רביעית

(סעיף 9(ב)(1))

חלק א': דרישות רמת הגנת סייבר

(1) דרישות שעניינן מדיניות לניתוח סיכונים והגנה על נכסי סייבר, כמפורט להלן:

(א) זיהוי ומיפוי נכסי הסייבר, ובכלל זה זיהוי ומיפוי שוטפים, של נכסי הסייבר (Cyber Assets), ובהם המחשבים והרשתות, תוכנות ומערכות מידע, מערכות תפעוליות, מוצרים דיגיטליים והאמצעים המחוברים אליהם (בתוספת זו ובתוספת השישית – נכסי סייבר), וכן זיהוי ומיפוי שוטפים של המשתמשים, התהליכים הארגוניים והשירותים המרכזיים (לרבות שירותים מקוונים), העושים שימוש בנכסי הסייבר ושל המידע והנתונים המאוחסנים, מעובדים ומועברים באמצעות נכסי הסייבר (בתוספת זו ובתוספת השישית – המידע והנתונים), ובחינה מקיפה, אחת לשנה קלנדרית (בתוספת זו – שנה) לפחות, של המיפוי שבוצע;

(ב) איתור וזיהוי סיכוני הסייבר, ובכלל זה ביצוע ותיעוד של בדיקות ומבדקי אבטחה תקופתיים בנכסי הסייבר, המידע והנתונים, לשם זיהוי סיכוני סייבר ופגיעויות (Vulnerabilities) בהם ורמת ההגנה שלהם, וכן איתור תצורות טכנולוגיות מסכנות וכשלים העלולים לפגוע בפעילות הארגון, בנכסיו, בתהליכי הליבה שלו או במשתמשיו ובגורמים המקושרים אליו או לשבש את פעילות הארגון ושירותי הליבה שלו;

(ג) ביצוע הערכה שיטתית ומתמשכת של סיכוני סייבר בנכסי הסייבר, במידע ובנתונים ובתהליכי הליבה של הארגון, ובכלל זה הערכה תקופתית, שתיבחן אחת לשנה לפחות, וכן בעת הטמעה או שינוי מהותי, לרבות סיום שימוש בנכס סייבר או בשירות שיכולה להיות לו השפעה על הארגון ותיעודם במסמך הערכת סיכונים ארגוני;

(ד) הכנת תוכנית עבודה לטיפול בסיכוני סייבר, לשם הגנת נכסי הסייבר, המידע והנתונים של הארגון, והבטחת רציפות השירותים שלו ותהליכי הליבה המתבססים עליהם (להלן – תוכנית העבודה לטיפול בסיכוני הסייבר), בהתחשב בהערכת הסיכונים, גודל הארגון, שרשרת הערך של הארגון, שקילת שיקולי תפעול, אישורה, אחת לשנה, בידי הנהלת הארגון, וכן יישום ועדכון של תוכנית העבודה, קיום בקרה על יישומה ותיעוד פעולות היישום והבקרה;

(ה) דרישה לקיום מסגרת ארגונית להגנת סייבר שתהיה אחראית על קידום ויישום תוכנית העבודה כאמור בפרט משנה (ד) ופרט (4)(ד) ותיעוד שוטף של הפעילויות המבוצעות במסגרת הארגונית האמורה;

(ו) הגנת תשתיות רשת, ובכלל זה קביעה, אישור בידי הנהלת הארגון והטמעה של נהלים להגנת רשתות המחשבים בארגון, באמצעות פריסה ויישום של אמצעים ומערכות הגנה לניטור ולאבטחת תשתיות תקשורת הנתונים הפנימית והחיצונית של הארגון, לרבות הקישורים (WAN – Wide Area Network) והממשקים (Interfaces) הנכנסים לארגון והיוצאים ממנו, וכן החיבורים (LAN – Local Area Network or WAN) בין יחידותיו השונות בהתאם להערכת הסיכון כאמור בפרטים (1)(ג) ו־(4)(ב), להגנה על נכסי הסייבר, המידע והנתונים, והשירותים והתהליכים הארגוניים;

(ז) דרישה להפרדת סביבות בארגון, פילוח רשתות (segmentation), והפרדת המתחמים (Domains) והשירותים השונים ברשת הארגון, והפרדה של רשתות, מתחמים ושירותים של צדדים שלישיים המופעלים בארגון או מקושרים אליו, הכול בהתאם לתוצאות הערכת הסיכונים ותוכנית העבודה כאמור בפרטים (1)(ד) ו־(4)(ד) לטיפול בסיכוני סייבר;

(ח) הגנה מפני תוכנה זדונית או עוינת, ובכלל זה פיתוח, אישור בידי הנהלת הארגון והטמעה של נהלים לאיתור, ניטור ומניעת הפעלתן של תוכנות כאמור, באמצעות אמצעים ומערכות הגנה המותאמים לסיכוני הסייבר, להגנה על נכסי הסייבר, המידע והנתונים, והשירותים והתהליכים הארגוניים;

(ט) עבודה בתצורה מאובטחת (Secured Configuration), ובכלל זה פיתוח, אישור בידי הנהלת הארגון והטמעה של נהלים לקביעה, תיעוד, יישום וניטור של תצורות עבודה מאובטחות בנכסי הסייבר ושל המידע והנתונים, לרבות צמצום פעולתה של תוכנה לא מורשית בהתאם למסמכי הערכת הסיכונים לפי פרטים (1)(ג) ו־(4)(ב) (בתוספת זו – מסמכי הערכת הסיכונים);

(י) פיתוח, אישור בידי הנהלת הארגון והטמעה של נהלים לניהול מחשבים שהם אמצעים ניידים, לשימוש בהם ולניטור פעילותם, הכול באמצעות אמצעים או מערכות הגנה מתאימים ובהתאם למסמכי הערכת הסיכונים;

(יא) פיתוח, אישור בידי הנהלת הארגון והטמעה של נהלים לניהול ושימוש באמצעי אחסון נשלפים ומדיה נתיקה במיתקני הארגון או במקומות אחרים, בהתאם למסמכי הערכת הסיכונים, הכול באמצעות אמצעים או מערכות הגנה מתאימים;

(2) דרישות שעניינן היערכות לאירועי סייבר (Cyber Events) ובכלל זה תקיפות סייבר (להלן – אירוע סייבר) והתמודדות עימם, כמפורט להלן:

(א) קביעה ויישום של מנגנון ארגוני לדיווח על אירועי סייבר המאפשר דיווח על אירועים חשודים על ידי מנהלים, עובדים, ספקים ולקוחות;

(ב) פיתוח, אישור ויישום של תוכנית ארגונית המותאמת למסמכי הערכת הסיכונים בידי הנהלת הארגון לניטור טכנולוגי קבוע להגנת סייבר, ובכלל זה קיומה של מסגרת לניטור של נכסי הסייבר במידע ובנתונים הארגוניים והפעלת כלים לניטור טכנולוגי, לרבות כלים לרישום פעילויות ביומנים וניתוחן, הכול לצורך איתור חריגות ואירועים חשודים;

(ג) סקירת יומנים (LOGS), ניהול ערכי סף להתרעה, ניתוח אירועים והפצת התרעות לגורמים הנוגעים בדבר במקרים המתאימים, בין השאר באמצעות קביעת נהלים בעניין ויישום אמצעים הנדרשים לכך, הכול באופן קבוע ומתמשך;

(ד) שמירת יומנים (LOGS) ובכלל זה תחזוקה, גיבוי והגנה עליהם לתקופת שמירה מוגדרת ומאושרת מראש, לרבות מניעת גישה או שינוי בלתי מורשים;

(ה) דרישה לקביעה ויישום של תהליך ארגוני לסיווג אירועי סייבר (Cyber Events) והתרעות, ובכלל זה קביעת קריטריונים להערכה וסיווג של חריגות שהתגלו באמצעות דיווח, ניטור או סקירת יומנים, לצורך תגובה מהירה ומבוקרת;

(ו) קביעה ויישום של תהליך ארגוני לזיהוי והכרזה על תקיפת סייבר (Cyber Incident), על בסיס הסיווג כאמור בפרט משנה (ה);

(ז) הכנה, אישור בידי הנהלת הארגון אחת לשנה והטמעה של תוכנית ארגונית לטיפול באירועי סייבר, הכוללת נהלים, תפקידים ותחומי אחריות לשם איתור והתמודדות עם אירועי סייבר, מניעתם, בלימתם, התאוששות מהם, תיעודם ודיווח עליהם;

(ח) מינוי והכשרה מראש של צוות ניהול משברי סייבר בארגון, אשר יופעל במהלך משבר שנגרם כתוצאה מתקיפת סייבר, לצורך ניהול ההתמודדות עם התקיפה, ובכלל זה קבלת החלטות ותיאום הפעולות להתמודדות עם התקיפה;

(ט) היערכות ארגונית מוקדמת להפעלה, בזמן אמת, של מסגרת מקצועית להתערבות ותגובה (IR – Incident Response) ייעודית לאירועי סייבר ושל אמצעים מתאימים;

(י) גיבוש ואישור בידי הנהלת הארגון של תוכניות ונהלים לתקשורת עם צוות ניהול משברי סייבר כאמור בפרט משנה (ח), עם מסגרת התערבות ותגובה כאמור בפרט משנה (ט) ועם רשויות וגורמים פנימיים וחיצוניים הנוגעים לעניין;

(יא) ביצוע, אחת לשנה לפחות, של תרגיל להנהלת הארגון ולצוות ניהול משברי סייבר, המשלב תגובה לאירועי סייבר, המשכיות עסקית (Business Continuity) והתאוששות מאסון (Disaster Recovery), ותיעודו;

(יב) ביצוע, אחת לשנה לפחות, של הכשרה ואימון מעשי או קיומה של הוכחת כשירות למסגרת מקצועית להתערבות ותגובה ייעודית לאירועי סייבר, לצוות הגנת הסייבר הארגוני ולצוות מערכות המידע והטכנולוגיות, לצורך התמודדות עם אירועי סייבר, ותיעודם;

(יג) קיום ותיעוד של תהליך הפקת לקחים, למידה ושיפור מאירועי סייבר בארגון;

(3) דרישות שעניינן רציפות תפקודית והמשכיות השירות, כמפורט להלן:

