תזכיר חוק

א. שם החוק המוצע

חוק הגנת הסייבר הלאומית, התשפ"ו-2026

ב. מטרת החוק המוצע והצורך בו

מטרת תזכיר החוק המוצע להביא להגנה לאומית טובה יותר על תפקודו הרציף והבטוח של מרחב הסייבר הלאומי, כחלק מחוסנה ובטחונה הלאומי של מדינת ישראל, בדגש על הגנת ארגונים חיוניים, ספקי שירותים דיגטליים ושירותי אחסון. החקיקה המקודמת מבוססת על הצרכים והאיומים בראייה לאומית, על החלטות הממשלה ומדיניותה בתחום הגנת הסייבר, התפיסה העומדת בבסיס החלטות הממשלה האמורות והניסיון שנצבר מאז קבלתן, במיוחד נוכח לקחי תקופת "חרבות ברזל" ו"עם כלביא". מדובר בחקיקה ממוקדת, דיפרנציאלית המבוססת על ניהול סיכונים ואיזון רגולטורי.

ג. עיקרי החוק המוצע

בחוק מוצע לעגן את מסגרת האסדרה והפיקוח על הגנת הסייבר הלאומית, תוך עיגון רוחבי של סמכויות וכלי הגנת הסייבר של משרדי הממשלה השונים, ואסדרה דיפרנציאלית ביחס למגזרים ולארגונים החיוניים בהם, וכן ביחס לספקי השירותים הדיגטליים ושירותי האחסון; זאת לצד קביעת חובות הארגונים, בדגש על הארגונים החיוניים, לפעול להגנת הסייבר, הן בשגרה והן בעת התמודדות עם תקיפת סייבר, כל זאת תוך הקפדה על שימור הגמישות הנדרשת בתחום עיסוק משתנה זה.

באמצעות קביעת מסגרת סמכויות ברורה, עקרונות פעולה מוגדרים ומנגנוני פיקוח ואכיפה, מבקש החוק המוצע לחזק את החוסן הלאומי במרחב הסייבר, לשפר את רמת המוכנות והתגובה לתקיפות סייבר, לעודד היערכות אשר עלותה נמוכה באופן ניכר מהעלות הכלכלית והחברתית הכרוכה בשיקום שלאחר התקיפה. בכך יתרום החוק המוצע ליציבות המשק, להגנה על על הציבור ולהגנה על רציפות תפקודם של השירותים החיוניים, כחלק מביטחונה הלאומי של מדינת ישראל.

ד. להלן נוסח תזכיר החוק המוצע

תזכיר חוק מטעם מערך הסייבר הלאומי – משרד ראש הממשלה:

תזכיר חוק הגנת הסייבר הלאומית, התשפ"ו -2026

פרק א': הגדרות

הגדרות 1. בחוק זה -

"ארגון" – מוסד כהגדרתו בסעיף 35 לפקודת הראיות [נוסח חדש], התשל"א-1975 או חלק ממנו;

"ארגון חיוני" – כמשמעותו בסעיף 8(א);

"ארגון חיוני למערכת הביטחון" – כמשמעותו בסעיף 20;

"גוף מונחה" – גוף המנוי בפרטים 2 ו-3 לתוספת הראשונה, בתוספת הרביעית או בתוספת החמישית לחוק הסדרת הבטחון בגופים ציבוריים;

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

"גוף ממשלתי" – גוף המנוי בטור א' בתוספת השניה, לרבות יחידות הסמך שלו, ובתנאי שאינו גוף שנמנה על הגופים המיוחדים ושאינו גוף מונחה;

"גורם מאסדר" – השר, או גורם אחר המנוי בטור ה' בתוספת הראשונה, האמון על האסדרה של רשות מוסמכת ביחס למגזר משק, המנוי בטור ב' לצדו;

"גורם מסמיך" – גורם המנוי בטור ד' בתוספת הראשונה או השנייה;

"חומר מחשב" – כהגדרתו בחוק המחשבים;

"חוק הגנת הפרטיות" – חוק הגנת הפרטיות, תשמ"א-1981[1];

"חוק המחשבים" – חוק המחשבים, תשנ"ה- 1995[2];

"חוק הסדרת הבטחון בגופים ציבוריים" – חוק הסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998[3];

"חוק העונשין" – חוק העונשין, התשל"ז- 1977[4];

"מגזר משק" – מגזר או תת מגזר משק המנוי בטור א' בתוספת הראשונה או השנייה ביחס אליו פועלת הרשות המוסמכת בהתאם לחוק זה;

"מחשב" – כהגדרתו בחוק המחשבים;

"הממונה" – עובד בכיר ברשות מוסמכת אשר דרגתו ראש אגף לפחות שהוסמך על ידי הגורם המסמיך להטיל עיצומים לפי חוק זה;

---

[1] ס"ח תשמ"א 1011, עמ' 128.
[2] ס"ח תשנ"ה מס' 1534, עמ' 366.
[3] ס"ח תשנ"ח 1685, עמ' 348.
[4] ס"ח תשל"ז מס' 864 , עמ' 226.

"מנהל בכיר במערך הסייבר הלאומי"- עובד בכיר במערך הסייבר הלאומי, אשר דרגתו ראש אגף לפחות, אשר ראש מערך הסייבר הלאומי הסמיך לעניין זה;

"מנהל בכיר ברשות מוסמכת" – עובד בכיר ברשות מוסמכת אשר דרגתו ראש אגף לפחות, אשר הגורם המסמיך הסמיכו לעניין זה;

"מערך הסייבר הלאומי", "המערך" – מערך הסייבר הלאומי לפי סעיף 2;

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

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

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

(2) מי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי אחסון או שירותים דיגטליים;

"עובד המדינה"- כהגדרתו בסעיף 7 לפקדות הנזיקין [נוסח חדש] התשכ"ח-1968;

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

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

"פגיעות חמורה" – נקודת תורפה במחשב או בחומר מחשב אשר אפשר לנצל לביצוע תקיפת סייבר שמערך הסייבר הלאומי מצא כי לנוכח מאפייניה היא יוצרת סיכון משמעותי לתקיפת סייבר;

"פלט" – כהגדרתו בחוק המחשבים;

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

"צה"ל" – צבא ההגנה לישראל;

"רשות מוסמכת" – גוף המנוי בטור ג' בתוספת הראשונה או בתוספת השנייה;

"רשות מקומית" – עיריה, 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 דיגטליים" – שירות שהוא אחד מאלה, הניתן עבור אחר:

(1) שירותי תוכנה, לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח של תוכנה;

(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;

"תוכנה" – כהגדרתה בחוק המחשבים;

"תקיפת סייבר" – פעולה או חשש ממשי לפעולה, 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 או הפרעה לשימוש בו;

(3) אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;

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

(5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט- 1979[5];

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

(7) הפרעה או מניעת נגישות של מחשב לרשת תקשורת;

פרק ב': מערך הסייבר הלאומי

מערך הסייבר הלאומי

2. (א) מערך הסייבר הלאומי הוא גוף מבצעי-טכנולוגי הפועל כיחידה עצמאית במשרד ראש הממשלה.

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

תפקידי מערך הסייבר הלאומי

3. (א) מערך הסייבר יהיה מופקד על קידום, תיאום, הפעלה וביצוע בהתאם לצורך, של מאמצי הגנת הסייבר הלאומית, ובכלל האמור יפעל לביצוע התפקידים הבאים:

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

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

(3) לחזק את החוסן הלאומי בהגנת סייבר ולקדם את ההתמודדות עם תקיפות סייבר;

---

[5] ס"ח תשל"ט 938, עמ' 118.

(4) לפעול להעלאת המודעות בציבור להתנהגות בטוחה במרחב הסייבר, ולפרסם התרעות והמלצות לציבור להעלאת רמת הגנת הסייבר;

(5) לקדם ולעודד מחקר ופיתוח של תחום הגנת הסייבר;

(6) לקדם בחינת והטמעת טכנולוגיות מתפתחות להגנת סייבר;

(7) לקדם שיתוף פעולה בתחום הגנת הסייבר במישור הבינלאומי ולערוך 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 (CERT), לרבות מרכז לאומי לקבלת דיווחים על תקיפות סייבר ופניות לעניין הגנת הסייבר ומרכז שליטה ובקרה לאומי למול איומי סייבר (NSOC);

(2) ינחה מקצועית את היחידות המגזריות לקידום הגנת הסייבר לרבות לעניין אופן יישום שנתי ורב שנתי של מדיניות ואסטרטגיית הסייבר הלאומית לצורך שיפור רמת ההגנה בסייבר במגזר ולעניין התמודדות עם תקיפות סייבר חמורות במגזר, ובכלל האמור יפעל, בהתאם לכל דין והסכם,לשתף עמן:

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

(ב) הערכות מקצועיות של מערך הסייבר הלאומי; מידע, לרבות מידע על תקיפות סייבר והתרעות לרבות מידע הנוגע לפגיעויות חמורות, אשר המערך מצא כי הם נדרשים להגנת הסייבר במגזר;

(ג) אמצעים טכנולוגיים העומדים לרשות מערך הסייבר הלאומי אשר מצא המערך כי הם נדרשים להגנת הסייבר במגזר.

ראש מערך הסייבר הלאומי

4. (א) הממשלה, לפי הצעת ראש הממשלה, תמנה את ראש מערך הסייבר הלאומי (בחוק זה – ראש מערך הסייבר הלאומי), בהתאם להוראות חוק שירות המדינה (מינויים), התשי"ט-1959[6].

(ב) ראש מערך הסייבר הלאומי יהיה מופקד על ניהול המערך ועל ביצוע תפקידיו וכן יהיו לו כל הסמכויות הנתונות לעובדי המערך.

---

[6] ס"ח תשי"ט 279, עמ' 86;

(ג) ראש מערך הסייבר הלאומי רשאי לאצול סמכות שניתנה לו לפי חוק זה, למנהל בכיר במערך הסייבר הלאומי, למעט הסמכות לפי סעיף 10(ה).

פרק ג': יחידה מגזרית ועובדים מוסמכים

יחידה מגזרית

5. ברשות מוסמכת תפעל יחידה לקידום הגנת הסייבר במגזר המשק, בהתאם להנחיה המקצועית של מערך הסייבר הלאומי (בחוק זה- "יחידה מגזרית"), אשר בין תפקידיה:

(א) לפעול לשיפור רמת הגנת הסייבר במגזר המשק בהתאם למדיניות ואסטרטגיית הגנת הסייבר הלאומית, לרבות באמצעות קידום אסדרה ייעודית בסייבר למגזר המשק או חלק ממנו והנחיות מקצועיות מגזריות;

(ב) למפות באופן שוטף את הארגונים החיוניים במגזר המשק;

(ג) לרכז את נתוני רמת ההגנה בסייבר בארגונים החיוניים במגזר המשק ולשתפם עם מערך הסייבר הלאומי באופן שוטף, ולכל הפחות אחת לרבעון;

(ד) לוודא פיקוח וכן את קיומו של מנגנון אכיפה במגזר המשק לפי חוק זה;

(ה) לפעול להנחיית ארגונים חיוניים במגזר המשק בטיפול בתקיפות סייבר חמורות לפי חוק זה;

(ו) לפעול לקידום תהליכי שיתוף מידע וידע הנוגע להגנת סייבר במגזר המשק, בכפוף לכל דין, בין היתר מול מרכז השליטה והבקרה (NSOC) הלאומי; יחידה מגזרית תוכל להפעיל לשם כך מרכז שליטה ובקרה מגזרי למול איומי סייבר (SOC מגזרי);

(ז) לפעול לקידום העלאת המודעות לסיכוני הסייבר במגזר המשק, ולפרסם התרעות והמלצות להעלאת רמת הגנת הסייבר במגזר בהתייעצות עם מערך הסייבר הלאומי;

(ח) להכין תכנית עבודה שנתית או רב שנתית, לרבות בהתאם לדגשי מערך הסייבר הלאומי ולאחר התייעצות עמו, שתאושר על ידי הגורם המסמיך ותוצג למערך הסייבר הלאומי;

(ט) להכין עדכון מסכם אחת לשנה, אשר יועבר למערך הסייבר הלאומי ויכלול בין השאר נתונים לפי סעיפים קטנים (ב), (ג), נתונים בדבר פיקוח ואכיפה ופעולות להטלת עיצומים על ארגון חיוני, פעולות לפי סעיפים קטנים (ו) ו- (ז), נתונים אודות תקיפות סייבר חמורות כמשמעותן בסעיף 14, שהתרחשו במגזר המשק ומתן הוראות לארגונים חיוניים לפי סעיף 15 או 16.

עובד מוסמך במערך הסייבר הלאומי ועובד מוסמך מגזרי

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

(ב) הגורם המסמיך ברשות מוסמכת, רשאי להסמיך מבין עובדי הרשות המוסמכת, עובד אחד או יותר, שיהיו נתונות לו הסמכויות הנתונות לעובד מוסמך מגזרי לפי חוק זה, כולן או חלקן, לשם ביצוע הוראות חוק זה במגזר המשק.

תנאים להסמכת עובד מוסמך

7. לא יוסמך עובד מוסמך מגזרי או עובד מוסמך במערך הסייבר הלאומי, לפי הוראות חוק זה אלא אם כן מתקיימים בו כל אלה:

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

(ב) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, בהתאם להוראות ראש מערך הסייבר הלאומי;

(ג) הגורם המסמיך מצא שהוא בעל ההכשרה, הידע, הכישורים והנסיון הנדרשים למילוי תפקידו בצורה נאותה, ובכלל זה ידע מעמיק בהגנת סייבר.

פרק ד': אסדרה לאומית בתחום הגנת הסייבר

סימן א': ארגון חיוני

ארגון חיוני

8. (א) ארגון חיוני הוא אחד מאלה:

(1) גוף ממשלתי;

(2) ארגון שמתקיימים לגביו התבחינים המגזריים המפורטים בתוספת השלישית לעניין ארגונים מאותו מגזר משק, ושאינו גוף מונחה, אלא אם קבע גורם מאסדר שהארגון אינו ארגון חיוני לפי סעיף קטן (ב);

(3) ארגון שקבע גורם מאסדר שהוא ארגון חיוני לפי סעיף קטן (ב).

(ב) גורם מאסדר רשאי לקבוע ביחס לארגון במגזר המשק, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, כי על אף שמתקיימים לגבי הארגון התבחינים לפי סעיף קטן א(2) הארגון אינו ארגון חיוני, או כי הארגון הוא ארגון חיוני גם אם לא מתקיימים לגביו התבחינים לפי אותו סעיף קטן, אם מתקיימים התנאים הבאים:

(1) מתקיימות נסיבות חריגות המצדיקות קביעה כאמור ביחס לארגון, בהתחשב בסוג הארגון, מאפייני פעילותו והשלכות פגיעת תקיפת סייבר בפעילותו , לרבות בהתייחס לביטחון המדינה, בטחון הציבור, חיי אדם, כלכלת המדינה או ברציפות אספקתם של שירותים חיוניים לציבור, ובכלל האמור בהתחשב בחשיבות זמינות השירות של הארגון, בחלופות לשירות, במספר המשתמשים התלויים בשירות הארגון, בנתח השוק של שירות הארגון, בפריסה הגיאוגרפית של השירות שמספק הארגון, ובתלות של ארגונים אחרים בשירות של הארגון ;

(2) הארגון אינו גוף מונחה ואינו ארגון חיוני במגזר משק אחר ;

(3) הגורם המאסדר שמע את עמדת הוועדה המייעצת בעניין, אשר תועבר בתוך 30 ימים מיום הפנייה אליה.