(א) ביצוע ניתוח השפעה עסקית (Business Impact Analysis – BIA), אחת לשנתיים לפחות, הכולל ביצוע הערכה של ההשפעה האפשרית של תקיפת סייבר על פעילות הארגון, ובהתאם לכך מיפוי, קביעה ואישור של יעדי רציפות תפקודית לנכסי הסייבר, המידע והנתונים והשירותים המרכזיים התלויים בהם;

(ב) הכנה, אישור בידי הנהלת הארגון, עדכון, מזמן לזמן, ויישום של תוכנית להמשכיות עסקית (BCP), המבוססת על הערכות סיכוני הסייבר כאמור בפרט (1)(ג) ובהתאם לניתוח ההשפעה העסקית כאמור בפרט משנה (א) (בפרט זה – הערכת הסיכונים וניתוח ההשפעה העסקית), הכוללת בין השאר יעדים, תפקידים, אנשי קשר, ערוצי תקשורת ותנאים להפעלת התוכנית או לסיום הפעלתה;

(ג) הכנה, אישור בידי הנהלת הארגון, עדכון אחת לשנתיים ויישום של תוכנית להתאוששות מאסון (DRP – Disaster Recovery Plan) בהיבטי הגנת סייבר, לצורך התאוששות מאירועי סייבר והשבת פעילותם של נכסי סייבר, מידע, נתונים ושירותים, המבוססת על הערכת הסיכונים ובהתאמה לתוכנית להמשכיות עסקית (BCP) וכוללת יעדי התאוששות (RTO/RPO), סדרי עדיפויות ורצף פעולות להתאוששות, תוכניות לשחזור ושיקום ומשאבים נדרשים, לרבות כוח אדם, משאבי מחשוב, תקשורת ותשתיות פיזיות;

(ד) הכנה, אישור בידי הנהלת הארגון, יישום ועדכון, באופן שוטף, של תוכנית גיבויים ארגונית למידע, נתונים ותצורות (Configurations), המבוססת על הערכת הסיכונים וניתוח ההשפעה העסקית, ועל תוכנית ההמשכיות העסקית והרציפות התפקודית, לצורך קידום ההתאוששות מאירועי סייבר, וכוללת, בין השאר, יעדי התאוששות מוגדרים והבטחת שלמות עותקי הגיבוי, אחסון מאובטח של גיבויים, בקרות גישה הולמות, נוהלי שחזור, ניהול גרסאות גיבוי ותקופות שמירת מידע ונתונים, וכן ביצוע, אחת לשנה לפחות, של בדיקות שחזור (Restorer) תקופתיות לעותקי הגיבוי, ותיעודן;

(ה) ביצוע, אחת לשנתיים לפחות, של תדריך לעובדי הארגון בישראל, המנויים בתוכנית לפי פרטי משנה (ב) ו־(ד), בעניין תוכנית ההמשכיות העסקית והתוכנית להתאוששות מאסון, ותיעודו;

(4) דרישות שעניינן הגנת סייבר בשרשרת האספקה, כמפורט להלן:

(א) ביצוע מיפוי שוטף של שרשרת האספקה של הארגון, ובכלל זה זיהוי הספקים, השירותים והמוצרים המסופקים על ידם והתלות של הארגון בהם, וכן זיהוי הסיכונים הנובעים מהם והשפעתם האפשרית על רמת הגנת הסייבר בנכסי הסייבר, במידע ובנתונים ובתהליכים הארגוניים;

(ב) ביצוע, באופן שוטף, של הערכת סיכונים לשם קביעת רמת הסיכון הנובעת משרשרת האספקה, והשפעתה על נכסי הסייבר, המידע והנתונים, התהליכים הארגוניים והשירותים של הארגון ותיעודה במסמך הערכת סיכונים בשרשרת האספקה;

(ג) מתן שאלון הגנת סייבר למילוי בידי ספקים או קבלת מידע על אודות רמת הגנת הסייבר אצל ספקים על ידי גורם מקצועי חיצוני ובלתי תלוי, לצורך הערכה של רמת הסיכון הכרוכה בהתקשרות עם הספק והשפעתה על רמת הגנת הסייבר בנכסי הסייבר, במידע ובנתונים ובתהליכים הארגוניים, לפני כל התקשרות עם ספק או חידושה, ואחת ל־24 חודשים ממועד ההתקשרות או החידוש;

(ד) הכנת תוכנית לטיפול בסיכוני סייבר שמקורם בשרשרת האספקה, לשם הגנת נכסי הסייבר, המידע והנתונים של הארגון, והבטחת רציפות השירותים שלו ותהליכי הליבה המתבססים עליהם, באמצעות נקיטת אמצעים או הפעלת מערכות הגנה, בחינתה, אחת לשנה, בידי הנהלת הארגון, עדכונה מזמן לזמן, ויישומה, וכן קיום בקרה על יישומה ותיעוד פעולות היישום והבקרה, הכול בהתאם לסיכוני הסייבר בשרשרת האספקה, להערכת הסיכונים שבוצעה לגביהם, למאפייני הארגון ולרמת ההגנה הקיימת בארגון;

(ה) הכללה, בחוזים עם ספקים, קבלני משנה ונותני שירותים, של הוראות שעניינן הגנת סייבר בעניינים נוספים על העניינים המנויים בפרט משנה (ג), אשר בהתאם למאפייני הספק מגדירות דרישות להגנה על נכסי הסייבר של הארגון והמידע והנתונים שלו, וכוללות, בין השאר, חובות דיווח על אירועים, מנגנוני ביקורת, טיפול בפגיעויות וסיכוני סייבר, דרישות הנוגעות להתקשרות עם ספקי משנה, ודרישות הנוגעות לסיום ההתקשרות;

(5) דרישות שעניינן פיתוח מאובטח, תחזוקה של מערכות וטיפול בחשיפות (Exposure) ובפגיעויות (Vulnerabilities), כמפורט להלן:

(א) לגבי ארגון העוסק בפיתוח תוכנה או חומרה – קביעה, אישור בידי הנהלת הארגון ועדכון, אחת לשנתיים, של נוהל לפיתוח מאובטח של מערכות ויישומים בארגון, בעצמו או באמצעות מיקור חוץ, אשר יכלול, בין השאר, הוראות להגנת סייבר בסביבת הפיתוח ובתהליך הפיתוח, וכן יישום עקרונות תכנון וקידוד מאובטחים, ויישום תהליכי בדיקות בנכסי הסייבר שבפיתוח, ולהגנה על נתוני הבדיקות וניהולם;

(ב) קביעה, בחינה בידי הנהלת הארגון, עדכון, אחת לשנה, והטמעה של הנחיות ונהלים מקצועיים לתהליכים של ניהול שינויים (Change Management), ניהול טלאי אבטחה (Security Patch Management), תחזוקה ועדכוני מערכת בנכסי הסייבר בארגון (Updates), לרבות עדכוני תוכנה וקושחה (Firmware), הכול בתוך פרק זמן סביר ממועד פרסום השינוי, הטלאי או העדכון, וכן ביצוע בקרה של הנהלת הארגון על יישום התהליך ותיעודה;

(ג) קביעה, אישור בידי הנהלת הארגון, עדכון באופן שוטף, והטמעה של הנחיות ונהלים מקצועיים לניהול פגיעויות (Vulnerability Management) וניהול חשיפות (Exposure Management) בנכסי הסייבר, המידע והנתונים של הארגון, אשר מסדירים בין השאר פעילות רציפה לאיתור פגיעויות ותצורות (Configurations) מסכנות בנכסי הסייבר של הארגון, המידע והנתונים שלו, ולאיתור חשיפות, בהתאם למסמכי הערכת הסיכונים, בין השאר, באמצעות ביצוע בדיקות טכנולוגיות ותהליכיות על נכסי הסייבר, המידע והנתונים של הארגון, עדכון רמת הסיכון בנכסי הסייבר בעקבות הפעילויות האמורות, ונקיטת אמצעים מתאימים לטיפול בפגיעויות, בתצורות המסכנות או בחשיפות שאותרו בתוך פרק זמן סביר בהתאם למאפייני הארגון, ובכלל זה ביצוע בקרה על הטיפול;

(6) דרישות שעניינן מדיניות ונהלים להערכת התועלת של הפעילות הארגונית להגנת סייבר, כמפורט להלן:

(א) גיבוש, אישור בידי הנהלת הארגון, עדכון שנתי ויישום של מדיניות ארגונית כוללת להגנה על נכסי הסייבר, המידע והנתונים, בארגון או בשרשרת האספקה שלו, הכוללת קביעת עקרונות יסוד להגנת סייבר, תחומי אחריות, תוכניות ונהלים הנוגעים להגנת סייבר, כמפורט בתוספת זו, וכן קביעת מנגנונים לפיקוח ובקרה על יישומם של אלה ותיעוד פעולת המנגנונים שנקבעו;

(ב) התאמה של מדיניות ונהלים ארגוניים מרכזיים, הקשורים למידע והנתונים, לשירותי הליבה של הארגון ולתהליכים הארגוניים, כך שיכללו התייחסות מתאימה להיבטי הגנת הסייבר;

(ג) מינוי מנהל הגנת סייבר ארגוני (Chief Information Security Officer – CISO), בעל ידע וניסיון מקצועי מתאימים, אשר ידווח ישירות למנהל הארגון, ויוקנו לו הסמכויות המתאימות למימוש המדיניות הארגונית האמורה בפרט משנה (א) ולניהול מערך הגנת הסייבר הארגוני, ובלבד שלא ימלא תפקיד נוסף בארגון אם מילוי התפקיד כאמור עלול להעמידו בחשש לניגוד עניינים במילוי תפקידו כמנהל הגנת סייבר ארגוני;

(ד) מינוי בעלי תפקידים נוספים שיעסקו בהגנת הסייבר וקביעת תחומי האחריות והסמכות שלהם, בידי הנהלת הארגון, בהתאם למאפייני הארגון ואופי פעילותו, בין השאר כמפורט בתוכנית העבודה לטיפול בסיכוני סייבר, בתוכנית הארגונית לטיפול באירועי סייבר, בתוכנית להמשכיות עסקית (BCP), בתוכנית להתאוששות מאסון (DRP) בהיבטי הגנת סייבר ובתוכנית לטיפול בסיכוני סייבר שמקורם בשרשרת האספקה, האמורות בפרטים (1)(ד), (2)(ז) ו־(3)(ב) ו־(ג), בהתאמה;

(ה) מינוי ועדת היגוי ארגונית להגנת סייבר, בראשות מנהל הארגון או דירקטור בארגון, שתתכנס פעמיים בשנה לפחות, תאשר את המדיניות הארגונית האמורה בפרט משנה (א) ובכלל זה את עקרונותיה, תדון בהערכת סיכוני הסייבר, בהתאם לתמונת המצב לגבי הגנת הסייבר בארגון, ותקבע סדר עדיפות לטיפול בהם, תקצה את המשאבים הנדרשים לכך, ותבצע מעקב אחר יישום התוכניות האמורות בפרט משנה (ד) ויעילותן, הכול על סמך הדיון שקיימה בהערכת סיכוני הסייבר כאמור;

(ו) הכנה על ידי הגורמים המקצועיים הרלוונטיים בארגון ואישור בידי הנהלת הארגון, אחת לשישה חודשים לפחות, של דוח על מצב הגנת הסייבר בארגון, הכולל, בין השאר, סקירת סיכוני סייבר בנכסי הסייבר, המידע והנתונים, והערכתם, סקירה של אירועי סייבר שקרו בארגון בתקופת הדוח והטיפול בהם, סקירה של פעולות שבוצעו לצמצום פגיעויות וחשיפות, מצב יישום תוכניות העבודה האמורות בפרט משנה (ד), רמת הכשירות הארגונית להתמודדות עם אירועי סייבר ולהבטחת הרציפות התפקודית בהתאם לסקירות האמורות, ומידת הציות של הארגון לחובות החלות עליו לפי דין ולהוראות תקן כאמור בחלק ב' לתוספת, שלפיו בחר הארגון, לפי סעיף 7(ב)(1), לקיים את הדרישות המנויות בתוספת זו;

(7) דרישות שעניינן היגיינת מחשב בסיסית והדרכות, כמפורט להלן:

(א) יישום תוכנית למניעת תקשוב צללים (Shadow IT), ובכלל זה גיבוש, אישור בידי ההנהלה ועדכון, מזמן לזמן, של נהלים ארגוניים בעניין שימוש בנכסי סייבר, המידע והנתונים השייכים לארגון או בעניין שימוש בנכסי סייבר, מידע ונתונים שאינם שייכים לארגון, שהשימוש בהם נעשה בבקרה של הארגון באמצעות נקיטת אמצעים והפעלת מערכות הגנה מתאימות, בהתאם למסמכי הערכת הסיכונים והחלת מנגנוני בקרה ואכיפה וביצוע הדרכות;

(ב) הכנה, אישור בידי הנהלת הארגון, עדכון, מזמן לזמן, ויישום של תוכנית שנתית להגברת מודעות לסיכוני סייבר, בהתאם למסמכי הערכת הסיכונים, וכן קיום הדרכות ותרגילים לעידוד התנהגות אחראית במרחב הסייבר להנהלה, לעובדים ולספקים, שתכליתם הקניית ידע וכלים לזיהוי אירועי סייבר ולהתמודדות עימם פעם בשנה לכל הפחות;

(ג) הכנה, אישור בידי הנהלת הארגון, עדכון, מזמן לזמן, ויישום של תוכנית שנתית להכשרה או תרגול מעשיים בתחום הגנת הסייבר לבעלי תפקידים רגישים בארגון, הכוללת הקניית ידע ומיומנויות לשימוש מאובטח במערכות ולמניעת אירועי סייבר הנובעים מפעילותם של בעלי תפקידים כאמור, וביצוע ההכשרה או התרגול כאמור אחת לשנה לפחות; לעניין זה, "בעלי תפקידים רגישים בארגון" - לרבות עובדים בעלי גישה מועדפת לנכסי סייבר, מידע ונתונים רגישים, מינהלנים (Administrators) או עובדים שתפקידם בארגון דורש מיומנויות מקצועיות מתקדמות בתחומי מחשוב וסייבר;

(8) דרישות שעניינן הצפנה והסתרה של נכסי סייבר, כמפורט להלן:

(א) קביעה, אישור בידי הנהלת הארגון, בחינה, אחת לשנתיים, והטמעה של נוהל לסיווג רמות הרגישות של נכסי הסייבר, המידע והנתונים בארגון, לרבות הסיווג הביטחוני שלהם, אם קיים בארגון, וכן דרישה לביצוע מיפוי בהתאם לנוהל כאמור, אחת לשנה לפחות, ולתיעודו;

(ב) גיבוש, אישור בידי הנהלת הארגון, עדכון, מזמן לזמן, ויישום של מדיניות, נהלים והנחיות מקצועיות לשמירה על הסודיות והמהימנות של המידע והנתונים בארגון, ולאימות המידע והנתונים, בהתאם לרגישות ולסיווג של נכסי הסייבר של הארגון כאמור בפרט משנה (א), זאת, בין השאר, באמצעות שימוש שוטף באמצעי הצפנה, תעודות אבטחה וחתימות דיגיטליות;

(ג) הצפנת המידע והנתונים, במעבר (In transit), מקצה לקצה, ובמנוחה (At rest), ובכלל זה הצפנת קבצים, מסדי נתונים ועותקי גיבוי, הכול באמצעות אמצעים, פרוטוקולים, אלגוריתמים ופתרונות הצפנה מקובלים, בהתאם לרמות הרגישות והסיווג של המידע והנתונים לפי המיפוי כאמור בפרט משנה (א), ובהתאם למדיניות ההצפנה, לנוהלי ההצפנה, כאמור בפרט משנה (ב) ולמסמכי הערכת הסיכונים;

(ד) קביעה, אישור בידי הנהלת הארגון, עדכון, מזמן לזמן, והטמעה של נהלים הנדרשים להפעלת תשתית טכנולוגית לניהול מפתחות הצפנה ותעודות אבטחה ככל שנדרש ובהתאם לאופי הארגון, הכוללים בין השאר, הוראות לעניין הפקה, אחסון, החלפה, אחזור והשמדה של חומר מחשב המשמש לקידוד הצפנה (חומר קריפטוגרפי), תוך הפרדה לוגית בין המידע והנתונים המוצפנים לבין אמצעי ניהול התשתית האמורה, וכן קביעת מנגנונים לפיקוח ובקרה על יישומם של הנהלים האמורים ולתיעוד פעולת המנגנונים שנקבעו;

(9) דרישות שעניינן בקרת גישה, ניהול נכסי סייבר והתייחסות לגורם האנושי:

(א) גיבוש, אישור בידי הנהלת הארגון, עדכון, אחת לשנה, ויישום של מדיניות ונהלים לבקרת גישה המבוססת על הסיכונים שזוהו כאמור בפרטים (1) ו־(4) ועל הרגישות והסיווג של נכסי הסייבר, המידע והנתונים כאמור בפרט (8), אשר קובעים רמות גישה והרשאה לנכסי הסייבר, המידע והנתונים, ומבטיחים יישום בפועל של עקרונות מקצועיים שעניינם מידור, הרשאת גישה מזערית (Least Privilege) והפרדת תפקידים (Segregation of Duties – SoD), באמצעות אמצעים ומערכות הגנה מתאימים ותהליכי בקרה ארגוניים, וכן קביעת מנגנונים לפיקוח ובקרה על יישומם של המדיניות והנהלים האמורים ותיעוד פעולת המנגנונים שנקבעו;

(ב) הטמעה ויישום טכנולוגי של אמצעי אימות מתקדמים, לרבות אימות רב־גורמי (Multi–Factor Authentication – MFA) בטכנולוגיה מקובלת, בכל גישה לנכס סייבר מרחוק, או בגישה לנכס סייבר המכיל מידע ונתונים רגישים או מסווגים או גישה לתהליכים רגישים, גישה לחשבונות של בעלי הרשאות מועדפות (Privileged Users) ומינהלנים (Administrative User), הכול בהתאם לסיכונים שזוהו כאמור בפרטים (1) ו־(4) ולרגישות והסיווג של נכסי הסייבר, המידע והנתונים, כאמור בפרט (8);

(ג) ניהול זהויות וגישה (IAM – Identity and Access Management), ובכלל זה כתיבה, אישור בידי הנהלת הארגון, עדכון, אחת לשנתיים, והטמעה של נהלים לניהול מחזור החיים של זהויות דיגיטליות, המבטיחים שיוך זהות ייחודית וחד־ערכית לכל משתמש ולכל נכס סייבר בהתאם ליכולות הטכניות שלו, ובהתאם למדיניות בקרת הגישה כאמור בפרט משנה (א), של הארגון, לרבות תהליכים הכוללים מתן גישה, הרשאות, ורישום ובקרה (Audit Trail) של הפעולות הקריטיות בהתאם למסמכי הערכת הסיכונים, וכן קביעת מנגנונים לפיקוח ובקרה על יישומם של הנהלים האמורים ותיעוד פעולת המנגנונים שנקבעו;

(ד) קביעה, אישור בידי הנהלת הארגון, עדכון, אחת לשנתיים, והטמעה של נהלים לאכיפה שוטפת של מדיניות בקרת הגישה, כאמור בפרט משנה (א), בכל הנוגע לחשבונות מועדפים, וכן שימוש באמצעי לניהול של חשבונות מועדפים (Management), חשבונות של מינהלנים (Administrators) וחשבונות רגישים אחרים בארגון;

(ה) קביעה, אישור בידי הנהלת הארגון, בחינה, אחת לשנה, והטמעה של נהלים לאבטחת מרכזי המחשבים (Data Centers) שבהם נמצאים נכסי סייבר, הכוללים הוראות לעניין אמצעים שיינקטו להגנה מפני חבלה ונזקים פיזיים לרבות נזקים סביבתיים, בקרת כניסה אליהם ובכלל זה ניהול מורשי כניסה ובהם ספקים, וניטור, בקרה ותיעוד רציפים של כניסות אליהם ופעילויות המבוצעות בהם, וכן ביצוע בקרה על יישומם של הנהלים האמורים ותיעודה;

(ו) קביעה, אישור בידי הנהלת הארגון, עדכון, אחת לשנתיים, והטמעה של נהלים לביצוע בדיקות רקע או מהימנות לעובדים בישראל, מנהלים בישראל ועובדי ספקים הפועלים מול הארגון בישראל, מזמן לזמן, בין השאר לפני קבלת גישה לנכסי הסייבר, המידע והנתונים, שיתבצעו בהתאם למסמכי הערכת סיכונים שזוהו כאמור בפרטים (1) ו־(4) ולרגישות והסיווג של נכסי הסייבר, המידע והנתונים, כאמור בפרט (8), וכן ביצוע בקרה על יישומם של הנהלים האמורים ותיעודה;

(ז) קביעה, אישור בידי הנהלת הארגון, עדכון, אחת לשנתיים, והטמעה של נהלים לניהול מחזור חיי העובד בהקשר של הגנת סייבר, הכוללים בין השאר הוראות לעניין הקצאה, שינוי או ביטול זהות, ניהול הרשאות וגישה בהתאם לתפקיד ולמדיניות בקרת הגישה, הפעלה או הסרה של אמצעי אימות, הדרכה ראשונית או תדריך פרידה, וקבלה או החזרה של נכסי סייבר וכן הוראות לעניין תיעוד כלל הפעילויות האמורות, וביצוע בקרה על יישום הנהלים, אחת לשנה לפחות.