בסעיף זה "הוועדה המייעצת" – ועדה בראשות עובד בכיר ברשות המוסמכת שהסמיך הגורם המאסדר, שיהיו חברים בה נציגי מערך הסייבר הלאומי, משרד האוצר, משרד הביטחון, שירות הביטחון הכללי והיעוץ המשפטי לממשלה.

(ג) קבע הגורם המאסדר כאמור בסעיף קטן (ב) יודיע על כך לארגון ויידע בכך את מערך הסייבר הלאומי בתוך 14 ימים בצירוף נימוקי ההחלטה ; קביעת הגורם המאסדר תיכנס לתוקף במועד מסירת ההודעה על הקביעה לארגון.

(ד) נקבע ארגון כארגון חיוני בהתאם לסעיף קטן (ב), יחולו לגביו ההוראות לפי סעיפים 10(ב) עד 10(ד) החל מתום 12 חודשים ממועד הקביעה כאמור.

(ה) ארגון שהוא ארגון חיוני לפי סעיף קטן א(2) ביותר ממגזר משק אחד, רשאי לפנות לגורמים המאסדרים באותם מגזרי משק, לצורך קביעתם, בהתייעצות עם מערך הסייבר הלאומי, את מגזר המשק האחד בו יוגדר הארגון כארגון חיוני לפי חוק זה.

(ו) הגורם המאסדר, בהתייעצות עם ראש מערך הסייבר הלאומי ועם שר האוצר, ובאישור ועדת החוץ והביטחון של הכנסת, רשאי בצו, לשנות את התבחינים המנויים בתוספת השלישית לעניין מגזר המשק, ובלבד ששינוי כאמור ייעשה על בסיס כללים ואמות מידה מקצועיים המיושמים במדינות מפותחות עם שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת.

תיקון התוספת הראשונה והתוספת השנייה

9. ראש הממשלה, לאחר שקילת המלצת ראש מערך הסייבר הלאומי, בהתייעצות עם הגורם המאסדר ושר האוצר, ובאישור ועדת החוץ והביטחון של הכנסת, רשאי לשנות את התוספת הראשונה או השנייה.

סימן ב': הגנת סייבר בארגונים וחובת דיווח

רמת הגנת סייבר

10. (א) ארגון אחראי להבטחת רמת הגנת סייבר ראויה לפעילותו בהתאם לסוג ואופי פעילותו ותוך ניהול סיכון הולם.

(ב) מבלי לגרוע מן האמור בסעיף קטן (א):

(1) ארגון חיוני יעמוד בדרישות רמת הגנה בסיסית המפורטות בחלק א' לתוספת הרביעית, באמצעות עמידה בהוראות הרלוונטיות באחד התקנים המנויים בחלק ב' לתוספת הרביעית וזאת תוך הבטחת הלימה לדרישות המפורטות בחלק א' לתוספת הרביעית.

(2) מערך הסייבר הלאומי יפרסם באתר האינטרנט שלו הודעות על עדכונים רלוונטיים של התקינה האמורה בסעיף קטן (1).

(3) ראש הממשלה, לאחר שקילת המלצת ראש מערך הסייבר הלאומי, באישור ועדת החוץ והביטחון של הכנסת, רשאי לשנות את התוספת הרביעית.

(ג) גורם מאסדר לפי התוספת הראשונה, רשאי, לאחר התייעצות עם ראש מערך הסייבר הלאומי, לקבוע בתקנות, או בהוראות אחרות שהוא מוסמך לתת לפי דין, דרישות בעניין רמת הגנת הסייבר של ארגונים חיוניים במגזר המשק, נוספות על הדרישות שבתוספת הרביעית.

(ד) ראש הרשות המוסמכת לפי התוספת השניה רשאי, לאחר התייעצות עם ראש מערך הסייבר הלאומי, ליתן הוראות לעניין רמת הגנת הסייבר של גופים ממשלתיים נוספות על הדרישות שבתוספת הרביעית.

(ה) (1) מצא ראש מערך הסייבר הלאומי כי מתקיים סיכון סייבר משמעותי העלול לאפשר תקיפת סייבר חמורה כמשמעותה בסעיף 14(א), נגד ארגונים חיוניים שונים, רשאי הוא, באישור ראש הממשלה להורות לארגון חיוני שביחס אליו עלול להתממש הסיכון, לנקוט אמצעים להתמודדות או מניעת הסיכון לאחר ששקל את ההשפעה על פעילות הארגון החיוני ועל צד שלישי לרבות על הזכות לפרטיות, את העלות הכלכלית המוערכת של יישום ההוראות ואת השפעתן האפשרית על הרציפות התפקודית של הארגון החיוני, למיטב ידיעתו ומצא כי אין בהוראה לפגוע במידה העולה על הנדרש בנסיבות העניין;

(2) הוראה כאמור בפסקה (1) תיקבע לתקופה שאינה עולה על 30 ימים ורשאי ראש המערך להאריך את תוקפה לתקופה אחת נוספת שאינה עולה על 30 ימים אם מצא שההוראה עדיין נדרשת;

(3) ההוראה תועבר לארגון החיוני באמצעות הרשות המוסמכת, אלא אם התקיימו נסיבות מיוחדות המצדיקות אחרת;

(4) על אף האמור בפסקה (1), רשאי ראש מערך הסייבר הלאומי לתת הוראה טרם קבלת אישור ראש הממשלה, אם שוכנע כי מתן ההוראה אינו סובל דיחוי, וכי אין סיפק לקבל את אישור ראש הממשלה מבעוד מועד. ניתנה הוראה לפי פסקה זו, ולא ניתן אישור ראש הממשלה תוך 48 שעות לאחר מתן ההוראה, יראו את ההוראה כאילו לא ניתנה, והארגון החיוני יעודכן על כך בדרך הקבועה בפסקה (3).

(ו) ארגון חיוני ישמור מידע ומסמכים המעידים על עמידתו בהוראות לפי סעיפים קטנים (ב) - (ה).

(ז) תקנות והוראות בהתאם לסעיפים קטנים (ב)-(ד) יקבעו על בסיס כללים ואמות מידה מקצועיים, המיושמים במדינות מפותחות עם שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת, לרבות בשל מגבלות או חלופות מצומצמות למתן השירותים, צרכים תפעוליים ייחודיים, הערכת איומים וסיכונים לרבות היערכות למצב חירום, או תנאי שוק ייחודיים.

חובת דיווח על תקיפת סייבר משמעותית

11. (א) נודע לארגון חיוני שמתרחשת נגדו, בפועל, תקיפת סייבר משמעותית שמתקיים לגביה אחד מהמפורטים להלן, ידווח על כך למנהל בכיר במערך הסייבר הלאומי ולמנהל בכיר ברשות המוסמכת בהתאם להוראות סעיפים קטנים (ב) ו- (ג):

(1) התקיפה עלולה לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות השירות של הארגון, לרבות בבטיחות של מערכת או תהליך חיוניים בארגון, 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 או גישה של גורם שאינו מורשה לנכס מידע משמעותי, ובכלל זה בדרך של פגיעה בתהליך הזדהות, שינויו, או הוצאתו שלא כדין של מידע לרבות בדרך של העתקתו על ידי גורם כאמור;

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

(ב) לשם מילוי חובתו בהתאם לסעיף זה, יגיש הארגון החיוני, 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 שתקיפתו עלולה לפגוע ישירות ובאופן ממשי בארגון אחר.

(ג) דיווח לפי סעיף זה יוגש למנהל בכיר במערך הסייבר הלאומי ולמנהל בכיר ברשות מוסמכת באמצעות המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר (CERT) שמפעיל מערך הסייבר הלאומי באופן מקוון באתר האינטרנט של המערך, בהודעה טלפונית למרכז הלאומי או בדרך אחרת שהורה עליה ראש מערך הסייבר הלאומי ופורסמה באתר האינטרנט כאמור. על אף האמור, רשאי הגורם המסמיך, לאחר יידוע מערך הסייבר הלאומי, לקבוע כי הדיווח יוגש לרשות המוסמכת באופן שיקבע, ויועבר על ידה למערך הסייבר הלאומי עם קבלתו.

(ד) בסמוך לאחר הטיפול בתקיפת הסייבר, ארגון חיוני ימסור דיווח מסכם כתוב באופן הקבוע בסעיף קטן (ג) בשינויים המחוייבים. הדיווח המסכם יכלול את הפרטים שלהלן:

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

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

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

סימן ג': סמכויות פיקוח

דרישת ידיעות ומסמכים

12. לשם פיקוח על ביצוע הוראות 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 ביצועו של חוק זה או להקל על ביצועו.

כניסה למקום

13. (א) לשם פיקוח על יישום הוראות סעיפים 10(ב) עד 10(ה) וסעיף 11, עובד מוסמך מגזרי רשאי להיכנס למקום ובלבד שלא יכנס למקום המשמש למגורים, אלא על פי צו של בית משפט.

(ב) עובד מוסמך מגזרי לא יעשה שימוש בסמכויות הנתונות לו לפי סעיף זה, אלא בעת מילוי תפקידו ואם יש בידו תעודה החתומה בידי הגורם המסמיך, המעידה על תפקידו ועל סמכויותיו של עובד מוסמך מגזרי, שאותה יציג על פי דרישה.

(ג) 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.

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

סימן ד': תקיפת סייבר חמורה

תקיפת סייבר חמורה

14. (א) בסימן זה "תקיפת סייבר חמורה" – תקיפת סייבר שהיה למנהל בכיר ברשות מוסמכת חשש ממשי כי מתקיים לגביה אחד או יותר מהתנאים הבאים ביחס אליה:

(1) תקיפת הסייבר עלולה לפגוע ברציפות התפקודית של ארגון חיוני לרבות בבטיחות של מערכת או תהליך שהם חיוניים בארגון ;

(2) תקיפת הסייבר עלולה לפגוע בזמינות, רציפות או מהימנות השירות שארגון חיוני מספק ;

(3) תקיפת הסייבר עלולה לאפשר גישה לגורם שאינו מורשה לנכס מידע משמעותי של הארגון החיוני ;

(4) תקיפת הסייבר בארגון חיוני בעלת מאפיינים המעידים על חומרת תקיפה מיוחדת, לרבות מיתאר התקיפה או זהות התוקף;

(5) תקיפת הסייבר בארגון חיוני עלולה לפגוע בביטחון המדינה, בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור בשל:

(א) מאפייני התקיפה, לרבות מתאר התקיפה או זהות התוקף;

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

(ב) היה למנהל בכיר ברשות מוסמכת יסוד סביר להניח כי תקיפת סייבר שמתרחשת או שקיים חשש ממשי כי היא עומדת להתרחש היא תקיפת סייבר חמורה נגד ארגון חיוני במגזר המשק או תקיפה כאמור הנעשית באמצעות הארגון החיוני, 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 סעיף זה.

מתן הוראות לארגון חיוני המנוי בתוספת הראשונה להתמודדות עם תקיפת סייבר חמורה

15. (א) קבע מנהל בכיר ברשות מוסמכת לפי התוספת הראשונה, כי תקיפת סייבר שמתרחשת או שקיים חשש ממשי כי היא עומדת להתרחש, נגד ארגון חיוני או באמצעותו, היא תקיפת סייבר חמורה הדורשת את מעורבותו, יודיע על כך עובד מוסמך מגזרי, בהתייעצות עם מערך הסייבר הלאומי, לארגון כאמור, לאחר שהזדהה בפניו, ויחולו הוראות אלה:

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

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

(3) הארגון 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 לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה, כאמור בפסקה (2), רשאי העובד המוסמך המגזרי, אם מצא שהדבר נדרש לאיתור התקיפה, מניעתה או בלימתה, ולאחר שהודיע לארגון על כוונתו לתת לו הוראות לפי פסקה זו ונתן לו הזדמנות להשמיע טענותיו, לתת לו, 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 העוסקים בעניינים הנוגעים לאיתור התקיפה, מניעתה או בלימתה, לרבות העתק מחומר מחשב, לידי העובד המוסמך;

(5) במתן הוראות לפי פסקה (4):

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

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

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

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

(ב) (1) מסר העובד המוסמך המגזרי לארגון הודעה כאמור בסעיף קטן (א), ימסור הארגון, בלא דיחוי, עדכון בדבר תקיפת הסייבר החמורה לכל ארגון העלול להיפגע מהתקיפה ישירות ובאופן ממשי, וידווח על כך בכתב לעובד המוסמך המגזרי, והכל 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, אם שוכנע כי קיימות נסיבות חריגות המצדיקות זאת, ובהתייעצות עם מערך הסייבר הלאומי, לפטור את הארגון החיוני מחובת היידוע כאמור בפסקה (1) או לדחות את מועד היידוע.

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

16. (א) קבע מנהל בכיר ברשות מוסמכת לפי התוספת השנייה, כי תקיפת סייבר שמתרחשת או שקיים חשש ממשי כי עומדת להתרחש נגד גוף ממשלתי או באמצעותו, היא תקיפת סייבר חמורה הדורשת את מעורבותו והודיע על כך לגוף הממשלתי, יפעל הגוף הממשלתי להתמודדות עם התקיפה בהתאם להוראות העובד המוסמך המגזרי, שינתנו בהתייעצות עם מערך הסייבר הלאומי.

(ב) במתן הוראות לפי סעיף קטן (א) ישקול העובד המוסמך המגזרי את השפעתן האפשרית על פעילות הגוף הממשלתי ועל צד שלישי, לרבות הזכות לפרטיות, ויורה לנקוט באמצעי שפגיעתו פחותה לאיתור התקיפה, מניעתה או בלימתה.

מתן הוראות להתמודדות עם תקיפת סייבר חמורה על ידי מערך הסייבר הלאומי

17. (א) סמכות לפי סעיפים 14, 15 ו-16 תהיה נתונה גם לעובד מוסמך במערך הסייבר הלאומי או מנהל בכיר במערך הסייבר הלאומי, כלפי ארגון חיוני וכלפי ספק שירותים דיגטליים ושירותי אחסון בשינויים המחויבים, ובמקום "ארגון חיוני" בסעיפים אלו, ייקרא "ארגון חיוני או ספקי שירותים דיגיטליים ושירותי אחסון".

(ב) על אף האמור בסעיף קטן (א), עובד מוסמך במערך הסייבר הלאומי יהיה רשאי לנקוט בפעולות לפי סעיפים 15 או 16 כלפי ארגון חיוני, אם קבע ראש מערך הסייבר הלאומי שיש מקום להיענות לבקשת רשות מוסמכת לסיוע בהפעלת סמכויותיה לפי סעיפים 15 או 16, או אם קבע שקיים חשש כי תקיפת סייבר חמורה תתפשט במהירות לארגונים רבים, תתפשט ליותר ממגזר משק אחד, תפגע בבטחון המדינה, או בבטחון הציבור. בסעיף קטן זה- ארגון חיוני- למעט ארגון חיוני ממגזר המשק שמערך הסייבר הלאומי הוא הרשות המוסמכת לגביו בהתאם לתוספת הראשונה.