חלק ב': תקינה

(1) תקן מספר ISO/IEC 27001 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת מידע, הגנת סייבר והגנת הפרטיות - מערכות ניהול אבטחת מידע – דרישות, שאושר על ידי הארגון והנציבות האמורים בחודש אוקטובר 2022, העומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; יחד עם תקן מספר ISO/IEC 27002 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת מידע, הגנת סייבר והגנת הפרטיות – מערכות ניהול אבטחת מידע – בקרות, שאושר על ידי הארגון והנציבות כאמור בחודש פברואר 2022, העומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן.

(2) תקן מספר ת"י 27001 בעניין מערכת ניהול אבטחת מידע, שאומץ על ידי מכון התקנים ביום ט' בשבט התשפ"ג (31 בינואר 2023) (בגרסתו העדכנית), העומד לעיון הציבור במכון התקנים, על עדכוניו מזמן לזמן; יחד עם תקן מספר ת"י 27002 בעניין אבטחת מידע, אבטחת סב"ר והגנה על הפרטיות – בקרות אבטחת מידע, שאומץ על ידי מכון התקנים ביום ט' בשבט התשפ"ג (31 בינואר 2023) (בגרסתו העדכנית), העומד לעיון הציבור במכון התקנים, על עדכוניו מזמן לזמן.

(3) תקן NIST Cybersecurity Framework (CSF) של המכון הלאומי לתקנים וטכנולוגיה של ארה"ב (NIST) בעניין בקרות אבטחה ופרטיות בעבור מערכות מידע וארגונים (במהדורתו השנייה), שאושר על ידי המכון האמור ביום י"ז באדר א' התשפ"ד (26 בפברואר 2024), העומד לעיון הציבור באתר האינטרנט של המכון האמור, על עדכוניו מזמן לזמן;

(4) תקן מספר NIST SP 800–53 של המכון הלאומי לתקנים וטכנולוגיה של ארה"ב (NIST) בעניין בקרות אבטחה ופרטיות בעבור מערכות מידע וארגונים (במהדורתו החמישית), קווי בסיס לבקרות הגנה להתמודדות ברמת השפעה בינונית או גבוהה (Moderate or High Impact), שאושר על ידי המכון האמור ביום ה' בתשרי התשפ"א (23 בספטמבר 2020), העומד לעיון הציבור באתר האינטרנט של המכון האמור, על עדכוניו מזמן לזמן.

תוספת חמישית

(סעיף 20(ז))

המספר המרבי של ארגונים שייקבעו כארגון חיוני למערכת הביטחון – 125

תוספת שישית

(סעיף 27(א) ו־(ב))

חלק א'

טור א' הדרישה שלא קוימה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
1. דרישה לביצוע זיהוי ומיפוי כמפורט בפרט (1)(א) לתוספת הרביעית, או לביצוע, אחת לשנה לפחות, של בחינה מקיפה של המיפוי שבוצע כאמור	640,000
2. דרישה לביצוע איתור וזיהוי של סיכוני סייבר, כמפורט בפרט (1)(ב) לתוספת הרביעית או לביצוע איתור של תצורות טכנולוגיות מסכנות וכשלים כמפורט באותו פרט	640,000
3. דרישה לביצוע הערכה שיטתית מתמשכת של סיכוני הסייבר בנכסי הסייבר, במידע, ובנתונים ובתהליכי הליבה של הארגון שתיבחן אחת לשנה לפחות, בעת ההטמעה או שינוי מהותי, לרבות סיום שימוש בנכס סייבר או בשירות, הכול, כמפורט בפרט (1)(ג) לתוספת הרביעית	640,000
4. דרישה להכנת תוכנית עבודה לטיפול בסיכוני הסייבר, לאישורה, ליישומה, לעדכונה, לקיום בקרה על יישומה, או לתיעוד פעולות היישום והבקרה, הכול כמפורט בפרט (1)(ד) לתוספת הרביעית	640,000
5. דרישה לקיום מסגרת ארגונית להגנת סייבר, לקידום או ליישום תוכנית העבודה כאמור בפרט (1)(ה) ובפרט (4)(ד) לתוספת הרביעית או תיעוד שוטף של הפעילויות המבוצעות במסגרת הארגונית האמורה כמפורט בפרט (1)(ה) לתוספת הרביעית	640,000
6. דרישה להגנת תשתיות רשת כמפורט בפרט (1)(ו) לתוספת הרביעית	640,000
7. דרישה להפרדת סביבות בארגון, פילוח רשתות (segmentation), או הפרדת המתחמים (Domains) והשירותים השונים ברשת הארגון, או הפרדה של רשתות, מתחמים ושירותים של צדדים שלישיים המופעלים בארגון או מקושרים אליו, כמפורט בפרט (1)(ז) לתוספת הרביעית	640,000
8. דרישה להגנה מפני תוכנה זדונית או עויינת כמפורט בפרט (1)(ח) לתוספת הרביעית	640,000
9. דרישה לעבודה בתצורה מאובטחת כמפורט בפרט (1)(ט) לתוספת הרביעית	640,000
10. דרישה לפיתוח, אישור בידי הנהלת הארגון או הטמעה של נהלים לניהול מחשבים שהם אמצעים ניידים, לשימוש בהם או לניטור פעילותם, כמפורט בפרט (1)(י) לתוספת הרביעית	640,000

טור א׳ הדרישה שלא קוימה	טור ב׳ סכום העיצום הכספי (בשקלים חדשים)
11. דרישה לפיתוח, אישור בידי הנהלת הארגון או הטמעה של נהלים לניהול ושימוש באמצעי אחסון נשלפים ומדיה נתיקה במיתקני הארגון או במקומות אחרים, כמפורט בפרט (1)(יא) לתוספת הרביעית	640,000
12. דרישה לקביעה ויישום של מנגנון ארגוני לדיווח על אירועי סייבר, כמפורט בפרט (2)(א) לתוספת הרביעית	640,000
13. פיתוח, אישור או יישום של תוכנית ארגונית המותאמת למסמכי הערכת הסיכונים בידי הנהלת הארגון לניטור טכנולוגי קבוע להגנת סייבר, כמפורט בפרט (2)(ב) לתוספת הרביעית	640,000
14. דרישה לסקירת יומנים, ניהול ערכי סף להתרעה, ניתוח אירועים להפצת התרעות לגורמים הנוגעים בדבר במקרים המתאימים, כמפורט בפרט (2)(ג) לתוספת הרביעית	640,000
15. דרישה לשמירת יומנים כמפורט בפרט (2)(ד) לתוספת הרביעית	640,000
16. דרישה לקביעה ויישום של תהליך ארגוני לסיווג אירועי סייבר והתרעות, כמפורט בפרט (2)(ה) לתוספת הרביעית	640,000
17. דרישה לקביעה וליישום של תהליך ארגוני לזיהוי והכרזה של תקיפת סייבר, כמפורט בפרט (2)(ו) לתוספת הרביעית	640,000
18. דרישה להכנה, לאישור בידי הנהלת הארגון אחת לשנה או להטמעה של תוכנית ארגונית לטיפול באירועי סייבר, כמפורט בפרט (2)(ז) לתוספת הרביעית	640,000
19. דרישה למינוי ולהכשרה מראש של צוות ניהול משברי סייבר בארגון, כמפורט בפרט (2)(ח) לתוספת הרביעית	640,000
20. דרישה להיערכות ארגונית מוקדמת להפעלה, בזמן אמת, של מסגרת מקצועית להתערבות ותגובה ייעודית לאירועי סייבר ושל אמצעים מתאימים, כמפורט בפרט (2)(ט) לתוספת הרביעית	640,000
21. דרישה לגיבוש ואישור, בידי הנהלת הארגון, של תוכניות ונהלים לתקשורת עם צוות ניהול משברי סייבר, עם מסגרת מקצועית להתערבות ותגובה ייעודית לאירועי סייבר ועם רשויות וגורמים פנימיים וחיצוניים הנוגעים לעניין, כאמור בפרט (2)(י) לתוספת הרביעית	640,000
22. דרישה לביצוע, אחת לשנה לפחות, של תרגיל להנהלת הארגון ולצוות ניהול משברי סייבר, כמפורט בפרט (2)(יא) לתוספת הרביעית	640,000
23. דרישה לביצוע, אחת לשנה לפחות, של הכשרה ואימון מעשי למסגרת מקצועית להתערבות ותגובה ייעודית לאירועי סייבר, לצוות הגנת הסייבר הארגוני ולצוות מערכות המידע והטכנולוגיות, ולתיעודם, כמפורט בפרט (2)(יב) לתוספת הרביעית	640,000
24. דרישה לקיום ולתיעוד של תהליך הפקת לקחים, למידה ושיפור מאירועי סייבר בארגון, כאמור בפרט (2)(יג) לתוספת הרביעית	320,000