(ג) החליט מנהל בכיר במערך הסייבר הלאומי על הפעלת סמכות בהתאם לסעיף קטן (ב), יידע בעניין את הרשות המוסמכת, והסמכויות לעניין תקיפת הסייבר נגד הארגון החיוני , יופעלו בהוראת עובד מוסמך של מערך הסייבר הלאומי בלבד, וזאת ככל הניתן בנסיבות העניין, באמצעות הרשות המוסמכת.

סמכות הכרזה של צה"ל

18. (א) הסמכות הנתונה למנהל בכיר לקבוע כי תקיפת סייבר היא תקיפה חמורה לפי סעיף 14 תהיה נתונה לראש חטיבת הגנה בסייבר בצה"ל לעניין תקיפת סייבר חמורה שהוא מצא שמתרחשת או שקיים חשש ממשי שהיא עומדת להתרחש כנגד או באמצעות ארגון חיוני, ארגון חיוני למערכת הביטחון או ספק שירותים דיגיטליים או שירותי אחסון, אם מצא כי יש חשש ממשי שיש בתקיפה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל בשל הנסיבות המפורטות באותו סעיף.

(ב) קבע ראש חטיבת ההגנה בסייבר בצה"ל כאמור בסעיף קטן (א) יראו את הקביעה כקביעת מנהל בכיר במערך הסייבר הלאומי, ולעניין ארגון חיוני למערכת הביטחון כקביעת מנהל בכיר במלמ"ב.

סימן ה': ארגון חיוני למערכת הביטחון

הגדרות

19. בסימן זה –

"גוף מונחה מלמ"ב" – גוף המנוי בפרטים 2 ו-3 לתוספת הראשונה לחוק הסדרת הבטחון בגופים ציבוריים;

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

"מערכת הביטחון" – צה"ל, משרד הביטחון, מלמ"ב וגופים מונחי מלמ"ב;

קביעת ארגון חיוני למערכת הביטחון

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

(1) הארגון מנוי ברשימת הספקים של מערכת הביטחון, ובלבד שהארגון אינו גוף מונחה;

(2) הארגון מספק למערכת הביטחון מוצרים, שירותים או טכנולוגיות וכן מספק או מחזיק ידע, שהם חיוניים לפעילות ביטחונית או מבצעית של מערכת הביטחון, אשר פגיעה בזמינותם ותפקודם עקב תקיפת סייבר עלולה לגרום לפגיעה משמעותית בביטחון המדינה או ברציפות התפקוד של מערכת הביטחון;

(3) היה הארגון ארגון חיוני לפי סעיף 8 לחוק, מצא, לאחר קבלת הסכמת הגורם המאסדר של מגזר המשק כי אין די בהגדרתו כארגון חיוני לצורך מענה לסיכון האמור בפסקה (2);

(4) ניתנה לארגון הזדמנות להשמיע את עמדתו בעניין.

(ב) המלצת ראש מלמ״ב כאמור בסעיף קטן (א) תינתן לאחר שקיים התייעצות עם הרמטכ״ל וקיבל את הסכמת ראש מערך הסייבר הלאומי. לא נתן ראש מערך הסייבר הלאומי הסכמתו , רשאי ראש מלמ״ב להביא את הסוגייה להכרעה בפני ראש המטה לביטחון לאומי.

(ג) קבע שר הביטחון לפי סעיף זה כי ארגון הוא ארגון חיוני למערכת הביטחון או קבע כי אין עוד צורך בהגדרת הארגון שנקבע כאמור כארגון החיוני למערכת הביטחון, יודיע על כך לארגון ויידע בכך את מערך הסייבר הלאומי, צה״ל, וביחס לארגון כאמור בסעיף קטן (א)(3) - הגורם המאסדר של מגזר המשק, , בתוך 14 ימים. קביעת שר הביטחון תיכנס לתוקף במועד מסירת ההודעה על הקביעה לארגון.

(ד) רשימת הארגונים החיוניים למערכת הביטחון לא תפורסם לציבור.

(ה) נקבע ארגון כארגון חיוני למערכת הביטחון, לא יוגדר כארגון חיוני לפי סעיף 8 לחוק ממועד קביעת שר הביטחון וכל עוד לא קבע אחרת.

סמכויות כלפי ארגון חיוני למערכת הביטחון

21. (א) סמכות הנתונה לפי חוק זה לגורם מסמיך ברשות מוסמכת, למנהל בכיר ברשות מוסמכת, לעובד מוסמך מגזרי ולממונה, תהיה נתונה בהתאמה לעובדי מלמ״ב, בשינויים המחוייבים, כלפי ארגון חיוני למערכת הביטחון.

(ב) סמכות הנתונה לפי חוק זה לגורם מאסדר תהיה נתונה לשר הביטחון כלפי ארגון חיוני למערכת הביטחון.

חובות ארגון חיוני למערכת הביטחון

22. נקבע ארגון כארגון חיוני למערכת הביטחון, יחולו לגביו הוראות החוק החלות על ארגון חיוני בשינויים המחויבים, למעט הסמכויות לפי סעיף 17 לחוק; ואולם ההוראות לפי סעיפים 10(ב) עד 10(ד) לחוק, יחולו לגבי הארגון החל מתום 6 חודשים ממועד הקביעה כאמור.

פרק ה׳: עיצום כספי

סימן א׳: עיצום כספי

עיצום כספי

23. (א) הפר ארגון חיוני לפי סעיף 8(א)(2) או 8(א)(3) שאינו ארגון חיוני לפי פרט 7 בתוספת הראשונה, הוראה מההוראות המפורטות בתוספת הרביעית, המפורטות בטור א׳ בתוספת החמישית, רשאי הממונה להטיל עליו עיצום כספי לפי הוראות פרק זה, בסכום הקבוע לגביו בטור ב׳ לצד אותה הוראה לפי העניין.

(ב) הפר ארגון חיוני לפי סעיף 8(א)(2) או 8(א)(3) שאינו ארגון חיוני לפי פרט 7 בתוספת הראשונה, הוראה מהוראות חוק זה כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בסכום של 300,000 שקלים חדשים:

(1) לא מילא הוראות מקצועיות שניתנו על ידי ראש מערך הסייבר הלאומי בניגוד לסעיף 10(ה);

(2) לא מסר לעובד מוסמך מגזרי בכתב, מידע או מסמך שהיה עליו לשמור בהתאם להוראות סעיף 10(ו) לפי דרישה שנמסרה לו בכתב, במועד או באופן שנקבעו בדרישה, בניגוד להוראות לפי סעיף 12;

(3) לא דיווח על תקיפת סייבר בניגוד להוראות סעיפים 11(א)-(ג) או לא מסר דיווח מסכם בניגוד להוראות סעיף 11(ד).

(ג) לא מילא ארגון חיוני לפי סעיף 8(א)(2) או 8(א)(3) שאינו ארגון חיוני לפי פרט 7 בתוספת הראשונה, או ספק שירותים דיגיטליים ושירותי אחסון הוראה לביצוע פעולות להגנת סייבר בחומר מחשב או הוראה למסירת ידיעה או מסמך, שניתנה לו בכתב, לפי סעיפים 15(א)(4) או 17, הנדרשת לשם איתור תקיפת סייבר חמורה, מניעתה או בלימתה רשאי הממונה להטיל עליו עיצום כספי בסכום של 300,000 שקלים חדשים.

(ד) לא יטיל הממונה עיצום כספי לפי חוק זה אם יש לרשות המוסמכת סמכות להטיל עיצום כספי בגין אותן נסיבות מכח חוק אחר.

הודעה על כוונת חיוב

24. (א) היה לממונה יסוד סביר להניח כי ארגון כאמור בסעיף 23 הפר הוראה מההוראות לפי חוק זה, (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 בפני הממונה לפי הוראות סעיף 25 וכי יראו את ההודעה על כוונת חיוב כדרישת תשלום אם המפר לא יממש את הזכות האמורה, כאמור בסעיף 26(ד);

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

זכות טיעון

25. מפר שנמסרה לו הודעה על כוונת חיוב לפי הוראות סעיף 24 רשאי לטעון את

טענותיו, בכתב, בפני 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 שירשמו.

החלטת הממונה ודרישת תשלום

26. (א) הממונה יחליט, לאחר ששקל את הטענות שנטענו לפי סעיף 25, אם להטיל על המפר עיצום כספי, ורשאי הוא להפחית את סכום העיצום הכספי לפי הוראות סעיף 28.

(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), שבה 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 25, בתוך התקופה האמורה באותו סעיף, יראו את ההודעה על כוונת החיוב, בתום אותה תקופה, כדרישת תשלום שנמסרה למפר במועד האמור.

הפרה נמשכת והפרה חוזרת

27. (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 מנהלית.

(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

28. (א) הממונה אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה ובתוספת החמישית, אלא לפי הוראות סעיף קטן (ב).

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

סכום מעודכן של העיצום הכספי

29. (א) העיצום הכספי יהיה לפי סכומו המעודכן ביום מסירת דרישת התשלום, ולגבי מפר שלא טען את טענותיו בפני הממונה כאמור בסעיף 26(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

30. על המפר לשלם את העיצום הכספי בתוך 30 ימים מיום מסירת דרישת התשלום כאמור בסעיף 26.

הפרשי הצמדה וריבית

31. לא שילם המפר עיצום כספי במועד, תיווסף על העיצום הכספי, לתקופת הפיגור, ריבית שקלית ודמי פיגורים לפי חוק פסיקת ריבית והצמדה, התשכ"א-1961[7], (בפרק זה – חוק פסיקת ריבית והצמדה).

פריסת תשלום העיצום הכספי

32. (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) עמד המפר בפריסת התשלומים כאמור, לא יתווספו לחובו דמי פיגורים בתקופת הפריסה.

(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 30.

גבייה

33. עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה-1995.

סימן ב: התראה מנהלית

[7] ס"ח תשכ"א 348, עמ' 192.

התראה מנהלית

34. (א) היה לממונה יסוד סביר להניח כי ארגון הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 23, והתקיימו נסיבות שקבע ראש מערך הסייבר הלאומי, בנהלים, באישור היועץ המשפטי לממשלה, רשאי הממונה, להטיל עליו עיצום כספי לפי הוראות סימן א', 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 יהא צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין כאמור בסעיף 27 וכן יציין את זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 35.

בקשה לביטול התראה מנהלית

35. (א) נמסרה למפר התראה מינהלית כאמור בסעיף 34, 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.

הפרה נמשכת והפרה חוזרת לאחר התראה

36. (א) נמסרה למפר התראה מנהלית לפי הוראות סימן זה והמפר המשיך להפר את ההוראה שבשלה נמסרה לו ההתראה, יראו את ההפרה כאמור כהפרה נמשכת לעניין סעיף 27, והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה הנמשכת, בהתאם להוראות סעיף 24, 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 27(ב), והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה החוזרת, בהתאם להוראות סעיף 24, בשינויים המחויבים.

סימן ג': שונות

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

37. על מעשה אחד המהווה הפרה של הוראות לפי חוק זה המנויות בסעיף 23 וכן מהווה הפרה לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד.

עיכוב ביצוע והחזר

38. (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

39. (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

(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 מנהליים 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[8], 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) הגורם המסמיך ברשות המוסמכת רשאי לקבוע דרכים נוספות לפרסום הפרטים האמורים בסעיף זה.

שמירת אחריות פלילית

40. (א) תשלום עיצום כספי או מסירת התראה מנהלית, לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה המנויות בפרק ז', 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.

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

שינוי התוספת החמישית

41. גורם מאסדר המנוי בטור ה' בתוספת הראשונה, אשר קבע תקנות לפי סעיף 10(ג), רשאי, בהתייעצות עם ראש מערך הסייבר הלאומי, בהסכמת שר המשפטים, ובאישור ועדת החוץ והביטחון של הכנסת, להוסיף פרטים חדשים לפרק א' בתוספת החמישית ביחס למגזרו ובלבד שסכום העיצום הכספי שייקבע בטור ב' לתוספת ביחס להפרות הנוספות לא יעלה על 640,000 שקלים חדשים.

פרק ו': סיוע להגנת סייבר

[8] ס"ח תשנ"ח 1667, עמ' 226.

סיוע מערך הסייבר לארגון המעוניין בכך

42. (א) במסגרת סיוע בהגנת סייבר של מערך הסייבר הלאומי, לארגון המעוניין בכך, רשאי עובד מערך הסייבר הלאומי לבצע פעולות סיוע הכרוכות בקבלת מידע אישי בתנאים הבאים:

(1) הוסברו לנציג הארגון כל אלה:

(א) הטעם המקצועי לסיוע;

(ב) הפעולות שיתבצעו כחלק מהסיוע ;

(ג) זכותו של הארגון שלא לקבל את הסיוע.

(2) לארגון יש מדיניות בנוגע לגישה ולעיבוד מידע אישי במסגרתה הובהרה אפשרות להעברת מידע אישי לצרכי הגנת הסייבר. ואולם, אם נדרש מתן סיוע דחוף לארגון שאין לו מדיניות כאמור, יכול שיינתן הסיוע אם התחייב הארגון ליידע את עובדיו על קבלת הסיוע בהגנת הסייבר ולפרסם מדיניות כאמור סמוך ככל הניתן לאחר קבלת הסיוע.

(3) במסגרת סיוע בהגנת סייבר לפי סעיף זה:

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

(ב) יעשה עובד מערך הסייבר הלאומי שימוש בטכנולוגיות ובשיטות פעולה באופן שיצמצם ככל האפשר את חשיפתו למידע אישי, ובכלל האמור כל אלה:

(1) מידע העלול לכלול מידע אישי לא יעובד על ידי אדם אלא אם קבע מנהל מוסמך כי אופי פעולת הסיוע מחייבת עיבוד על ידי אדם, ובכלל זה אם קיים חשש לתקיפת סייבר אשר המידע נדרש לבחינתה, או אם נדרש לבצע מבדק חדירות למערכות הארגון;

(2) עיבוד אדם כאמור בפסקה (1):

(א) יבוצע על ידי מורשי גישה בלבד אשר עברו הכשרה לעניין הגנה על מידע אישי כפי שיקבע ראש מערך הסייבר הלאומי;

(ב) יתועד באופן שיאפשר פיקוח ובקרה על אופן ביצועה, על מועד ביצועה ועל זהות מבצע הפעולה. תיעוד לפי פסקה זו יישמר על ידי מערך הסייבר הלאומי למשך 3 שנים לפחות.

(4) פעולת סיוע להגנת סייבר בחומר מחשב, למעט פעולה בהעתק חומר מחשב שנמסר למערך הסייבר הלאומי, תתבצע על ידי נציג הארגון.

(5) על אף האמור בסעיף קטן (4), מטעמים מיוחדים ובאישור ראש מערך הסייבר הלאומי פעולת סיוע להגנת סייבר בחומר מחשב תתבצע על ידי מערך הסייבר הלאומי לבקשת הארגון בכתב ובנוכחות נציג הארגון.