טור א׳ הדרישה שלא קוימה	טור ב׳ סכום העיצום הכספי (בשקלים חדשים)
25. דרישה לביצוע ניתוח השפעה עסקית, כמפורט בפרט (3)(א) לתוספת הרביעית, אחת לשנתיים לפחות, ולביצוע של מיפוי, קביעה או אישור של יעדי רציפות תפקודית לנכסי הסייבר, המידע והנתונים והשירותים המרכזיים התלויים בהם, בהתאם לניתוח שבוצע כאמור	640,000
26. דרישה להכנה, לאישור בידי הנהלת הארגון, לעדכון, מזמן לזמן, או ליישום של תוכנית להמשכיות עסקית, כמפורט בפרט (3)(ב) לתוספת הרביעית	640,000
27. דרישה להכנה, לאישור בידי הנהלת הארגון, לעדכון אחת לשנתיים או ליישום של תוכנית להתאוששות מאסון (DRP) בהיבטי הגנת סייבר, לצורך התאוששות מאירועי סייבר והשבת פעילותם של נכסי סייבר, מידע, נתונים ושירותים, כמפורט בפרט (3)(ג) לתוספת הרביעית	640,000
28. דרישה להכנה, לאישור בידי הנהלת הארגון, ליישום או לעדכון, באופן שוטף של תוכנית גיבויים ארגונית למידע, נתונים ותצורות ועל תוכנית ההמשכיות העסקית והרציפות התפקודית, כמפורט בפרט (3)(ד) לתוספת הרביעית, וכן דרישה לביצוע, אחת לשנה לפחות, של בדיקות שחזור תקופתיות לעותקי הגיבוי ולתיעודן, כאמור באותו פרט	640,000
29. דרישה לביצוע, אחת לשנתיים לפחות, של תדריך לעובדי הארגון בישראל, המנויים בתוכנית לפי פרטים (3)(ב) ו־(3)(ד) לתוספת הרביעית, בעניין תוכנית ההמשכיות העסקית והתוכנית להתאוששות מאסון, ותיעודו, כאמור בפרט (3)(ה) לתוספת הרביעית	320,000
30. דרישה לביצוע מיפוי שוטף של שרשרת האספקה של הארגון, כמפורט בפרט (4)(א) לתוספת הרביעית	640,000
31. דרישה לביצוע, באופן שוטף, הערכת סיכונים לשם קביעת רמת הסיכון הנובעת משרשרת האספקה, והשפעתה על נכסי הסייבר, המידע והנתונים, התהליכים הארגוניים והשירותים של הארגון ותיעודה במסמך הערכת סיכונים בשרשרת האספקה, כאמור בפרט (4)(ב) לתוספת הרביעית	640,000
32. דרישה למתן שאלון הגנת סייבר למילוי בידי ספקים או קבלת מידע על אודות רמת הגנת הסייבר אצל ספקים על ידי גורם מקצועי חיצוני ובלתי תלוי, כמפורט בפרט (4)(ג) לתוספת הרביעית, לפני כל התקשרות עם ספק או חידושה, ואחת ל־24 חודשים ממועד ההתקשרות עם ספק או החידוש	320,000
33. דרישה להכנת תוכנית לטיפול בסיכוני סייבר שמקורם בשרשרת האספקה, כמפורט בפרט (4)(ד) לתוספת הרביעית, ודרישה לבחינתה, אחת לשנה, בידי הנהלת הארגון, לעדכונה מזמן לזמן, ליישומה, לקיום בקרה על יישומה או לתיעוד פעולות היישום והבקרה כמפורט באותו פרט	640,000
34. דרישה להכללה של הוראות שעניינן הגנת סייבר, כמפורט בפרט (4)(ה) לתוספת הרביעית, בחוזים עם ספקים, קבלני משנה ונותני שירותים	320,000

טור א׳ הדרישה שלא קוימה	טור ב׳ סכום העיצום הכספי (בשקלים חדשים)
35. דרישה מארגון העוסק בפיתוח תוכנה או חומרה – לקביעה, לאישור בידי הנהלת הארגון, או לעדכון, אחת לשנתיים, של נוהל לפיתוח מאובטח של מערכות ויישומים בארגון, כמפורט בפרט (5)(א) לתוספת הרביעית, ודרישה ליישום עקרונות תכנון וקידוד מאובטחים, ליישום תהליכי בדיקות בנכסי הסייבר שבפיתוח, או להגנה על נתוני הבדיקות וניהולם, כאמור באותו פרט	320,000
36. דרישה לקביעה, לבחינה בידי הנהלת הארגון, לעדכון, אחת לשנה, או להטמעה של הנחיות ונהלים מקצועיים לתהליכים של ניהול שינויים, ניהול טלאי אבטחה, תחזוקה ועדכוני מערכת בנכסי הסייבר בארגון, לרבות עדכוני תוכנה וקושחה, כמפורט בפרט (5)(ב) לתוספת הרביעית, ולביצוע בקרה בידי הנהלת הארגון על יישום התהליך ותיעוד הבקרה שבוצעה, כאמור באותו פרט	640,000
37. דרישה לקביעה, לאישור בידי הנהלת הארגון, לעדכון באופן שוטף, או להטמעה של הנחיות ונהלים מקצועיים לניהול פגיעויות וניהול חשיפות בנכסי הסייבר, המידע והנתונים של הארגון, כמפורט בפרט (5)(ג) לתוספת הרביעית, ודרישה לעדכון רמת הסיכון בנכסי הסייבר בעקבות הפעילויות האמורות, או נקיטת אמצעים מתאימים לטיפול בפגיעויות, בתצורות המסכנות או בחשיפות שאותרו כמפורט באותו פרט	640,000
38. דרישה לגיבוש, לאישור בידי הנהלת הארגון, לעדכון שנתי או ליישום של מדיניות ארגונית כוללת להגנת על נכסי הסייבר, המידע והנתונים בארגון או בשרשרת האספקה שלו, כמפורט בפרט (6)(א) לתוספת הרביעית, או דרישה לקביעת מנגנונים לפיקוח ובקרה על יישומם של אלה ולתיעוד פעולת המנגנונים שנקבעו, כאמור באותו פרט	640,000
39. דרישה להתאמה של מדיניות ונהלים ארגוניים מרכזיים, הקשורים למידע והנתונים, לשירותי הליבה של הארגון ולתהליכים הארגוניים, כך שיכללו התייחסות מתאימה להיבטי הגנת הסייבר, כאמור בפרט (6)(ב) לתוספת הרביעית	320,000
40. דרישה למינוי מנהל הגנת סייבר ארגוני, בעל ידע וניסיון מקצועי מתאימים, כמפורט בפרט (6)(ג) לתוספת הרביעית	640,000
41. דרישה למינוי בעלי תפקידים נוספים שיעסקו בהגנת סייבר ולקביעת תחומי האחריות והסמכות שלהם, בידי הנהלת הארגון, בהתאם למאפייני הארגון ואופי פעילותו, כמפורט בפרט (6)(ד) לתוספת הרביעית	320,000
42. דרישה למינוי ועדת היגוי ארגונית להגנת סייבר, בראשות מנהל הארגון או דירקטור בארגון, שתפעל באופן המפורט בפרט (6)(ה) לתוספת הרביעית	320,000
43. דרישה להכנה על ידי הגורמים המקצועיים הרלוונטיים בארגון ולאישור בידי הנהלת הארגון, אחת לשישה חודשים לפחות, של דוח על מצב הגנת הסייבר בארגון, כמפורט בפרט (6)(ו) לתוספת הרביעית	640,000

טור א׳ הדרישה שלא קוימה	טור ב׳ סכום העיצום הכספי (בשקלים חדשים)
44. דרישה ליישום תוכנית למניעת תקשוב צללים, ובכלל זה דרישה לגיבוש, לאישור בידי הנהלת הארגון, או לעדכון מזמן לזמן של נהלים ארגוניים כמפורט בפרט (7)(א) לתוספת הרביעית, או דרישה להחלת מנגנוני בקרה ואכיפה או ביצוע הדרכות, כאמור באותו פרט	640,000
45. דרישה להכנה, לאישור בידי הנהלת הארגון, לעדכון, מזמן לזמן או ליישום של תוכנית שנתית להגברת מודעות לסיכוני סייבר, בהתאם למסמכי הערכת הסיכונים, או דרישה לקיום הדרכות ותרגילים לעידוד התנהגות אחראית במרחב הסייבר, להנהלה, לעובדים ולספקים, פעם בשנה לכל הפחות, כמפורט בפרט (7)(ב) לתוספת הרביעית	320,000
46. דרישה להכנה, לאישור בידי הנהלת הארגון, לעדכון, מזמן לזמן, או ליישום של תוכנית שנתית להכשרה או תרגול מעשיים בתחום הגנת הסייבר לבעלי תפקידים רגישים בארגון, כמפורט בפרט (7)(ג) לתוספת הרביעית, ודרישה לביצוע ההכשרה או התרגול כאמור אחת לשנה לפחות, כאמור באותו פרט	320,000
47. דרישה לקביעה, לאישור בידי הנהלת הארגון, בחינה, אחת לשנתיים, או להטמעה של נוהל לסיווג רמות הרגישות של נכסי הסייבר, המידע והנתונים בארגון, לרבות הסיווג הביטחוני שלהם, אם קיים בארגון, או דרישה לביצוע מיפוי בהתאם לנוהל כאמור, אחת לשנה לפחות, ולתיעודו, כאמור בפרט (8)(א) לתוספת הרביעית	640,000
48. דרישה לגיבוש, לאישור בידי הנהלת הארגון, לעדכון, מזמן לזמן, או ליישום של מדיניות, נהלים והנחיות מקצועיות לשמירה על הסודיות והמהימנות של המידע והנתונים בארגון ולאימות המידע והנתונים בהתאם לרגישות ולסיווג של נכסי הסייבר של הארגון, כמפורט בפרט (8)(ב) לתוספת הרביעית	640,000
49. דרישה להצפנת המידע והנתונים במעבר, מקצה לקצה ובמנוחה, כמפורט בפרט (8)(ג) לתוספת הרביעית	640,000
50. דרישה לקביעה, לאישור בידי הנהלת הארגון, לעדכון, מזמן לזמן, או להטמעה של נהלים הנדרשים להפעלת תשתית טכנולוגית לניהול מפתחות הצפנה ותעודות אבטחה ככל שנדרש ובהתאם לאופי הארגון כמפורט בפרט (8)(ד) לתוספת הרביעית, וכן דרישה לקביעת מנגנונים לפיקוח ובקרה על יישומם של הנהלים האמורים או לתיעוד פעולת המנגנונים שנקבעו, כאמור באותו פרט	640,000
51. דרישה לגיבוש, לאישור בידי הנהלת הארגון, לעדכון, אחת לשנה, או ליישום של מדיניות ונהלים לבקרת גישה כמפורט בפרט (9)(א) לתוספת הרביעית, או דרישה לקביעת מנגנונים לפיקוח ובקרה על יישומם של המדיניות והנהלים האמורים ולתיעוד פעולת המנגנונים שנקבעו, כאמור באותו פרט	640,000
52. דרישה להטמעה ויישום טכנולוגי של אמצעי אימות מתקדמים, כמפורט בפרט (9)(ב) לתוספת הרביעית, בכל גישה כאמור באותו פרט ובאופן האמור בו	640,000