(ב) ארגון שקיבל סיוע בהגנת הסייבר רשאי בכל עת להודיע בכתב למערך הסייבר הלאומי שאינו מעוניין בו עוד, והסיוע יופסק בהקדם האפשרי.

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

(ד) מתן סיוע של מערך הסייבר הלאומי להגנת הסייבר לפי סעיף זה לארגון במגזר משק יבוצע לאחר התייעצות עם הרשות המוסמכת.

(ה) סיוע לפי סעיף זה יכול שינתן גם על ידי רשות מוסמכת לעניין מגזר המשק במסגרת הפעלת מרכז שליטה ובקרה מגזרי, והכל בשינויים המחויבים.

(ו) בסעיף זה:

"ארגון" – ארגון אשר קבע ראש מערך הסייבר הלאומי כי קיים אינטרס לאומי בסיוע לו לפי סעיף זה, או ארגון שקבע מנהל בכיר במערך הסייבר הלאומי כי קיים אינטרס לאומי לסייע לו לפי סעיף זה אגב תקיפת סייבר נגדו או באמצעותו;

"סיוע בהגנת סייבר" פעולות לצורך סיוע במניעת, איתור או התמודדות עם תקיפת סייבר, לרבות, פעולות הכרוכות בקבלת מידע בעל ערך הגנתי באופן חד פעמי או רציף או בקבלת גישה למחשב או לחומר מחשב;

"עיבוד" – כהגדרתו בחוק הגנת הפרטיות.

איתור פגיעויות במרחב

43. (א) עובד מערך הסייבר הלאומי רשאי, לצורך ביצוע תפקידיו, לפעול לאיתור פגיעויות חמורות המוכרות לו ולמתן התראה עליהן.

(ב) פעולות כאמור בסעיף קטן (א), ייעשו במטרה לאתר את הפגיעויות בארגונים, באופן שאינו מאפשר גישה למערכות מחשוב שיש הגבלה על נגישותן לציבור מרשת האינטרנט או מרשת ציבורית אחרת ואשר לא צפויה להיות לו השפעה משמעותית על תפקוד מחשב שביחס אליו מאותרת הפגיעות החמורה, תוך מיקוד במידע הטכנולוגי המצומצם ביותר המאפשר לזהות את קיומה או היעדרה של הפגיעות החמורה, תוך ניסיון שלא להיחשף למידע אישי, וללא איסוף מידע אישי.

פרק ז': עונשין

עונשין

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

(1) לא נקט באמצעים שעליהם הורה ראש מערך הסייבר הלאומי בניגוד לסעיף 10(ה);

(2) לא מילא הוראה שניתנה על-ידי עובד מוסמך מגזרי או עובד מוסמך מטעם מערך הסייבר הלאומי, לפי העניין, בניגוד לסעיף 15(א)(4), 16(א), או 17(ב).

(ב) היתה 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.

45. (א) נושא משרה בתאגיד חייב לפקח ולעשות כל שניתן למניעת עבירות לפי סעיף 44(א) בידי תאגיד או בידי עובד בתאגיד; 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.

(ב) נעברה עבירה לפי סעיף 44(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.

46. אדם שגילה מידע אישי שהתקבל מארגון לפי חוק זה או עשה שימוש במידע אישי שהתקבל מארגון לפי חוק זה, בניגוד להוראות סעיף 49, דינו – מאסר שלוש שנים.

פרק ח': הוראות שונות

חוות דעת מקדמית

47. (א) רשות מוסמכת תיתן לבקשת ארגון חיוני, חוות דעת מקדמית, על התאמת אופן יישום דרישה המנויה בתוספת הרביעית.

(ב) רשות מוסמכת רשאית לדרוש ידיעות ומסמכים נוספים הדרושים לה לצורך מתן חוות הדעת המקדמית.

הסתייעות במומחה

48. (א) לשם הפעלת סמכויות עובד מוסמך מגזרי או עובד מוסמך במערך הסייבר הלאומי לפי חוק זה, וכן לשם הפעלת סמכויות עובד לפי סעיפים 42 ו- 43 (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 יחודיים.

(ב) מומחה חיצוני יפעל מטעמו של עובד מוסמך בהתאם להנחייתו ולהוראותיו ובפיקוחו; מומחה חיצוני לא יפעיל סמכות הכרוכה בהפעלה של שיקול הדעת שניתן לרשות מוסמכת או לעובדיה או למערך הסייבר הלאומי או לעובדיו.

(ג) כניסת מומחה חיצוני למקום לפי סעיף 13 המבוצעת ללא עובד מוסמך מגזרי הנוכח במקום, תיעשה בתנאים המפורטים בסעיף 13, ובתנאי שהמקום אינו מקום מגורים 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 ולחזור בו מהסכמתו עד לתחילת בחינת המומחה החיצוני.

(ד) מנהל בכיר ברשות מוסמכת או מנהל בכיר במערך הסייבר הלאומי לפי העניין (להלן 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 או הוגש נגדו כתב אישום בעבירה כאמור.

(ה) מומחה חיצוני יעמוד בתנאים הבאים:

(1) לא ימונה כמומחה חיצוני ולא יכהן כמומחה חיצוני כאמור 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.

(ו) הרואה עצמו נפגע מפעולה של מומחה חיצוני, רשאי לפנות בתלונה מנומקת בכתב, לגורם המאשר לפי סעיף קטן (ד); הגורם המאשר יבחן את התלונה ויענה לפונה בתוך 45 ימים; מצא הגורם המאשר שהתלונה היתה מוצדקת – יודיע על כך למתלונן ולמומחה החיצוני, בצירוף החלטתו; מצא הגורם המאשר שהתלונה לא היתה מוצדקת, יודיע על כך בכתב למתלונן ולמומחה החיצוני.

(ז) דינו של מומחה חיצוני כדין עובדי המדינה לעניין ההוראות הנוגעות לעובדי הציבור בחוק העונשין, וההוראות בחוק שירות הציבור (מתנות), התש"ם-1979[9].

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

(ט) 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[10] ;

"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.

סודיות, הגבלת שימוש ומחיקה

49. (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, או למטרת ביצוע סמכות של אדם להגנת סייבר לפי דין, או לפי צו בית משפט.

(ב) מידע אישי שהתקבל לפי חוק זה יישמר בהיקף המזערי הנדרש, וימחק לאחר שנתיים לכל היותר מעת קבלתו, אלא אם הוא חיוני לזיהוי מאפייני תקיפת סייבר או להתמודדות עם תקיפת סייבר או חשש לה או שהוא נדרש להליכים לפי פרק ה' או פרק ז'.

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

---

[9] ס"ח תש"ם 944, עמ' 2 ;
[10] ס"ח תשכ"ח 541 , עמ' 234 ;

תיעוד

50. עובד מוסמך מגזרי או עובד מוסמך במערך הסייבר הלאומי יתעד בכתב את ההוראות שניתנו לארגון לפי סעיפים 15, 16 או 17 וימסור לו נוסח כתוב של ההוראות שאינו מכיל מידע מסווג, ברמת "שמור" ומעלה, בהקדם האפשרי לאחר מתן ההוראה.

אסדרה

51. אסדרה לעניין הגנת סייבר או שיש לה השפעה משמעותית על הגנת סייבר, תיקבע לאחר התייעצות עם ראש מערך הסייבר הלאומי. בסעיף זה "אסדרה" – כהגדרתה בחוק עקרונות האסדרה, תשפ"ו-2021[11].

תצהיר ופטור

52. (א) הגיש ארגון חיוני ממגזר המנוי בתוספת השישית למנהל בכיר ברשות מוסמכת, תצהיר בדבר יישום הנחיות הגנת סייבר בהתאם לתקן, לעניין פעילות הליבה של הארגון בצירוף האישור המנוי בתוספת השישית, לא יחולו על הארגון החובות החלות על ארגון חיוני לפי חוק זה למעט החובה לפי סעיף 11, לתקופה של שנתיים החל מיום מסירת התצהיר.

(ב) הגיש ספק שירותים דיגטליים ושירותי אחסון, שאינו ארגון חיוני, למנהל בכיר ברשות מוסמכת תצהיר בדבר אספקת שירותי האחסון, השירותים הדיגיטליים, או אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור, תוך יישום הוראות התקן לעניין שירותי הליבה אותם מספק או לעניין השירותים כאמור שנגדם בוצעה התקיפה בצירוף אישור המנוי בתוספת השישית, לא יחולו על הספק הוראות סעיף 17 לתקופה של שנתיים.

(ג) גורם מאסדר רשאי, לאחר התייעצות עם ראש מערך הסייבר הלאומי, להוסיף לתוספת השישית מגזר משק שאינו מנוי בו, אם מצא כי עמידה בתקן מקנה את רמת ההגנה הגבוהה הנדרשת בהתאם לסעיף זה, בשים לב למאפייני הפעילות היחודיים לארגונים חיוניים במגזר, וכן רשאי הוא לקבוע תנאים נוספים לתקן האמור לצורך כך.

(ד) בסעיף זה התקן- NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (control baseline for Moderate or High impact)

שמירת דינים

53. (א) הוראות חוק זה באות להוסיף על חוק שירות הביטחון הכללי, תשס"ב-2002[12] ועל הוראות כל דין ולא לגרוע מהן.

(ב) מבלי לגרוע מהוראות סעיף קטן (א), הוראות חוק זה באות להוסיף על החלטות מנהל, החלטות ממשלה או הסכם קיים או עתידי, בעניין הנוגע להגנת הסייבר, אולם במקרה של סתירה, יגברו הוראות חוק זה.

---

[11] ס"ח תשפ"ב 2933, עמ' 125;
[12] ס"ח תשמ"ו 1170, עמ' 107.

קבלת אגבית של מידע מתקשרות בין מחשבים

54. קבלת מידע מתקשרת בין-מחשבים אגב ביצוע פעולות לשם הגנת סייבר בחומר מחשב לפי חוק זה, לא תיחשב האזנת סתר לפי חוק האזנת סתר, התשל"ט- 1979[13].

דיווח

55. (א) ראש מערך הסייבר הלאומי יציג לועדת החוץ והביטחון של הכנסת אחת לשנה, דוח על תמונת המצב של רמת הגנת הסייבר הלאומית ועל הפעולות שננקטו על-ידי המערך לצורך חיזוק החוסן הלאומי בהגנת הסייבר וקידום 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 שקבע מאסדר כי יוחרגו מהגדרת ארגון חיוני אף שעמדו בתבחינים המגזריים, או שנכללו כארגון חיוני על אף שלא עמדו בתבחינים, לפי סעיף 8(ב), בחלוקה למגזרים והנימוק שנקבע לכך;

(2) מספר ההוראות שניתנו לפי סעיף 10(ה) וסוגי הארגונים להן ניתנו; וביחס לכל הוראה שניתנה לפי סעיף 10(ה), על מהות ההוראה שניתנה והאם ניתן אישור ראש הממשלה בטרם מתן ההוראה וסוגי הארגונים להן ניתנו.

(ג) הדוח והדיווחים לפי חוק זה יהיו חסויים ופרסומם אסור.

תקנות

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

תיקון חוק בתי משפט לעניינים מנהליים

57. בחוק בתי משפט לענינים מינהליים, התש"ס-2000[14], בתוספת הראשונה בסופה יבוא:

"69. החלטה לפי החוק להגנת הסייבר הלאומית, התשפ"ו- 2026 למעט החלטות הממשלה".

תיקון חוק חופש המידע

58. בחוק חופש המידע, תשנ"ח-1998[15], בסעיף 14(א)(17), בסופו יבוא:

"(17) וכן פעילות חטיבות מערך הסייבר הלאומי העוסקות בהגנת סייבר מול המשק, או בהגנת הסייבר של המערך, ופעילות יחידת הביטחון במערך הסייבר הלאומי."

תחולה ותחילה

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

---

[13] ס"ח תשל"ט 938, עמ' 118.
[14] ס"ח תש"ס 1739, עמ' 190
[15] ס"ח תשנ"ח 1667, עמ' 226.

(ב) על אף האמור בסעיף קטן (א), תחולת סעיפים 10(ב)-(ג), 11, 15 ו-17 12 חודשים מיום פרסום החוק.

תוספת ראשונה

(סעיפים 1, 9)

טור א' **מגזר משק**	**טור ב'** **תת ענף מגזר משק (אם נדרש)**	**טור ג'** **רשות מוסמכת**	**טור ד'** **הגורם המסמיך**	**טור ה'** **שר ממונה או גורם מאסדר**
1. תקשורת		משרד התקשורת	מנכ"ל משרד התקשורת	שר התקשורת
2. אנרגיה		משרד האנרגיה	מנכ"ל משרד האנרגיה	שר האנרגיה
3. בריאות		משרד הבריאות	מנכ"ל משרד הבריאות	שר הבריאות
4. כימיקלים/ רעלים/ חומרים מסוכנים		המשרד להגנת הסביבה	מנכ"ל המשרד להגנת הסביבה	השר להגנת הסביבה
5. מים וביוב		הרשות הממשלתית למים ולביוב	מנהל הרשות הממשלתי למים וביוב	מועצת רשות המים והביוב

טור א' מגזר משק	טור ב' תת ענף מגזר משק (אם נדרש)	טור ג' רשות מוסמכת	טור ד' הגורם המסמיך	טור ה' שר ממונה או גורם מאסדר
6. תחבורה	(1) תחבורה ציבורית יבשתית (2) תחבורה ימית (3) תחבורה אוויריות (4) תשתיות תחבורתיות וניהוליות	משרד התחבורה	מנכ"ל משרד התחבורה	שר התחבורה
7. רשויות מקומיות		מערך הסייבר הלאומי	ראש מערך הסייבר הלאומי	ראש הממשלה
8. משכ"ל		משרד הכלכלה	מנכ"ל משרד הכלכלה	שר הכלכלה
9. שירותים דיגיטליים ושרותי אחסון		מערך הסייבר הלאומי	ראש מערך הסייבר הלאומי	ראש הממשלה

טור א' מגזר משק	טור ב' תת ענף מגזר משק (אם נדרש)	טור ג' רשות מוסמכת	טור ד' הגורם המסמיך	טור ה' שר ממונה או גורם מאסדר
10. חקלאות		משרד החקלאות ובטחון המזון	מנכ"ל משרד החקלאות ובטחון המזון	שר החקלאות ובטחון המזון

תוספת שנייה

(סעיפים 9,1)

טור א' מגזר במשק	טור ב' תת מגזר (אם נדרש)	טור ג' רשות מוסמכת	טור ד' הגורם המסמיך	טור ה'
משרדי הממשלה		מערך הדיגטל	ראש מערך הדיגטל	השר האמון על מערך הדיגיטל כפי שתקבע הממשלה בהחלטותיה

תוספת שלישית

(סעיף 8(א))

טור א' מגזר המשק	טור ב' תת-מגזר	טור ג' התבחין
1. תקשורת		ספק מורשה כהגדרתו בחוק התקשורת (בזק ושידורים), התשמ"ב–1982[16] (בפרט זה- חוק התקשורת), ובלבד שיש לו לכל הפחות אחד מאלה: 1. 200,000 מנויים, כהגדרתו בחוק התקשורת; 2. 200,000 יחידים המקבלים שירות בזק, כהגדרתו בחוק התקשורת, מכוח הסכם התקשרות, בין שהתקשרו עם הספק המורשה באופן ישיר ובין שאחרים התקשרו עם הספק המורשה למענם, ובלבד שאינם מספקים שירות בזק לאחר.

[16] ס"ח תשמ"ב 1060, עמ' 218.

2. אנרגיה	חשמל	אחד מאלה: 1. ארגון שבבעלותו או בשליטתו הישירה או העקיפה מיתקנים המשמשים לייצור חשמל בהספק מצטבר העולה על 100 מגוואט. 2. ארגון המנהל מיתקנים המשמשים לייצור חשמל בהספק מצטבר העולה על 100 מגוואט ולו שליטה ובקרה על פעילות ייצור החשמל במתקנים כאמור.
	גז טבעי	בעל רישיון חלוקה או בעל רשיון גז טבעי דחוס
	דלק וגפ"מ	גפ"מ – ארגון אשר מושך מבתי זיקוק או מייבא גפ"מ בכמות שנתית של-20,000 טון או יותר. דלק- ארגון המושך בנזין, סולר וקרוסין במסופים בכמות שנתית של-200,000 קוב או יותר.
3. בריאות		אחד מאלה: 1.בית חולים כללי כהגדרתו בחוק התחשבנות בין בתי חולים לקופות חולים לשנים 2021 עד 2025 (התחשבנות בעד שירותי בריאות בבתי חולים ציבוריים כלליים), תשפ"ב-2021[17]. 2. קופת חולים ששר הבריאות הכיר בה לפי חוק ביטוח בריאות ממלכתי, התשנ"ד-1994[18].
4. כימיקלים, רעלים וחומרים מסוכנים		ארגון העומד בכל התנאים הבאים: (א) הוא אחד מאלה: 1. מפעלי טיפול, סילוק או השבה של פסולת מסוכנת לרבות קרקע מזוהמת, כאמור בפריט 5.1 לתוספת השלישית לחוק החומרים המסוכנים, תשנ"ג-1993[19] (להלן בפרט זה- התוספת השלישית);

[17] ס"ח תשפ"ב 2932 ,עמ' 20.
[18] ס"ח תשנ"ד 1469 , עמ' 156.
[19] ס"ח תשנ"ג 1408, עמ' 28.

		2. מטמנה, למעט מטמנה לפסולת אינרטית כאמור בפריט 5.4 לתוספת השלישית; 3. ארגון העוסק בפעילות של אחסון זמני של פסולת מסוכנת לפני העברתה לטיפול או סילוק כמפורט בפרטים 5.1, 5.4, 5.6 ו- 5.7 למעט אחסון זמני, לפני איסוף, באתר שבו נוצרה כאמור בפריט 5.5 לתוספת השלישית. (ב) הארגון מוכרז כמפעל חיוני, כהגדרתו בחוק שירות עבודה בשעת- חירום, תשכ"ז-1967[20].
5. מים וביוב		אחד מאלה: 1. תאגיד מים שלו 250,000 משתמשים מחוברים ומעלה; 2. מתקן טיהור שפכים שמספר התושבים שמזרימים אליו שפכים הוא 500,000 לפחות; 3. מתקן טיהור שפכים שכמות מי הקולחין המטוהרים שהוא מפיק ומשמשים להשקיה חקלאית עולה על 80 מלמ"ק בשנה; 4. מתקן התפלה שכמות המים המותפלים שהוא מפיק עולה על 80 מלמ"ק בשנה.
6. תחבורה	תחב"צ יבשתית	אחד מאלה: 1. מפעיל תחבורה ציבורית המסיע יותר מ-14 מיליון נוסעים בשנה או בעל 1000 כלי רכב ציבוריים או יותר; 2. בעל היתר הפעלה למערכת מסילת ברזל מקומית על פי תקנות מסילות הברזל תשע"ב-2012; 3. מפעיל תחבורה ציבורית באמצעות מערכות ייחודיות (רכבל, אוטונמיה וכד').
		אחד מאלה:

[20] ס"ח תשכ"ז 503, עמ' 86.

	תחבורה אוירית	1. מפעיל אווירי שהוא בעל רישיון הפעלה אווירית לפי הפרק השלושה עשר לתקנות הטיס (הפעלת כלי טיס וכללי טיסה), התשמ״ב-1981 2. מכון בדק הנותן שירותים למפעיל אווירי כאמור בפסקה (1). 3. בעל רישיון הפעלה ליחידת נת״א לכטב״מ
	תחבורה ימית	אחד מאלה: 1. מפעיל שירותי ספנות שנפח ההובלה הימית שבאחריותו מהווה לפחות 20% מתנועת המטענים אל ישראל וממנה, במהלך שנים עשר חודשים רצופים. 2. חברת נמל או תאגיד מורשה כהגדרתו בחוק רשות הספנות והנמלים, התשס״ד-2004[21].
	תשתיות תחבורתיות וניהוליות	אחד מאלה: 1. חברה ממשלתית, תאגיד או זכיין המורשים על ידי הממשלה לניהול דרך או רשת דרכים בינעירוניות. 2. חברת תשתית ממשלתית שהוכרה כזרוע ביצוע של משרד התחבורה. 3. מרכז ניהול תנועה מטרופוליני גדול (ת״א, ירושלים, חיפה, ב״ש).
7. רשויות מקומיות		רשות מקומית שלה 90,000 תושבים רשומים או יותר.
8. משכ״ל	יצור ושיווק מזון	אחד מאלה: 1. מחסן חירום יעודי המאחסן מוצרי מזון חיוניים כפי שקבעה הרשות העליונה למזון במשרד הכלכלה;

[21] ס״ח תשס״ד 1951, עמ׳ 456.

		2. ארגון העוסק בייצור, עיבוד, אריזה או שיווק לציבור של מוצרי מזון, המחזיק בנתח שוק של 15% או יותר, באחת או יותר מתתי הקטגוריות של מזון המוגדרות כקטגוריות ליבה לפי תקן COICOP 01.1.x ; 3. ארגון המפעיל מערך לוגיסטי לשינוע, אחסון ושיווק מזון, לרבות בקירור,המחזיק בנתח שוק של 15% או יותר משוק הפצת המזון הארצי ; 4. ארגון קמעונאי מזון המחזיק בנתח שוק של 4% או יותר ממכירות המזון לציבור בישראל.
9. שירותים דיגיטליים ושירותי אחסון		ספק שירותים דיגיטליים או שירותי אחסון, למעט ספק כאמור אשר כל שירותיו ניתנים מחוץ לישראל, והעומד בכל אלה: א. אחד מהתנאים הבאים: (1) בעל מחזור כספי שנתי של 40 מלש"ח ומעלה ; (2) מעסיק 50 עובדים או יותר ; (3) מספק לממשלת ישראל או לגוף מונחה-שירותים דיגיטליים או שירותי אחסון מהסוג המנוי בפסקה (ב) בפרט זה. ב. מספק אחד מאלה לפחות: 1. ספק נקודת חילוף אינטרנט (IXP): ספק המעמיד לרשות אחרים מתקן רשת המאפשר חיבור גומלין בין יותר משתי רשתות עצמאיות, לשם העברת תעבורת אינטרנט ביניהן. 2. רשם שמות מתחום (Domain Registrar): ספק המוסמך למכור שמות מתחם (Domains) לציבור הרחב ולנהל את הרישום שלהם מול המרשם.

		3. ספק DNS: ספק המספק שירותי ניתוב שמות מתחם לרשת האינטרנט, לרבות שירותי ניתוב רקורסיביים לציבור המשתמשים או שירותי ניתוב סמכותיים עבור צדדים שלישיים, והוא אינו מפעיל שרתי שמות שורשיים. 4. מנהל מרשם TLD: ספק שהוקנתה לו סיומת אינטרנט מסוימת והוא אחראי לניהול אותה סיומת, לרבות רישום שמות מתחם וההפעלה הטכנית של אותה סיומת. 5. שירות מחשוב ענן (Cloud Computing): שירות של אספקת תשתית דיגיטלית המאפשר גישה מרחוק, לפי דרישה, למאגר משאבי מחשוב הניתנים להרחבה ולשיתוף, ובכלל זה משאבי רשת, שרתים, אחסון, יישומים או שירותים דיגיטליים אחרים. 6. שירות מרכז נתונים (Data Center) ואירוח: שירות הכולל החזקה, הפעלה או ניהול של מבנה או קבוצת מבנים המיועדים לאירוח, חיבור ותפעול מרכזי של ציוד טכנולוגיית מידע ותקשורת ורשת, המספקים שירותי אחסון, עיבוד או העברת נתונים, ובכלל זה שירותי אחסון של אתרי אינטרנט, שירותי אחסון של מדיות וגיבוי פיזי/לוגי, וכן המתקנים הנדרשים לאספקת חשמל ולבקרת סביבה לצורך כך. 7. רשת אספקת תוכן (CDN): רשת של שרתים מבוזרים גיאוגרפית למטרת הבטחת זמינות גבוהה, נגישות או אספקה מהירה של תוכן ושירותים דיגיטליים למשתמשי אינטרנט בשם ספקי תוכן ושירותים. 8. שירות אמון אלקטרוני (Trust Service):

		שירות אלקטרוני שמטרתו יצירה, אימות או אימות נוסף של חתימות אלקטרוניות, חותמות אלקטרוניות, חותמות זמן אלקטרוניות, שירותי מסירה רשומה אלקטרונית, תעודות לאימות אתרים, או שימור חתימות או חותמות אלקטרוניות. 9. שירות הפצת מסרים קצרים (SMS): פלטפורמה להפצת דיוור או הודעות טקסט קצרות או התראות אוטומטיות המיועדות לציבור הרחב או ללקוחות עסקיים. 10. שירות ניהול זהויות וגישה (IAM): שירות המספק מערכת או תהליך לאימות זהות משתמשים, ניהול הרשאות וניהול גישה מאובטחת למערכות ארגוניות, לרבות אימות רב-שלבי או גישה מאוחדת. 11. שירות תיווך תעבורה (Reverse Proxy): שירות מנוהל המספק סינון ותיווך תעבורה בין רשת פנימית לבין רשת האינטרנט, לרבות איזון עומסים, הסתרת כתובות או הגנה מפני תקיפות. 12. שירות ניהול ממשקי תוכנה (API Management): שירות המנהל, מנטר ומגן על ממשקי תוכנה בין גופים שונים, לרבות שער API וממשקי בנקאות פתוחה. 13. שירות טכנולוגיית מידע מנוהל (MSP): שירות מנוהל הכולל התקנה, ניהול, תפעול או תחזוקה של מוצרי טכנולוגיית מידע ותקשורת, רשתות, תשתיות, יישומים או כל רשת או מערכת מידע אחרת, לרבות באמצעות סיוע או ניהול פעיל באתר הלקוח או מרחוק.

		14. שירות אבטחת סייבר מנוהל (MSSP): שירות תקשוב מנוהל שמטרתו ניהול סיכוני אבטחת סייבר של הלקוח, כולם או חלקם, לרבות ניטור, זיהוי, תגובה או ייעוץ שוטף, לרבות מודיעין על איומי סייבר. 15. שירות למערכות תפעוליות ותעשייתיות (OT/ICS/SCADA/IoT): שירות מנוהל הכולל התקנה, אינטגרציה, ניהול או תחזוקה של מערכות תפעוליות, מערכות בקרה תעשייתיות או רכיבי אינטרנט של הדברים, המשמשים להפעלה, שליטה, אבטחה או בקרה על תהליכים תעשייתיים או תפעוליים. 16. שירותי ישומי ליבה עסקיים (SaaS/PaaS עסקי): שירות דיגיטלי המאפשר שימוש בישומי ניהול ארגוניים או במערכות מידע ארגוניות, וכן פיתוחם, תחזוקתם או הנגשתם, בין אם הוא ניתן כתוכנה (Software as a Service – SaaS), כטפלטפורמה (Platform as s Service – PaaS), באמצעות התקנה מקומית אצל הלקוח, או בכל אמצעי טכנולוגי אחר. 17. שוק מקוון: שירות דיגיטלי המאפשר לצרכנים ולספקים להתקשר ביניהם בחוזי מכר או מתן שירותים באמצעות תקשורת אלקטרונית. 18. מנוע חיפוש מקוון: שירות דיגיטלי המאפשר למשתמשים לבצע חיפוש, רחב של אתרי אינטרנט, על בסיס שאילתה בכל נושא, ומציג תוצאות הכוללות קישורים למקורות מידע הקשורים לתוכן המבוקש. 19. פלטפורמת רשת חברתית: שירות דיגיטלי המאפשר למשתמשים ליצור ביניהם

		קשר, לשתף, לגלות או להחליף תכנים, לרבות באמצעות מסרים, פרסומים, סרטונים או המלצות, על פני מכשירים שונים ובאמצעות רשת האינטרנט. 20. מתווכי נתונים (Data brokers): שירותים דיגיטליים מסחריים העוסקים באיסוף, צבירה, העשרה, ניתוח ומכירה או שיתוף של מידע מזוהה על אנשים, ארגונים וישויות דיגיטליות.
10. חקלאות		משק חקלאי, ארגון חקלאי, או תאגיד פרטי סטטוטורי, או יצרן חקלאי העוסק בעבור השוק בישראל בגידול, עיבוד, ייבוא, אחסון גרעינים או חיטה, או שיווק ביצים, והמחזיק בנתח שוק של 20% או יותר מהתוצרת בענף החקלאות הפרטני. בפרט זה "יצרן חקלאי" - כהגדרתו בחוק לעידוד השקעות הון בחקלאות, התשמ"א-1980[22].

[22] ס"ח תשמ"א 996, עמ' 56.

תוספת רביעית

(סעיף 10(ב))

חלק א' – דרישות רמת הגנה

א. מדיניות לניתוח סיכונים והגנה על נכסי סייבר

1. זיהוי ומיפוי מתמשכים, ולכל הפחות אחת לשנה, של נכסי הסייבר (לרבות מערכות מידע, מערכות תפעוליות ומוצרים דיגיטליים), נתונים, מושאי אבטחת המידע והגנת הסייבר והתהליכים המרכזיים התלויים בהם;
2. ביצוע הערכות יזומות ובדיקות אבטחה, ותיעודן, לצורך הערכה וזיהוי של סיכוני סייבר ולקביעת רמת הגנת הסייבר של הארגון, וכן לאיתור תצורות טכנולוגיות המסכנות את הארגון נכסיו או ארגונים המקושרים אליו, אשר עלולות לשבש תהליכים חיוניים;
3. ניהול והערכה מתמשכים של סיכוני הסייבר, הקשורים לנכסי הסייבר, לנתונים ולתהליכים של הארגון, אחת לשנה לפחות ובכל פרויקט טכנולוגי חדש.
4. הכנת, יישום ועדכון תכנית עבודה מאושרת על ידי דרג ניהולי ובקרה על יישומה על ידו, לטיפול בתחום הגנת הסייבר ותיעוד יישומה;
5. קיומו של צוות ליישום הגנת סייבר לצורך ביצוע תוכנית העבודה השוטפת לטיפול בתחום הגנת הסייבר;
6. יישום נהלים ואמצעים, ופריסת מערכות הגנה, לאבטחת תשתית תקשורת הנתונים הפנימית והחיצונית של הארגון – לרבות הקישורים והממשקים הנכנסים והיוצאים מהארגון – וכן החיבורים בין יחידותיו השונות.
7. הטמעת נהלים, אמצעים ומערכות הגנה לאיתור או מניעת שימוש בתוכנות זדוניות או בלתי מורשות, בהתאמה לסיכונים שמופו של הנכסים, הנתונים והתהליכים הארגוניים.
8. הפרדת ופילוח רשתות הארגון, השירותים והמתחמים השונים ברשת בהתאם לתוצאות הערכת הסיכונים ותוכנית מענה, ובדומה הפרדת ופילוח מערכות ורשתות של צדדים שלישיים;
9. אימוץ אמצעים מתאימים לקביעה, תיעוד, יישום וניטור של תצורות מאובטחות של חומרה, תוכנה, שירותים ורשתות.
10. קביעה, ויישום של מדיניות ונהלים לניהול ושימוש באמצעים ניידים, לרבות הגדרת תצורות מאובטחות והגנה על נכסי הארגון ונתוניו.
11. כתיבה, יישום ואכיפה של מדיניות ונהלים לניהול אמצעי אחסון נשלפים ומדיה נתיקה במתקני הארגון ובמיקומים אחרים.