טור א׳ הדרישה שלא קוימה	טור ב׳ סכום העיצום הכספי (בשקלים חדשים)
53. דרישה לניהול זהויות וגישה, ובכלל זה דרישה לכתיבה, לאישור בידי הנהלת הארגון, לעדכון, אחת לשנתיים, או להטמעה של נהלים לניהול מחזור החיים של זהויות דיגיטלית, כמפורט בפרט (9)(ג) לתוספת הרביעית, או דרישה לקביעת מנגנונים לפיקוח ובקרה על יישומם של הנהלים האמורים ולתיעוד פעולת המנגנונים שנקבעו, כאמור באותו פרט	320,000
54. דרישה לקביעה, לאישור בידי הנהלת הארגון, לעדכון, אחת לשנתיים, או להטמעה של נהלים לאכיפה שוטפת של מדיניות בקרת הגישה, כמפורט בפרט 9(ד) לתוספת הרביעית, או דרישה לשימוש באמצעי לניהול חשבונות, כמפורט באותו פרט	640,000
55. דרישה לקביעה, לאישור בידי הנהלת הארגון, לבחינה, אחת לשנה, או להטמעה של נהלים לאבטחת מרכזי המחשבים שבהם נמצאים נכסי סייבר, כמפורט בפרט (9)(ה) לתוספת הרביעית, או דרישה לביצוע בקרה על יישומם של הנהלים האמורים ותיעודה, כאמור באותו פרט	320,000
56. דרישה לקביעה, לאישור בידי הנהלת הארגון, לעדכון, אחת לשנתיים, או להטמעה של נהלים לביצוע בדיקות רקע או מהימנות לעובדים בישראל, מנהלים בישראל או עובדי ספקים הפועלים מול הארגון בישראל, מזמן לזמן, כמפורט בפרט (9)(ו) לתוספת הרביעית, או דרישה לביצוע בקרה על יישומם של הנהלים האמורים ותיעודה, כאמור באותו פרט	320,000
57. דרישה לקביעה, לאישור בידי הנהלת הארגון, לעדכון, אחת לשנתיים, או להטמעה של נהלים לניהול מחזור חיי העובד בהקשר של הגנת סייבר, כמפורט בפרט (9)(ז) לתוספת הרביעית, וכן דרישה לביצוע בקרה על יישומם, אחת לשנה לפחות, כאמור באותו פרט	320,000

חלק ב׳

טור א׳ הדרישה שלא קוימה	טור ב׳ סכום העיצום הכספי (בשקלים חדשים)

תוספת שביעית

(סעיף 52)

טור א׳ הנחיות	טור ב׳ המסמך
לעניין מגזר השירותים הדיגיטליים ושירותי האחסון	
1. הארגון מיישם את הדרישות לצורך עמידה בתקן NIST SP 800–53 של המכון הלאומי לתקנים וטכנולוגיה של ארה״ב (NIST) בעניין בקרות אבטחה ופרטיות בעבור מערכות מידע וארגונים (NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (control baseline for (impact) Moderate or High), שאושר על ידי המכון האמור ועומד לעיון הציבור באתר המכון, על עדכוניו מזמן לזמן	אחד מאלה: (1) אישור על הימצאות הארגון ברשימת FedRAMP Marketplace המפורסמת באתר האינטרנט של Fedramp בסטטוס Authorized, בצירוף תצהיר מאת נושא משרה בארגון כמשמעותו בסעיף 49 (בתוספת זו – נושא משרה) לעניין הימצאות הארגון ברשימה כאמור; (2) אישור בדיקה מפורט (Assessment), המעיד על עמידת הארגון בדרישות תקן control baselines for Moderate or High impact NIST 800–53 בשירותי הליבה שלו, מטעם 3PAO (Third–Party Assessment Organization) בלתי תלוי והמוכר על ידי ה־American Association for Laboratory Accreditation (A2LA); בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בדרישות התקן בשירותי הליבה שלו כאמור; (3) אישור בדיקה מפורט (Assessment), המעיד על עמידת הארגון בדרישות תקן control baselines for Moderate or High impact NIST 800–53 בשירותי הליבה שלו, מטעם גוף בדיקות סייבר באיחוד האירופי, בלתי תלוי, העומד בתקן ISO/IEC 17020 והמוכר לעניין זה על ידי European co–operation for Accreditation; בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בדרישות התקן בשירותי הליבה שלו כאמור; (4) אישור בדיקה מפורט (Assessment), המעיד על עמידת הארגון בדרישות תקן control baselines for Moderate or High impact NIST 800–53 בשירותי הליבה שלו, מטעם גוף בדיקות סייבר ישראלי בלתי תלוי העומד בתקן ISO/IEC 17020 אשר הוסמך לעניין זה על ידי הרשות הלאומית להסמכת מעבדות שהוקמה לפי חוק הרשות הלאומית להסמכת מעבדות, התשנ״ז–1997[34] (להלן – הרשות להסמכת מעבדות); על הסמכה כאמור יחולו ההוראות לפי החוק, בשינויים המחויבים; הרשות להסמכת מעבדות תקבע כללים לעניין הסמכה של גופים כאמור בהסכמת מערך הסייבר הלאומי, בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בדרישות התקן בשירותי הליבה שלו כאמור

[34] ס״ח התשנ״ז, עמ׳ 156.

טור א׳ הנחיות	טור ב׳ המסמך
2. הארגון עומד בכל אלה:	
(1) הארגון עומד בדרישות לצורך עמידה באחד מתקני הליבה שלהלן:	כל אלה:
(א) תקן מספר ISO/IEC 27001 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת מידע, הגנת סייבר והגנת הפרטיות – מערכות ניהול אבטחת מידע – דרישות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27001 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי בעניין אבטחת מידע, הגנת סייבר והגנת הפרטיות – מערכות ניהול אבטחת מידע – דרישות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	(1) תעודת הסמכה בתוקף, שניתנה או חודשה לארגון במהלך 36 החודשים האחרונים, על ידי גוף הסמכה (Certification Body) בעל אקרדיטציה מתאימה מטעם פורום האקרדיטציה הבין־לאומי (בתוספת זו – IAF); (2) אישור על ישימות התקן (SoA – Statement of Applicability) המפרטת את כלל בקרות ה־Annex A הרלוונטיות לתחומי פעילות הארגון בלא אי־התאמות קריטיות (Major Non–conformities) פתוחות;
(ב) תקן מספר IEC/ISA 62443 של האיגוד הבין־לאומי לאוטומציה (ISA) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת מערכות אוטומציה ובקרה תעשייתית, שאושר על ידי האיגוד והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הנציבות האמורה, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 62443 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי בעניין אבטחת מערכות אוטומציה ובקרה תעשייתית, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של אותו מכון, על עדכוניו מזמן לזמן	כל אלה: (1) תעודת הסמכה בתוקף, שניתנה או חודשה לארגון או לשירות ליבה במהלך 36 החודשים האחרונים על ידי גוף הסמכה (Certification Body) בעל אקרדיטציה מתאימה מטעם ה־IECEE או ה־IAF, המעידה על עמידה בחלקי התקן הרלוונטיים; (2) צירוף דוח מבדק מסכם המאשר עמידה ברמת האבטחה (Security Level) הנדרשת וללא אי־התאמות קריטיות (Major Non–conformities) פתוחות;
(ג) הנחיה CIS Critical Security Controls – Implementation Group 3 (IG3) של המרכז לאבטחת אינטרנט (CIS) בעניין בקרות אבטחה קריטיות ליישום מתקדם, שאושר על ידי המרכז האמור ועומדת לעיון הציבור באתר האינטרנט של המרכז האמור, על עדכוניה מזמן לזמן	דוח אימות תאימות (Attestation of Compliance) מלא בעבור רמת IG3, שניתן במהלך 12 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי, המחזיק בחברות פעילה ב־CIS SecureSuite, המעיד על יישום מלא של כלל בקרות ה־Safeguards, בלא אי־התאמות קריטיות (Major Gaps) פתוחות; בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון ביישום מלא של כלל הבקרות כאמור;
(ד) הנחיה Cybersecurity Maturity Model Certification (CMMC) Level 3, של משרד ההגנה האמריקאי (DoD) בעניין הסמכת מודל בשלות להגנת סייבר ברמת מומחה, שאושר על ידי המשרד האמור ועומד לעיון הציבור באתר האינטרנט של המשרד האמור, על עדכוניה מזמן לזמן	תעודת הסמכה בתוקף לדרגה CMMC Level 3, שניתנה או חודשה לארגון במהלך 36 החודשים האחרונים על ידי משרד ההגנה האמריקאי (DoD) באמצעות ה־DIBCAC (Defense Contract Management Agency – Defense Industrial BaseCybersecurity Assessment Center) ובלא אי־התאמות קריטיות פתוחות;