ב. היערכות והתמודדות עם אירועי סייבר

12. כתיבה, יישום ועדכון עיתי של תוכנית ארגונית מאושרת ומנוטרת לטיפול באירועי סייבר, המפרטת תפקידים, תחומי אחריות ונהלים לאיתור, מניעה, בלימה, התאוששות,התמודדות, תיעוד ודיווח על תקיפות סייבר.
13. מינוי והכשרה מראש של צוות ניהול משברים ארגוני, שיפעל במהלך תקיפת סייבר;
14. קיומה של היערכות מקדימה של הארגון להתרחשות אירוע סייבר באמצעות צוותי תגובה מוגדרים, נהלי תגובה, סדרי פעולות ומענים טכנולוגים;
15. ביצוע ותיעוד של תרגילים בדרג הניהולי המשלבים תגובה לאירועי סייבר והמשכיות עסקית, אחת לשנה;
16. ביצוע הכשרות ואימונים מעשיים, להתמודדות עם אירועי סייבר, עבור צוות ניהול המשברים ארגוני, צוות התגובה לאירועים, צוות יישום אבטחת המידע ואנשי מערכות המידע והטכנולוגיות, אחת לשנה;
17. פיתוח ויישום תוכנית ארגונית לניטור טכנולוגי, הקובעת נהלים ושימוש בכלים לניטור ורישום פעילויות (רישום יומנים **logs**), הקשורות לנכסי סייבר, לתקשורת ולנתונים, במטרה לאתר חריגות ואירועים חשודים.
18. קביעת נהלים ויישום אמצעים לסקירת יומנים **(logs)** באופן קבוע ומתמשך, הכוללים קביעת ספים להתרעה והפצת התרעות במקרים המתאימים.
19. תחזוקה וגיבוי של יומנים (**logs**), לתקופת שמירה מוגדרת מראש ומאושרת, והגנה עליהם מפני גישה או שינוי בלתי מורשים.
20. קיומו של מנגנון ארגוני המאפשר למנהלים, עובדים, ספקים ולקוחות לדווח על אירועים חשודים;
21. קיומם של קריטריונים על בסיסם תיעשה הערכה וסיווג לחריגות שמתגלות מדיווח או באמצעות ניטור ומעבר לפעולת תגובה מהירה;
22. קיומו של תהליך ארגוני לבחינת דיווחים או תוצאות ניטור והכרזה על אירוע סייבר;
23. הימצאותם של תכניות ונהלי תקשורת עם צוותי התערבות, רשויות וגורמים פנימיים וחיצוניים רלוונטיים;
24. קיומו ותיעודו של תהליך הפקת לקחים ולמידה ושיפור מאירועי סייבר;

ג. רציפות תפקודית והמשכיות השירות

25. ביצוע ניתוח השפעה עסקית (**BIA**) להערכת ההשפעה הפוטנציאלית של תקיפת סייבר, אחת לשנתיים לפחות, לרבות תקיפה חמורה, ובהתאם לכך מיפוי של יעדי הרציפות התפקודית לנכסי הסייבר, הנתונים והשירותים החיוניים התלויים בהם.
26. כתיבת, יישום ועדכון תוכנית ארגונית סדורה ומאושרת להמשכיות עסקית (**BCP**) המבוססת על הערכות סיכונים וניתוח ההשפעות העסקיות, לרבות יעדים, תפקידים, אנשי קשר, ערוצי תקשורת ותנאים להפעלה וביטול;
27. קיומה של תכנית מאושרת להתאוששות מאסון (**DRP**) בהיבטי הגנת סייבר ואבטחת מידע, בהתחשב ברשימת סיכונים פוטנציאליים ויכולות התאוששות, שתכלול יעדי התאוששות (**RTO/RPO**), רצף התאוששות, תוכניות שחזור ושיקום ספציפיות ומשאבים נדרשים, ותכלול התייחסות לכוח אדם, משאבי מחשוב, תקשורת ותשתיות פיזיות.
28. כתיבת, יישום, עדכון ותרגול של תוכניות גיבוי המבוססות על הערכת הסיכונים ותוכנית ההמשכיות העסקית, לרבות זמני התאוששות מוגדרים (**RTO/RPO**), הבטחת שלמות עותקי הגיבוי, אחסון מאובטח, בקרות גישה הולמות לגיבויים, נהלי שחזור, גרסאות גיבוי ותקופות שמירת נתונים.
29. היערכות משאבית אשר תספק את הצורך לרציפות התהליכים העסקיים, ומערכות ונכסי המידע - הנדרשים בשגרה ובחירום לרבות יתירות של ציוד, מערכות רשת ונתונים, תכנון רכש ומעורבות ספקים;
30. ביצוע תדריכים, הכשרות ותרגול לתכנית ההמשכיות העסקי, המשכיות השירות וההתאוששות מאסון עבור הנהלת הארגון, צוותי יישום אבטחת המידע ואנשי מערכות המידע והטכנולוגיות;

ד. הגנת סייבר בשרשרת האספקה

31. כתיבת, יישום ועדכון מדיניות ארגונית ונוהלי עבודה להגנה בסייבר מפני איומים בשרשרת האספקה ועבודה מול ארגונים מול ספקים ונותני שירותים;
32. מיפוי מתמשך של שרשרת האספקה של הארגון, לרבות זיהוי השירותים והמוצרים המתקבלים מספקים והשפעתם על רמת הגנת הסייבר ואבטחת המידע הארגוני בנכסי הסייבר, התקשורת, הנתונים

והתהליכים;

33. הערכת הסיכון וחישוב רמת הסיכון הנובע משרשרת האספקה על נכסי הסייבר, הנתונים, התהליכים או השירותים של הארגון;

34. מתן שאלון הגנת סייבר לספקים, בכל התקשרות וכל שמונה עשר חודשים מתחילתה, לטובת הערכה עצמית והצהרה על רמת הסיכון בסייבר שלהם, במטרה לאמוד את רמת הסיכון אלין חשוף הארגון מצד הספק;

35. ביצוע בדיקות עיתיות וסקרי חוסן מטעם הארגון על אופן הגנת נכסי הסייבר והנתונים הארגוניים, המצויים בחצרות הספק;

36. קביעת, יישום, בקרה ועדכון תכנית הגנה ארגונית, לצמצום רמת הסיכון אל מול הספקים בהתאם לרמת ההגנה הקיימת בנכסים;

37. הכללת סעיפי הגנת סייבר בחוזים עם ספקים ונותני שירותים, המפרטים דרישות הגנת סייבר ואבטחת מידע, חובות דיווח על אירועים, זכויות ביקורת, טיפול בפרצות, חולשות וחשיפות, דרישות לקבלני משנה והתחייבויות עם סיום החוזה.

ה. פיתוח ותחזוקה של מערכות, חשיפה וטיפול בפגיעויות ותהליכי רכש

38. כתיבת, יישום ועדכון של נוהל פיתוח מאובטח מאושר, הן לפיתוח פנימי והן לפיתוח במיקור חוץ. הנוהל יכלול ניתוח דרישות אבטחה, יישום עקרונות תכנון וקידוד מאובטחים, הגדרת דרישות אבטחה לסביבות פיתוח, יישום תהליכי בדיקות אבטחה, והגנה וניהול של נתוני בדיקה.

39. כתיבת, יישום ועדכון הנחיות ונהלים מקצועיים לתהליכים וכלים לאכיפת תצורות מאובטחות, ניהול שינויים, וביצוע תיקונים ותחזוקה בנכסי סייבר, לרבות עדכוני מערכת בנכסי הסייבר בארגון (**Updates**)– הן עבור מערכות חדשות והן עבור מערכות קיימות.

40. כתיבת, יישום ועדכון של הנחיות ונהלים מקצועיים לניהול מחזורי של טלאי אבטחה (**Security Patch Management**) בנכסי הסייבר והנתונים של הארגון, – הן עבור מערכות חדשות והן עבור מערכות קיימות.

41. כתיבת, יישום ועדכון עתי של הנחיות ונהלים מקצועיים לניהול פגיעויות טכניות בנכסי הסייבר והנתונים של הארגון, הערכת החשיפה לפגיעויות, ונקיטת אמצעים מתאימים לטיפול בהן בזמן סביר;

42. גיבוש ויישום מדיניות "גילוי פגיעויות מתואם" (**Coordinated Vulnerability Disclosure - CVD**), הכוללת ערוץ מאובטח לקבלת

דיווחים מחוקרים חיצוניים על פרצות אבטחה בנכסי הארגון;

ו. מדיניות ונהלים להערכת האפקטיביות של מאמץ ההגנה

43. כתיבה, אישור, יישום, בקרה ועדכון של מדיניות ארגונית לאבטחת מידע והגנת סייבר;
44. מינוי ממונה הגנת סייבר הכפוף למנהל הארגון, והגדרת אחריות ישירה של ההנהלה הבכירה לאישור ופיקוח על אמצעי ניהול סיכוני הסייבר;
45. הגדרת תפקידים לעניין הגנת הסייבר, מינוי בעלי התפקידים, וקביעת תחומי אחריות וסמכויות;
46. מינוי משתתפים, קיומה ופעילות שוטפת של וועדת היגוי לאבטחת מידע והגנת סייבר בראשות מנהל הארגון – לפחות פעמיים בשנה;
47. כתיבת, יישום ועדכון עתי של נהלים ארגוניים בתחום הגנת הסייבר ואבטחת מידע, והתאמת נהלים ארגוניים קיימים לאיומי הסייבר;
48. מעקב תקופתי אחר יישום תכנית העבודה להגנת סייבר ויעילות האמצעים שננקטו להפחתת סיכונים על ידי מנהל הארגון או וועדת ההיגוי;
49. הכנת דו"ח כל שישה חודשים על פעילות הגנת הסייבר ואבטחת המידע בארגון, מידת הציות לחובות שבדין ומידת הציות לתכנית ניהול הסיכונים הארגונית בהתאמה לתקינה שאומצה מחלק ב' לתוספת;

ז. היגיינת מחשב בסיסית והדרכות

50. כתיבה, יישום אחת לרבעון ועדכון תכנית מודעות עובדים בתחום אבטחת הסייבר להנהלה, עובדים וספקים שתכליתה עידוד התנהגות סייבר אחראית, לרבות זיהוי וטיפול באירועי סייבר;
51. כתיבת, יישום ועדכון תוכנית הכשרה ותרגול מעשית לעובדים שתפקידם דורש מיומנויות ומומחיות באבטחת סייבר;

ח. הצפנה והסתרת נכסי סייבר

52. כתיבת נוהל ויישום תהליך עיתי, ולכל הפחות אחת לשנה, לסיווג נכסי הסייבר, הרשתות והנתונים של הארגון לרבות לפי רמת אבטחה נדרשת, רגישות וסוג;
53. הגדרה, יישום, אכיפה ועדכון של מדיניות ונהלי הצפנת הנתונים בארגון, והשימוש באמצעים קריפטוגרפים, לרבות מפתחות הצפנה,

תעודות אבטחה וחתימות דיגיטליות, כדי להבטיח הגנה על סודיות, אותנטיות ושלמות הנתונים ואימות ברמה גבוהה, בהתאם לסיווג נכסי הארגון ותוצאות הערכת הסיכונים;

54. הצפנת נתוני הארגון במעבר ובמנוחה, תוך מתן עדיפות להצפנה מקצה לקצה, – בהתאם למיפוי נכסי המידע וניהול הסיכונים – תוך שימוש באמצעים, פרוטוקולים, אלגוריתמים ופתרונות הצפנה מקובלים מאושרים;

55. כתיבת נהלים והקמה וניהול של תשתית לניהול מפתחות הצפנה ותעודות אבטחה, הכוללים בין היתר, הפקה, אחסון, החלפה, אחזור והשמדה של חומר קריפטוגרפי, תוך הפרדה לוגית בין הנתונים המוצפנים לבין אמצעי ניהול התשתית;

ט. בקרת גישה, ניהול נכסים, וטיפול בגורם האנושי

56. כתיבה, יישום ואכיפה טכנולוגית של מדיניות בקרת גישה מבוססת סיכון, המגדירה את רמות ההרשאה לכלל נכסי הסייבר, הרשתות והנתונים. המדיניות תבטיח יישום בפועל של עקרונות "הצורך לדעת", "הרשאה מינימלית" והפרדת תפקידים (**SoD**);

57. הטמעה ויישום טכנולוגי של אמצעי אימות מתקדמים, לרבות אימות רב-שלבי (**MFA**) חזק ומתמשך. היישום יהיה בהתאם לסיווג הנתונים ורמת הסיכון, ובתוך כך חובה עבור כל גישה מרחוק, גישה לנכסים קריטיים וגישה של חשבונות בעלי הרשאות מועדפות וגבוהות;

58. כתיבה ויישום תהליכי ניהול מחזור חיי זהות דיגיטלית, המבטיחים הצמדת זהות ייחודית וחד-ערכית לכל משתמש או רכיב טכנולוגי, תוך קיום רישום ובקרה (**Audit Trail**) על כלל הפעולות המבוצעות בזהויות אלו.

59. כתיבה, יישום שבועי ועדכון של מדיניות ונהלי בקרת גישה ואימות מתקדמים ומאושרים לחשבונות "פריבילגיים" (בעלי הרשאות מועדפות וגבוהות). הנהלים יחולו על בעלי תפקידים רגישים ומנהלי מערכת (**Administrators**) האמונים והמנהלים מערכות מידע קריטיות, נכסי סייבר ליבתיים, תשתיות תקשורת, מערכות ניהול מרכזיות ומערכות להגנת סייבר;

60. הגדרה ויישום טכנולוגי של הפרדה לוגית או פיזית בין מערכות הנכללות בפרט 59, לבין יישומים עסקיים אחרים;

61. כתיבה ויישום של מדיניות ונהלים להגנה פיזית על אתרי הארגון, מתקני המחשוב (**Data Centers**) ותשתיות התקשורת, למניעת גישה לא מורשית, נזק או הפרעה לנכסי הסייבר ורשתות התקשורת;

62. כתיבה, יישום ועדכון של נהלים לביצוע בדיקות רקע ומהימנות אבטחתית לעובדים, מנהלים וספקים הבאים במגע עם נכסי סייבר ותהליכים קריטיים, טרם קבלתם ועל בסיס עיתי.
63. כתיבה, יישום ועדכון של נהלים להסדרת פעולות הגנת סייבר הנדרשות בעת קליטת עובדים, שינויי תפקידים בתוך הארגון, וסיום העסקה – לרבות ביטול מיידי של הרשאות גישה והחזרת נכסים פיזיים.

חלק ב'- תקינה

1. ISO/IEC 27002 יחד עם ISO/IEC 27001
2. ת"י 27002 יחד עם ת"י 27001
3. NIST Cybersecurity Framework(CSF)
4. NIST SP 800-53 (control baselines for Moderate or High impact)

תוספת חמישית

(סעיפים 41,23)

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
1. ארגון שלא זיהה וביצע מיפוי מתמשך, ולכל הפחות אחת לשנה, של נכסי הסייבר (לרבות מערכות מידע, מערכות תפעוליות ומוצרים דיגיטליים), נתונים, מושאי אבטחת המידע והגנת הסייבר והתהליכים המרכזיים התלויים בהם בניגוד להוראות פרט (1) בתוספת הרביעית;	640,000
2. ארגון שלא ביצע הערכות יזומות ובדיקות אבטחה, ותיעוד אותן, לצורך הערכה וזיהוי של סיכוני סייבר ולקביעת רמת הגנת הסייבר של הארגון, וכן לאיתור תצורות טכנולוגיות המסכנות את הארגון נכסיו או ארגונים המקושרים אליו, אשר עלולות לשבש תהליכים חיוניים בניגוד להוראות פרט (2) בתוספת הרביעית;	640,000
3. ארגון שלא ניהל וביצע הערכה מתמשכת של סיכוני הסייבר, הקשורים לנכסי הסייבר, לנתונים ולתהליכים של הארגון, אחת לשנה לפחות ובכל פרויקט טכנולוגי חדש בניגוד להוראות פרט (3) בתוספת הרביעית;	640,000

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	4. ארגון שלא הכין, יישם ועידכן תכנית עבודה מאושרת על ידי דרג ניהולי וביצע בקרהעל יישומה על ידו, לטיפול בתחום הגנת הסייבר ותיעוד יישומה בניגוד להוראות פרט (4) בתוספת הרביעית;
640,000	5. ארגון שלא מינה צוות ליישום הגנת סייבר לצורך ביצוע תוכנית העבודה השוטפת לטיפול בתחום הגנת הסייבר בניגוד להוראות פרט (5) בתוספת הרביעית;
640,000	6. ארגון שלא יישם נהלים ואמצעים, ופרס מערכות הגנה, לאבטחת תשתית תקשורת הנתונים הפנימית והחיצונית של הארגון – לרבות הקישורים והממשקים הנכנסים והיוצאים מהארגון – וכן החיבורים בין יחידותיו השונות בניגוד להוראות פרט (6) בתוספת הרביעית;
640,000	7. ארגון שלא הטמיע נהלים, אמצעים ומערכות הגנה לאיתור או מניעת שימוש בתוכנות זדוניות או בלתי מורשות, בהתאמה לסיכונים שמופו של הנכסים, הנתונים והתהליכים הארגוניים בניגוד להוראות פרט (7) בתוספת הרביעית;

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	8. ארגון שלא ביצע הפרדה ופילוח של רשתות הארגון, השירותים והמתחמים השונים ברשת בהתאם לתוצאות הערכת הסיכונים ותוכנית מענה, ובדומה הפרדת ופילוח מערכות ורשתות של צדדים שלישיים בניגוד להוראות פרט (8) בתוספת הרביעית;
640,000	9. ארגון שלא אימץ אמצעים מתאימים לקביעה, תיעוד, יישום וניטור של תצורות מאובטחות של חומרה, תוכנה, שירותים ורשתות בניגוד להוראות פרט (9) בתוספת הרביעית;
640,000	10. ארגון שלא קבע ויישם מדיניות ונהלים לניהול ושימוש באמצעים ניידים, לרבות הגדרת תצורות מאובטחות והגנה על נכסי הארגון ונתוניו בניגוד להוראות פרט (10) בתוספת הרביעית;
640,000	11. ארגון שלא כתב, יישם ואכף מדיניות ונהלים לניהול אמצעי אחסון נשלפים ומדיה נתיקה במתקני הארגון ובמיקומים אחרים בניגוד להוראות פרט (11) בתוספת הרביעית;

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
12. ארגון שלא כתב, יישם ועדכן באופן עיתי של תוכנית ארגונית מאושרת ומנוטרת לטיפול באירועי סייבר, המפרטת תפקידים, תחומי אחריות ונהלים לאיתור, מניעה, בלימה, התאוששות,התמודדות, תיעוד ודיווח על תקיפות סייבר בניגוד להוראות פרט (12) בתוספת הרביעית;	640,000
13. ארגון שלא מינה והכשירמראשצוות ניהול משברים ארגוני, שיפעל במהלך תקיפת סייבר בניגוד להוראות פרט (13) בתוספת הרביעית;	640,000
14. ארגון שלא נערך היערכות מקדימה להתרחשות אירוע סייבר באמצעות צוותי תגובה מוגדרים, נהלי תגובה, סדרי פעולות ומענים טכנולוגים בניגוד להוראות פרט (14) בתוספת הרביעית;	640,000
15. ארגון שלא ביצע ותיעד תרגילים בדרג הניהולי המשלבים תגובה לאירועי סייבר והמשכיות עסקית, אחת לשנה בניגוד להוראות פרט (15) בתוספת הרביעית;	640,000

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
16. ארגון שלא ביצע הכשרות ואימונים מעשיים, להתמודדות עם אירועי סייבר, עבור צוות ניהול המשברים ארגוני, צוות התגובה לאירועים, צוות יישום אבטחת המידע ואנשי מערכות המידע והטכנולוגיות, אחת לשנה בניגוד להוראות פרט (16) בתוספת הרביעית;	640,000
17. ארגון שלא פיתח ויישם תוכנית ארגונית לניטור טכנולוגי, הקובעת נהלים ושימוש בכלים לניטור ורישום פעילויות (רישום יומנים- **logs**), הקשורות לנכסי סייבר, לתקשורת ולנתונים, במטרה לאתר חריגות ואירועים חשודים בניגוד להוראות פרט (17) בתוספת הרביעית;	640,000
18. ארגון שלא קבע נהלים ויישם אמצעים לסקירת יומנים **(logs)** באופן קבוע ומתמשך, הכוללים קביעת ספים להתרעה והפצת התרעות במקרים המתאימים בניגוד להוראות פרט (18) בתוספת הרביעית;	640,000

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
320,000	19. ארגון שלא ביצע תחזוקה וגיבוי של יומנים (**logs**), לתקופת שמירה מוגדרת מראש ומאושרת, או לא הגן עליהם מפני גישה או שינוי בלתי מורשים בניגוד להוראות פרט (19) בתוספת הרביעית.
640,000	20. ארגון שאין בו מנגנון ארגוני המאפשר למנהלים, עובדים, ספקים ולקוחות לדווח על אירועים חשודים בניגוד להוראות פרט (20) בתוספת הרביעית;
320,000	21. ארגון שלא נקבעו בו קריטריונים על בסיסם תיעשה הערכה וסיווג לחריגות שמתגלות מדיווח או באמצעות ניטור ומעבר לפעולת תגובה מהירה בניגוד להוראות פרט (21) בתוספת הרביעית;
640,000	22. ארגון שאין בו תהליך ארגוני לבחינת דיווחים או תוצאות ניטור והכרזה על אירוע סייבר בניגוד להוראות פרט (22) בתוספת הרביעית;

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
23. ארגון שאין בו תכניות ונהלי תקשורת עם צוותי התערבות, רשויות וגורמים פנימיים וחיצוניים רלוונטיים בניגוד להוראות פרט (23) בתוספת הרביעית;	320,000
24. ארגון שלא מתקיים ומתועדבו תהליך הפקת לקחים ולמידה ושיפור מאירועי סייבר בניגוד להוראות פרט (24) בתוספת הרביעית;	320,000
25. ארגון שלא ביצע ניתוח השפעה עסקית **(BIA)** להערכת ההשפעה הפוטנציאלית של תקיפת סייבר, אחת לשנתיים לפחות, לרבות תקיפה חמורה, ובהתאם לכך מיפוי של יעדי הרציפות התפקודית לנכסי הסייבר, הנתונים והשירותים החיוניים התלויים בהם בניגוד להוראות פרט (25) בתוספת הרביעית;	640,000

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
26. ארגון שלא כתב, יישם ועדכן תוכנית ארגונית סדורה ומאושרת להמשכיות עסקית (**BCP**) המבוססת על הערכות סיכונים וניתוח ההשפעות העסקיות, לרבות יעדים, תפקידים, אנשי קשר, ערוצי תקשורת ותנאים להפעלה וביטול בניגוד להוראות פרט (26) בתוספת הרביעית;	640,000
27. ארגון שאין בו תכנית מאושרת להתאוששות מאסון (**DRP**) בהיבטי הגנת סייבר ואבטחת מידע, בהתחשב ברשימת סיכונים פוטנציאליים ויכולות התאוששות, שתכלול יעדי התאוששות (**RTO/RPO**), רצף התאוששות, תוכניות שחזור ושיקום ספציפיות ומשאבים נדרשים, ותכלול התייחסות לכוח אדם, משאבי מחשוב, תקשורת ותשתיות פיזיות בניגוד להוראות פרט (27) בתוספת הרביעית;	640,000

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
28. ארגון שלא כתב, יישם, עדכן ותרגל תוכניות גיבוי המבוססות על הערכת הסיכונים ותוכנית ההמשכיות העסקית, לרבות זמני התאוששות מוגדרים (**RTO/RPO**), הבטחת שלמות עותקי הגיבוי, אחסון מאובטח, בקרות גישה הולמות לגיבויים, נהלי שחזור, גרסאות גיבוי ותקופות שמירת נתונים בניגוד להוראות פרט (28) בתוספת הרביעית;	640,000
29. ארגון שלא נערך משאבית באופן שיספק את הצורך לרציפות התהליכים העסקיים, ומערכות ונכסי המידע - הנדרשים בשגרה ובחירום לרבות יתירות של ציוד, מערכות רשת ונתונים, תכנון רכש ומעורבות ספקים בניגוד להוראות פרט (29) בתוספת הרביעית;	320,000
30. ארגון שלא ביצע תדריכים, הכשרות ותרגול לתכנית ההמשכיות העסקי, המשכיות השירות וההתאוששות מאסון עבור הנהלת הארגון, צוותי יישום אבטחת המידע ואנשי מערכות המידע והטכנולוגיות בניגוד להוראות פרט (30) בתוספת הרביעית;	320,000

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
31. ארגון שלא כתב, יישם ועדכן מדיניות ארגונית ונהלי עבודה להגנה בסייבר מפני איומים בשרשרת האספקה ועבודה מול ארגונים, מול ספקים ומול נותני שירותים בניגוד להוראות פרט (31) בתוספת הרביעית;	640,000
32. ארגון שלא ביצע מיפוי מתמשך של שרשרת האספקה של הארגון, לרבות זיהוי השירותים והמוצרים המתקבלים מספקים והשפעתם על רמת הגנת הסייבר ואבטחת המידע הארגוני בנכסי הסייבר, התקשורת, הנתונים והתהליכים בניגוד להוראות פרט (32) בתוספת הרביעית;	640,000
33. ארגון שלא ביצע הערכת סיכון וחישוב רמת הסיכון הנובע משרשרת האספקה על נכסי הסייבר, הנתונים, התהליכים או השירותים של הארגון בניגוד להוראות פרט (33) בתוספת הרביעית;	640,000

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
34. ארגון שלא נתן שאלון הגנת סייבר לספקים, בכל התקשרות וכל שמונה עשר חודשים מתחילתה, לטובת הערכה עצמית והצהרה על רמת הסיכון בסייבר שלהם, במטרה לאמוד את רמת הסיכון אלין חשוף הארגון מצד הספק בניגוד להוראות פרט (34) בתוספת הרביעית;	320,000
35. ארגון שלא ביצע בדיקות עיתיות וסקרי חוסן מטעם הארגון על אופן הגנת נכסי הסייבר והנתונים הארגוניים, המצויים בחצרות הספק בניגוד להוראות פרט (35) בתוספת הרביעית;	320,000
36. ארגון שלא קבע, יישם, ביצע בקרה ועדכן את תכנית ההגנה הארגונית, לצמצום רמת הסיכון אל מול הספקים בהתאם לרמת ההגנה הקיימת בנכסים בניגוד להוראות פרט (36) בתוספת הרביעית;	640,000

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
37. ארגון שלא כלל סעיפי הגנת סייבר בחוזים עם ספקים ונותני שירותים, המפרטים דרישות הגנת סייבר ואבטחת מידע, חובות דיווח על אירועים, זכויות ביקורת, טיפול בפרצות, חולשות וחשיפות, דרישות לקבלני משנה והתחייבויות עם סיום החוזה בניגוד להוראות פרט (37) בתוספת הרביעית.	320,000
38. ארגון שלא כתב, יישם ועדכן נוהל פיתוח מאובטח מאושר, הן לפיתוח פנימי והן לפיתוח במיקור חוץ שכולל ניתוח דרישות אבטחה, יישום עקרונות תכנון וקידוד מאובטחים, הגדרת דרישות אבטחה לסביבות פיתוח, יישום תהליכי בדיקות אבטחה, והגנה וניהול של נתוני בדיק בניגוד להוראות פרט (38) בתוספת הרביעית	320,000

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	39. ארגון שלא כתב, יישם ועדכן הנחיות ונהלים מקצועיים לתהליכים וכלים לאכיפת תצורות מאובטחות, ניהול שינויים, וביצוע תיקונים ותחזוקה בנכסי סייבר, לרבות עדכוני מערכת בנכסי הסייבר בארגון (**Updates**)– הן עבור מערכות חדשות והן עבור מערכות קיימות בניגוד להוראות פרט (39) בתוספת הרביעית;
640,000	40. ארגון שלא כתב, יישם ועדכן הנחיות ונהלים מקצועיים לניהול מחזורי של טלאי אבטחה (**Security Patch Management**) בנכסי הסייבר והנתונים של הארגון, – הן עבור מערכות חדשות והן עבור מערכות קיימות בניגוד להוראות פרט (40) בתוספת הרביעית;
640,000	41. ארגון שלא כתב, יישום ועדכן באופן עתי הנחיות ונהלים מקצועיים לניהול פגיעויות טכניות בנכסי הסייבר והנתונים של הארגון, הערכת החשיפה לפגיעויות, ונקיטת אמצעים מתאימים לטיפול בהן בזמן סביר בניגוד להוראות פרט (41) בתוספת הרביעית;