טור א׳ הנחיות	טור ב׳ המסמך
(2) הארגון עומד במבדק AICPA SOC 2 Type 2 – Trust Services Criteria Report של אגודת רואי החשבון המוסמכים האמריקאית (AICPA) בעניין דיווח על בקרות בארגון שירות בהתבסס על קריטריונים של שירותי אמון, שאושר על ידי האגודה האמורה ועומד לעיון הציבור באתר האינטרנט של האגודה האמורה, על עדכוניו מזמן לזמן	דוח אימות תאימות Attestation, שנערך על ידי משרד רואי חשבון כהגדרתו בחוק רואי חשבון, התשט״ו–1955[35], (CPA firm) מוסמך בעל אקרדיטציה מטעם ה־AICPA, ולא חלפו מעל 24 חודשים ממועד סיום תקופת הביקורת המפורטת בו; הדוח האמור יכלול לכל הפחות את עקרונות הבקרה: Availability, Security ו־Confidentiality, ויאשר את אפקטיביות הבקרות לאורך תקופת הביקורת;
(3) הארגון מיישם את אחת החלופות לעניין ניהול תקרית שלהלן:	
(א) תקן מספר ISO/IEC 27035 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין ניהול תקריות אבטחת מידע – עקרונות ותהליכים, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27035 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27035 בעניין ניהול תקריות אבטחת מידע – עקרונות ותהליכים, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן.	דוח ביקורת תקופתי שניתן במהלך 12 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי, המעיד כי תהליכי ההיערכות לניהול אירועי סייבר מיושמים בפועל בהלימה לדרישות התקן; על התצהיר או דוח הביקורת לפרט את קיומם של מנגנונים סדורים לניטור, זיהוי, דיווח, סיווג, הערכה, תגובה ותיעוד של אירועי סייבר (Cyber Events), בצירוף תצהיר מאת נושא משרה לעניין הלימה לדרישות התקן של תהליכי ההיערכות לניהול אירועי סייבר המיושמים בפועל כאמור;
(ב) עמידה בדרישות ההגנה המנויות בפרט (2) בחלק א׳ לתוספת הרביעית	דוח ביקורת תקופתי על ידי גוף בודק חיצוני ובלתי תלוי, שניתן במהלך 12 החודשים האחרונים, המעיד על עמידה נאותה בכלל הדרישות הקבועות בפרט (2) בחלק א׳ לתוספת הרביעית, בצירוף תצהיר מאת נושא משרה לעניין עמידה נאותה בכלל הדרישות הקבועות כאמור;
(4) הארגון עומד באחת החלופות לעניין רציפות תפקודית שלהלן:	
(א) תקן מספר ISO 22301 של ארגון התקינה הבין־לאומי (ISO) בעניין אבטחה וחוסן – מערכות ניהול רציפות עסקית – דרישות, שאושר על ידי הארגון האמור, העומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 22301 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO 22301 בעניין אבטחה וחוסן – מערכות ניהול רציפות עסקית – דרישות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן.	תעודת הסמכה שניתנה או חודשה לארגון במהלך 36 החודשים האחרונים על ידי גוף הסמכה (Certification Body) בעל אקרדיטציה מתאימה מטעם ה־IAF, בלא אי־התאמות קריטיות (Major Non– conformities) פתוחות;

[35] ס״ח התשט״ו, עמ׳ 26.

טור ב׳ המסמך	טור א׳ הנחיות
דוח ביקורת תקופתי שניתן במהלך 12 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי, המעיד כי טכנולוגיות המידע והתקשורת (ICT) של הארגון תוכננו ותוחזקו בהתאם לעקרונות מוכנות טכנולוגיות המידע והתקשורת להמשכיות עסקית (IRBC), כמפורט בתקן. על המסמך לכלול ניתוח פערים אל מול בקרות המוכנות, אישור לקיום ניתוח השפעה עסקי (BIA), קיומן של אסטרטגיות התאוששות מותאמות ליעדי ה־RTO/RPO הארגוניים, בצירוף תצהיר מאת נושא משרה לעניין תכנון ותחזוק טכנולוגיות מידע והתקשורת בהתאם לעקרונות כמפורט בתקן כאמור;	(ב) תקן מספר ISO/IEC 27031 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין טכנולוגיית המידע – שיטות אבטחה – קווים מנחים למוכנות טכנולוגיות המידע והתקשורת לרציפות עסקית, המצוי באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת"י 27031 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27031 בעניין טכנולוגיית המידע – שיטות אבטחה – קווים מנחים למוכנות טכנולוגיות המידע והתקשורת לרציפות עסקית, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן
דוח ביקורת תקופתי על ידי גוף בודק חיצוני ובלתי תלוי, שניתן במהלך 12 החודשים האחרונים, המעיד על עמידה נאותה בכלל הדרישות הקבועות בפרט (3) בחלק א׳ לתוספת הרביעית, בצירוף תצהיר מאת נושא משרה לעניין עמידה בדרישות הקבועות כאמור.	(ג) עמידה בדרישות ההגנה המנויות בפרט (3) בחלק א׳ לתוספת הרביעית
	(5) הארגון עומד באחת החלופות לעניין שרשרת אספקה שלהלן:
דוח מבדק התאמה עדכני או אישור בחינה (Attestation), שנערכו במהלך 12 החודשים האחרונים על ידי גוף ביקורת עצמאי בתחומי הגנת הסייבר, המאשר כי הארגון הטמיע את בקרות אבטחת שרשרת האספקה של טכנולוגיות המידע והתקשורת (ICT), בהתאם להנחיות חלק שלוש לתקן. על הדוח לכלול הוכחות לניהול סיכוני ספקים, בקרת שלמות רכיבים ותהליכי רכישה מאובטחים, בצירוף תצהיר מאת נושא משרה לעניין הטמעת בקרות שרשרת האספקה של הטכנולוגיות המידע והתקשורת בהתאם להנחיות האמורות;	(א) תקן מספר ISO/IEC 27036–3 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת סייבר – יחסי ספקים – חלק 3: קווים מנחים לאבטחת שרשרת האספקה של חומרה, תוכנה ושירותים, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת"י 27036 חלק 3 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27036–3 בעניין אבטחת סייבר – יחסי ספקים – חלק 3: קווים מנחים לאבטחת שרשרת האספקה של חומרה, תוכנה ושירותים, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן

טור א׳ הנחיות	טור ב׳ המסמך
(ב) תקן מספר ISO/IEC 27036–4 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת מידע, הגנת סייבר והגנת הפרטיות – אבטחת מידע ליחסי ספקים – חלק 4: קווים מנחים לאבטחת שירותי ענן, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27036 חלק 4 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27036–4 בעניין אבטחת מידע, הגנת סייבר והגנת הפרטיות – אבטחת מידע ליחסי ספקים – חלק 4: קווים מנחים לאבטחת שירותי ענן, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	כל אלה: (1) דוח מבדק התאמה עדכני או אישור בחינה (Attestation), שנערכו במהלך 24 החודשים האחרונים על ידי גוף ביקורת עצמאי בתחומי הגנת הסייבר, המאשר כי הבקרות בחלק 4 של התקן הוטמעו בארגון; (2) אישור על ישימות התקן (SoA) המפרט את ההתייחסות לבקרות שירותי הענן וניהול הספקים בהתאם להנחיות חלק 4 בתקן, ללא אי־התאמות פתוחות; (3) צירוף תצהיר מאת נושא משרה לעניין הטמעה של הבקרות בחלק 4 של התקן בארגון כאמור;
(ג) מתודת שרשרת אספקה של מערך הסייבר הלאומי – מודל רוחבי, סוג A (פלטינה), רמת סיכון 2, בעניין ניהול ההגנה בסייבר על שרשרת האספקה, המגדירה סט בקרות סדור לבחינת חוסנם של ספקים ועמידותם בפני תקיפות סייבר, כפי שפורסמה על ידי המערך, העומדת לעיון הציבור באתר המערך, על עדכוניה מזמן לזמן	אישור עמידה במתודת מערך הסייבר הלאומי, המאשר כי הארגון עומד בדרישות ״מודול רוחבי – סוג A״ ברמת סיכון 2, שניתן או חודש במהלך 24 החודשים האחרונים על ידי גוף התעדה נבחר, הנכלל ברשימת מבצעי הפעילויות אישור עמידה במתודה, המפורסמת באתר האינטרנט של המערך;
(ד) עמידה בדרישות ההגנה המנויות בפרט (4) בחלק א׳ לתוספת הרביעית	דוח ביקורת תקופתי על ידי גוף בודק חיצוני ובלתי תלוי, שניתן במהלך 12 החודשים האחרונים, המעידים על עמידה נאותה בכלל הדרישות הקבועות בפרט 4 בחלק א׳ לתוספת הרביעית, בצירוף תצהיר מאת נושא משרה לעניין עמידה נאותה בדרישות כאמור.
(6) הארגון עומד באלה, בהתאם לסוג השירות שהוא מספק:	
(א) הארגון מספק שירותי IXP ועומד בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן. על המסמך להביע כי תשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגים, בצירוף תצהיר מאת נושא משרה לעניין תכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור;
(ב) הארגון מספק שירותי TLD ועומד בתקן ICANN Registry Operator Accreditation (Registry Agreement)	הסכם רישום (Registry Agreement) חתום ובתוקף מול תאגיד ICANN, המלווה בדוחות תאימות (Compliance Reports) המעידים על עמידה במדדי רמת השירות (SLAs) הטכניים והתפעוליים הנדרשים;

טור א׳ הנחיות	טור ב׳ המסמך
(ג) הארגון מספק שירותי Domain Registrars ועומד בהסכם ICANN Registry Operator Accreditation (Registry Agreement) של תאגיד האינטרנט להקצאת שמות ומספרים (ICANN) בעניין הסכם רישום למפעילי מאגרי שמות מתחם (Registry), שאושר על ידי התאגיד האמור ועומד לעיון הציבור באתר האינטרנט של התאגיד האמור, על עדכוניו מזמן לזמן	הסכם חתום ובתוקף מטעם ה־ICANN, המעיד על מעמד הארגון כרשם מוסמך (Accredited Registrar), בסטטוס "In Compliance" בלא הודעות הפרה (Notice of Breach) פתוחות;
(ד) הארגון הוא DNS Provider ועומד בתקן בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת"י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן; על המסמך להתייחס לכך שתשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגיים, בצירוף תצהיר מאת נושא משרה לעניין תכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור;
(ה) הארגון מספק שירותי אמון ומיישם את אחד מהתקנים האלה:	
(1) תקן מספר ETSI EN 319 401 של מכון התקנים האירופי לתקשורת (ETSI) בעניין חתימות אלקטרוניות ותשתיות (ESI); דרישות מדיניות כלליות לספקי שירותי אמון, שאושר על ידי המכון האמור ועומד לעיון הציבור באתר האינטרנט של המכון האמור, על עדכוניו מזמן לזמן	תעודת הסמכה (Conformity Certificate) בתוקף שניתנה או חודשה במהלך 24 החודשים האחרונים, על ידי גוף להערכת התאמה (CAB) בעל אקרדיטציה מתאימה, המעידה כי הארגון מקיים את בקרות התקן בלא חריגות קריטיות (Non–conformities) המשפיעות על מהימנות השירות;
(2) תקן מספר ETSI EN 319 102–1 של מכון התקנים האירופי לתקשורת (ETSI) בעניין נהלים ליצירה ואימות של חתימות דיגיטליות מסוג AdES, שאושר על ידי המכון האמור ועומד לעיון הציבור באתר האינטרנט של המכון האמור, על עדכוניו מזמן לזמן.	תעודת הסמכה (Conformity Certificate) בתוקף, שניתנה או חודשה לארגון במהלך 24 החודשים האחרונים, מטעם גוף הערכת תאימות (CAB) בעל אקרדיטציה רשמית לפי תקנת eIDAS, המעידה על עמידה מלאה בדרישות בלא חריגות קריטיות (Non–conformities);
(ו) הארגון מספק שירותי ענן מסוג CSP ועומד בכל אלה:	
(1) מבדק CSA STAR Certification Level 2 של ארגון ברית אבטחת הענן (CSA) בעניין הסמכה לאבטחת ענן ברמה 2 (צד שלישי), שאושר על ידי הארגון האמור ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן.	תעודת הסמכה (Conformity Certificate) בתוקף, שניתנה או חודשה על ידי גוף הסמכה (CB) מורשה ובעל אקרדיטציה מטעם ה־IAF, המעידה על עמידה בבקרות ה־Cloud Controls Matrix (CCM), בלא אי־התאמות קריטיות פתוחות (Non–conformities);

טור ב׳ המסמך	טור א׳ הנחיות
דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן. על המסמך להביע כי תשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגיים, בצירוף תצהיר מאת נושא משרה לעניין תכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור;	(2) בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן
	(ז) הארגון מספק שירותי ענן מסוג Saas/Paas ועומד באחד מאלה:
דוח מבדק התאמה (Compliance Report) חתום על ידי גוף ביקורת חיצוני, שניתן במהלך 24 החודשים האחרונים, המעיד על יישום של מסגרת ה־Application Security Framework (ASF) בצירוף תיעוד רכיבי אבטחת היישומים (ASC) והוכחות לשילוב בקרות אבטחה בתהליכי מחזור חיי הפיתוח הארגוניים. על הדוח לשקף עמידה בדרישות הרלוונטיות מתוך חלקי התקן השונים, בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בדרישות הרלוונטיות מתוך חלקי התקן השונים;	(1) תקן מספר ISO/IEC 27034 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת אפליקציות (יישומים), שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27034 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27034 בעניין אבטחת אפליקציות (יישומים), שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן
דוח הערכת בשלות מפורט (Maturity Model) חתום על ידי גוף חיצוני ובלתי תלוי, שניתן במהלך 24 החודשים האחרונים, ומעיד על רמת היישום של 15 תחומי האבטחה (Security Practices) המוגדרים במודל ה־OWASP SAMM, בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בדרישות המודל;	(2) הנחיה OWASP SAMM של קרן OWASP בעניין מודל בשלות לאבטחת תוכנה (Software Assurance Maturity Model), שאושר על ידי קרן זו ועומדת לעיון הציבור באתר האינטרנט של הקרן האמורה, על עדכוניה מזמן לזמן
דוח ביקורת של גוף בלתי תלוי המעיד כי תהליכי הפיתוח עומדים בפרקטיקות המוגדרות ב־SSDF (Prepare the Organization, Protect the Software, Produce Well–Secured Software, Respond to Vulnerabilities), בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בפרקטיקות האמורות.	(3) הנחיה NIST SSDF (SP 800–218) של המכון הלאומי לתקנים וטכנולוגיה (NIST) בעניין מסגרת לפיתוח תוכנה מאובטחת (Secure Software Development Framework), שאושר על ידי המכון האמור ועומדת לעיון הציבור באתר האינטרנט של המכון האמור, על עדכוניה מזמן לזמן
דוח ביקורת תקופתי שניתן במהלך 12 החודשים האחרונים על ידי גוף בודק חיצוני ובלתי תלוי, המעיד על עמידה נאותה בכלל הדרישות הקבועות בפרט (5) בחלק א׳ לתוספת הרביעית, בצירוף תצהיר מאת נושא משרה לעניין עמידה בדרישות האמורות;	(4) עמידה בדרישות ההגנה המנויות בפרט (5) בחלק א׳ לתוספת הרביעית
	(ח) הארגון מספק שירותי Data Centers ועומד בכל אלה:

טור א׳ הנחיות	טור ב׳ המסמך
(1) בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת"י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן.	דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן; על המסמך להתייחס לכך שתשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגיים, בצירוף תצהיר מאת נושא משרה לעניין תכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור.
(2) אחד מהתקנים שלהלן:	
(א) תקן ANSI/TIA 942 של איגוד תעשיית הטלקומוניקציה (TIA) בעניין תקן תשתית טלקומוניקציה למרכזי נתונים (Data Centers), שאושר על ידי האיגוד האמור ועומד לעיון הציבור באתר האינטרנט של האיגוד האמור, על עדכוניו מזמן לזמן.	תעודת הסמכה (Audit Certificate) בתוקף, שניתנה או חודשה במהלך 36 החודשים האחרונים על ידי גוף הסמכה מורשה (Certification Body) הפועל מטעם תוכנית האקרדיטציה של TIA, המציינת את רמת הדירוג (Rated Level) של שירות ה־Data Center ובלא אי־התאמות קריטיות פתוחות.
(ב) תקן מספר ISO/IEC 22237 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין טכנולוגיית מידע – מיתקנים ותשתיות של מרכזי נתונים, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן	תעודת הסמכה שניתנה או חודשה במהלך 36 החודשים האחרונים, על ידי גוף התעדה (Certification Body) בעל אקרדיטציה רשמית מטעם ה־IAF, המעידה כי מיתקן ה־Data Center עומד בדרישות התכנון, התשתית והתפעול בהתאם לרמות הזמינות (Availability Classes) וההגנה הפיזית הנדרשות, ובלא אי־התאמות קריטיות פתוחות.
(ט) הארגון מספק שירותי CDN ועומד בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת"י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן. על המסמך להביע כי תשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגיים; הדוח האמור יוגש בצירוף תצהיר מאת נושא משרה לעניין תכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור;
(י) הארגון מספק שירותי MSP ועומד בתקן מספר ISO/IEC 27043 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין עקרונות ותהליכים לחקירת תקריות אבטחה, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת"י 27043 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27043 בעניין עקרונות ותהליכים לחקירת תקריות אבטחה, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	דוח מבדק התאמה (Compliance Report) חתום על ידי גוף ביקורת חיצוני, שניתן במהלך 24 החודשים האחרונים, המעיד על יישום של מסגרת ה־Application Security Framework (ASF) בצירוף תיעוד רכיבי אבטחת היישומים (ASC) והוכחות לשילוב בקרות אבטחה בתהליכי מחזור חיי הפיתוח הארגוניים. על הדוח לשקף עמידה בדרישות הרלוונטיות מתוך חלקי התקן השונים, בצירוף תצהיר מאת נושא משרה לעניין עמידת הארגון בדרישות הרלוונטיות מתוך חלקי התקן השונים.

טור א׳ הנחיות	טור ב׳ המסמך
(יא) הארגון מספק שירותי MSP מרחוק, ועומד בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן. על המסמך להביע כי תשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגיים, בצירוף תצהיר מאת נושא משרה לעניין תיכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור.
(יב) הארגון מספק שירותי MSSP ועומד בתקן מספר ISO/IEC 27043 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין עקרונות ותהליכים לחקירת תקריות אבטחה, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27043 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27043 בעניין עקרונות ותהליכים לחקירת תקריות אבטחה, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן.	דוח תקופתי שניתן או חודש במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי, המעיד כי תהליכי החקירה הדיגיטלית וההיערכות לאירועים בארגון תואמים את עקרונות התקן. על הדוח האמור לכלול פירוט של המתודולוגיה לטיפול בראיות דיגיטליות (Digital Evidence) ולאשר כי הבקרות מיושמות בלא אי־התאמות קריטיות פתוחות, בצירוף תצהיר מאת נושא משרה לעניין התאמת תהליכי החקירה הדיגיטלית וההיערכות לאירועים בארגון לעקרונות התקן כאמור.
(יג) הארגון מספק שירותי MSSP ועומד בתקן מספר ISO/IEC 27033 של ארגון התקינה הבין־לאומי (ISO) והנציבות הבין־לאומית לאלקטרוטכניקה (IEC) בעניין אבטחת רשתות, שאושר על ידי הארגון והנציבות האמורים ועומד לעיון הציבור באתר האינטרנט של הארגון האמור, על עדכוניו מזמן לזמן; או תקן ישראלי מספר ת״י 27033 של מכון התקנים הישראלי, המאמץ את התקן הבין־לאומי ISO/IEC 27033 בעניין אבטחת רשתות, שאושר על ידי מכון התקנים הישראלי ועומד לעיון הציבור בספרייה ובאתר האינטרנט של מכון התקנים הישראלי, על עדכוניו מזמן לזמן	דוח ביקורת תקופתי שניתן במהלך 36 החודשים האחרונים על ידי גוף ביקורת חיצוני ובלתי תלוי המוסמך מטעם ה־IAF, המעיד כי בקרות אבטחת הרשת של הארגון תוכננו ויושמו בהתאם להנחיות התקן. על המסמך להביע כי תשתית הרשת נסקרת כחלק ממערך ניהול אבטחת המידע (ISMS) תוך הלימה מלאה להצהרת הישימות (SoA) הארגונית ועדכונים טכנולוגיים, בצירוף תצהיר מאת נושא משרה לעניין תיכנון ויישום של בקרות אבטחת הרשת של הארגון בהתאם להנחיות התקן כאמור.