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
320,000	42. ארגון שלא גיבש ויישם מדיניות "גילוי פגיעויות מתואם" (**Coordinated Vulnerability Disclosure - CVD**), הכוללת ערוץ מאובטח לקבלת דיווחים מחוקרים חיצוניים על פרצות אבטחה בנכסי הארגון בניגוד להוראות פרט (42) בתוספת הרביעית;
640,000	43. ארגון שלא כתב, אישר, יישם, ביצע בקרה ועדכן את המדיניות הארגונית לאבטחת מידע והגנת סייבר בניגוד להוראות פרט (43) בתוספת הרביעית;
640,000	44. ארגון שלא מינה ממונה הגנת סייבר הכפוף למנהל הארגון, והגדרת אחריות ישירה של ההנהלה הבכירה לאישור ופיקוח על אמצעי ניהול סיכוני הסייבר בניגוד להוראות פרט (44) בתוספת הרביעית;
320,000	45. ארגון שלא הגדיר תפקידים לעניין הגנת הסייבר, לא מינה את בעלי התפקידים, או לא קבע תחומי אחריות וסמכויות בניגוד להוראות פרט (45) בתוספת הרביעית;

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
320,000	46. ארגון שלא מינה משתתפים, לא התקיימה בו ולא ביצע פעילות שוטפת של וועדת היגוי לאבטחת מידע והגנת סייבר בראשות מנהל הארגון – לפחות פעמיים בשנה בניגוד להוראות פרט (46) בתוספת הרביעית;
320,000	47. ארגון שלא כתב, יישם ועדכן באופן עתי נהלים ארגוניים בתחום הגנת הסייבר ואבטחת מידע, או לא ביצע התאמה של נהלים ארגוניים קיימים לאיומי הסייבר בניגוד להוראות פרט (47) בתוספת הרביעית;
640,000	48. ארגון שלא ביצע מעקב תקופתי אחר יישום תכנית העבודה להגנת סייבר ויעילות האמצעים שננקטו להפחתת סיכונים על ידי מנהל הארגון או וועדת ההיגוי בניגוד להוראות פרט (48) בתוספת הרביעית;

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	49. ארגון שלא הכין דו״ח כל שישה חודשים על פעילות הגנת הסייבר ואבטחת המידע בארגון, מידת הציות לחובות שבדין ומידת הציות לתכנית ניהול הסיכונים הארגונית בהתאמה לתקינה שאומצה מחלק ב׳ לתוספת בניגוד להוראות פרט (49) בתוספת הרביעית;
320,000	50. ארגון שלא כתב או יישם אחת לרבעון ועדכן תכנית מודעות עובדים בתחום אבטחת הסייבר להנהלה, עובדים וספקים שתכליתה עידוד התנהגות סייבר אחראית, לרבות זיהוי וטיפול באירועי סייבר, בניגוד להוראות פרט (50) בתוספת הרביעית;
320,000	51. ארגון שלא כתב, יישם ועדכן תוכנית הכשרה ותרגול מעשית לעובדים שתפקידם דורש מיומנויות ומומחיות באבטחת סייבר בניגוד להוראות פרט (51) בתוספת הרביעית;

טור א' ההפרה	טור ב' סכום העיצום הכספי (בשקלים חדשים)
52. ארגון שלא כתב נוהל או לא יישם תהליך עיתי, ולכל הפחות אחת לשנה, לסיווג נכסי הסייבר, הרשתות והנתונים של הארגון לרבות לפי רמת אבטחה נדרשת, רגישות וסוג בניגוד להוראות פרט (52) בתוספת הרביעית;	640,000
53. ארגון שלא הגדיר, יישם אכף ועדכן מדיניות ונהלי הצפנת הנתונים בארגון, והשימוש באמצעים קריפטוגרפים, לרבות מפתחות הצפנה, תעודות אבטחה וחתימות דיגיטליות, כדי להבטיח הגנה על סודיות, אותנטיות ושלמות הנתונים ואימות ברמה גבוהה, בהתאם לסיווג נכסי הארגון ותוצאות הערכת הסיכונים בניגוד להוראות פרט (53) בתוספת הרביעית;	640,000
54. ארגון שלא הצפין את נתוני הארגון במעבר ובמנוחה, תוך מתן עדיפות להצפנה מקצה לקצה, – בהתאם למיפוי נכסי המידע וניהול הסיכונים – תוך שימוש באמצעים, פרוטוקולים, אלגוריתמים ופתרונות הצפנה מקובלים מאושרים בניגוד להוראות פרט (54) בתוספת הרביעית;	640,000

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	55. ארגון שלא כתב נהלים, לא הקים או לא ניהל תשתית לניהול מפתחות הצפנה ותעודות אבטחה, הכוללים בין היתר, הפקה, אחסון, החלפה, אחזור והשמדה של חומר קריפטוגרפי, תוך הפרדה לוגית בין הנתונים המוצפנים לבין אמצעי ניהול התשתית בניגוד להוראות פרט (55) בתוספת הרביעית;
640,000	56. ארגון שלא כתב, יישם ואכף טכנולוגית מדיניות בקרת גישה מבוססת סיכון, המגדירה את רמות ההרשאה לכלל נכסי הסייבר, הרשתות והנתונים. המדיניות תבטיח יישום בפועל של עקרונות "הצורך לדעת", "הרשאה מינימלית" והפרדת תפקידים (**SoD**) בניגוד להוראות פרט (56) בתוספת הרביעית;

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	57. ארגון שלא הטמיע ויישם טכנולוגית אמצעי אימות מתקדמים, לרבות אימות רב-שלבי (**MFA**) חזק ומתמשך, בהתאם לסיווג הנתונים ורמת הסיכון, ובתוך כך חובה עבור כל גישה מרחוק, גישה לנכסים קריטיים וגישה של חשבונות בעלי הרשאות מועדפות וגבוהות בניגוד להוראות פרט (57) בתוספת הרביעית;
320,000	58. ארגון שלא כתב, או יישם תהליכי ניהול מחזור חיי זהות דיגיטלית, המבטיחים הצמדת זהות ייחודית וחד-ערכית לכל משתמש או רכיב טכנולוגי, תוך קיום רישום ובקרה (**Audit Trail**) על כלל הפעולות המבוצעות בזהויות אלו בניגוד להוראות פרט (58) בתוספת הרביעית;

טור ב׳ סכום העיצום הכספי (בשקלים חדשים)	טור א׳ ההפרה
640,000	59. ארגון שלא כתב, יישם באופן שבועי או עדכן מדיניות ונהלי בקרת גישה ואימות מתקדמים ומאושרים לחשבונות "פריבילגיים" (בעלי הרשאות מועדפות וגבוהות), שיחולו על בעלי תפקידים רגישים ומנהלי מערכת (**Administrators**) האמונים והמנהלים מערכות מידע קריטיות, נכסי סייבר ליבתיים, תשתיות תקשורת, מערכות ניהול מרכזיות ומערכות להגנת סייבר בניגוד להוראות פרט (59) בתוספת הרביעית;
640,000	60. ארגון שלא הגדיר או יישם טכנולוגית הפרדה לוגית או פיזית בין מערכות הנכללות בפרט 59, לבין יישומים עסקיים אחרים, בניגוד להוראות פרט (60) בתוספת הרביעית;
320,000	61. ארגון שלא כתב ויישם מדיניות ונהלים להגנה פיזית על אתרי הארגון, מתקני המחשוב (**Data Centers**) ותשתיות התקשורת, למניעת גישה לא מורשית, נזק או הפרעה לנכסי הסייבר ורשתות התקשורת בניגוד להוראות פרט (61) בתוספת הרביעית;

טור ב' סכום העיצום הכספי (בשקלים חדשים)	טור א' ההפרה
320,000	62. ארגון שלא כתב, יישם או עדכן נהלים לביצוע בדיקות רקע ומהימנות אבטחתית לעובדים, מנהלים וספקים הבאים במגע עם נכסי סייבר ותהליכים קריטיים, טרם קבלתם ועל בסיס עיתי בניגוד להוראות פרט (62) בתוספת הרביעית;
320,000	63. ארגון שלא כתב, יישם או עדכן נהלים להסדרת פעולות הגנת סייבר הנדרשות בעת קליטת עובדים, שינויי תפקידים בתוך הארגון, וסיום העסקה – לרבות ביטול מיידי של הרשאות גישה והחזרת נכסים פיזיים בניגוד להוראות פרט (63) בתוספת הרביעית.

תוספת שישית

(סעיף 52)

א. המגזר

המגזר
מגזר השירותים הדיגיטליים ושירותי האחסון

ב. אישור- לעניין תוספת זו- אחד מהאישורים הבאים:

1. אישור על הימצאות הארגון ברשימת **FedRAMP Marketplace** המפורסמת באינטרנט בסטטוס **Authorized**.
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)**.
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** (**EA**)
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 (**ISRAC**) . על הסמכה כאמור יחולו ההוראות לפי חוק הרשות הלאומית להסמכת מעבדות, בשינויים המחויבים. הרשות להסמכת מעבדות תקבע כללים לעניין הסמכה של גופים כאמור בהסכמת מערך הסייבר הלאומי.

בפרט זה-

"חוק הרשות הלאומית להסמכת מעבדות"- חוק הרשות הלאומית להסמכת מעבדות, התשנ"ז-1997[23].

"הרשות הלאומית להסמכת מעבדות" – הרשות הלאומית להסמכת מעבדות שהוקמה לפי חוק הרשות הלאומית להסמכת מעבדות.

[23] ס"ח תשנ"ז 1624, עמ' 156.

דברי הסבר

כללי

מרחב הסייבר מהווה זה מכבר מרחב פעולה מערכתי, חוצה גבולות ורב מימדי, המשמש כתשתית אסטרטגית לפעילות אנושית, כלכלית, חברתית ובעל השפעה מכרעת על תהליכים, מגמות ועיצוב פני התקשורת האנושית.

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

מדינת ישראל היא אחת המדינות המותקפות ביותר בסייבר בעולם. מתחילת הלחימה במסגרת "חרבות ברזל" בחודש אוקטובר 2023, ניכרה עלייה בהיקף ובעוצמה של תקיפות הסייבר נגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלה היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עלולות להוביל לפגיעה בחיי אדם, הן בשגרה והן בחירום. האיום בולט במיוחד בנוגע לארגונים חיוניים כגון בתחום האנרגיה, בריאות, תחבורה, תקשורת, ועוד, כמו גם ביחס לארגונים במגזר השירותים הדיגטליים ושירותי האחסון. פוטנציאל הפגיעה בארגונים אלו, מעצם מהותם, חורג מהנזק העלול להיגרם לארגון הבודד הנתקף, ועלול להביא לפגיעה רחבה יותר בציבור או במשק. על כן נדרש מענה שיביא להגנה הנדרשת על הארגונים ומכאן גם להגנה על המשק, על ליבת החוסן הלאומי, הגנה על ביטחון המדינה, ביטחון הציבור ורציפות אספקתם של שירותים חיוניים.

על אף חומרת הסיכון הנשקף מתקיפות הסייבר והנזקים הממשיים העלולים להיגרם מתקיפות כאמור, כמו גם התועלת הברורה בהתגוננות ומניעת תקיפה על פני התמודדות עם השלכות התקיפה ועלויות ההתאוששות והשיקום לאחריה - ארגונים רבים במשק הישראלי אינם נוקטים באמצעים מספקים להגנה בסייבר, בעיקר נוכח היעדר הפנמת הסיכון מתקיפות, ובכך מתגברת משמעותית ההסתברות למתקפות סייבר מוצלחות ובעלות השלכות קשות.

במרבית מדינות המערב קיימת רגולציה מתקדמת בתחום הגנת הסייבר, בדגש על מדינות האיחוד האירופי, בריטניה, אוסטרליה וקנדה. נציבות האיחוד האירופאי אישרה בנובמבר 2022 עדכון של הרגולציה שהתקבלה כבר בשנת 2016 (NIS Directive), בנושא הגנת סייבר. בנוסף לחובות הקיימות זה מכבר מתוקף NIS Directive וביניהן גיבוש אסטרטגית הגנת סייבר, הקמת גופים לאומיים מוסמכים בתחום הסייבר וגיבוש אסדרה לתשתיות קריטיות וחיוניות, הדירקטיבה העדכנית (NIS2) הרחיבה את מספר המגזרים המפוקחים ואת היקף המפוקחים בכל מגזר, וכן חיזקה את סמכויות הפיקוח והאכיפה.

על אף חשיבותו המכרעת של מרחב הסייבר, בולטת בהיעדרה מסגרת חקיקתית, ייעודית ומקיפה, בראייה לאומית. מצב זה יוצר פער משמעותי בין רמת האיום הגבוהה לבין יכולת המדינה להבטיח רמת הגנה נאותה, סדורה על נכסים ותשתיות בעלי חשיבות לאומית.

סיכוני הסייבר בישראל והשלכותיהם האפשריות, ובהמשך לכך חיוניות החקיקה הלאומית הנדרשת לאסדרת תחום, זה קיבלו בישראל ביטוי בין השאר בדוחות שונים של מבקר המדינה.

מטרת תזכיר החוק המוצע להביא להגנה לאומית טובה יותר על תפקודו הרציף והבטוח של מרחב הסייבר הלאומי, כחלק מחוסנה ובטחונה הלאומי של מדינת ישראל, בדגש על הגנת ארגונים חיוניים וספקי שירותים דיגטליים ושירותי אחסון. החקיקה המקודמת מבוססת על הצרכים והאיומים בראייה לאומית, על החלטות הממשלה ומדיניותה בתחום הגנת הסייבר, התפיסה העומדת בבסיס החלטות הממשלה האמורות והניסיון שנצבר מאז קבלתן, במיוחד נוכח לקחי תקופת "חרבות ברזל" ו"עם כלביא". מדובר בחקיקה ממוקדת, דיפרנציאלית המבוססת על ניהול סיכונים ואיזון רגולטורי.

בחוק מוצע לעגן את **מסגרת האסדרה והפיקוח על הגנת הסייבר הלאומית**, תוך עיגון רוחבי של סמכויות וכלי הגנת הסייבר של משרדי הממשלה השונים, ואסדרה דיפרנציאלית ביחס למגזרים ולארגונים החיוניים בהם, וכן ביחס לספקי השירותים הדיגטליים ושירותי האחסון; זאת לצד קביעת חובות הארגונים, בדגש על הארגונים החיוניים, לפעול להגנת הסייבר, הן בשגרה והן בעת התמודדות עם תקיפת סייבר, כל זאת תוך הקפדה על שימור הגמישות הנדרשת בתחום עיסוק משתנה זה.

יודגש כי תזכיר החוק המוצע נועד להביא לאסדרה של הגנת הסייבר הלאומית בראייה מתכללת, כהשלמה להסדרה הלאומית הקיימת לעניין תשתית מדינה קריטית בהתאם לחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998, וכן כהשלמה להסדרים המגזריים במגזרי המשק השונים ככל שקיימים.

באמצעות קביעת מסגרת סמכויות ברורה, עקרונות פעולה מוגדרים ומנגנוני פיקוח ואכיפה, מבקש תזכיר החוק המוצע לחזק את החוסן הלאומי במרחב הסייבר, לשפר את רמת המוכנות והתגובה לתקיפות סייבר, לעודד היערכות אשר עלותה נמוכה באופן ניכר מהעלות הכלכלית והחברתית הכרוכה בשיקום שלאחר התקיפה. בכך יתרום החוק המוצע ליציבות המשק, להגנה על על הציבור ולהגנה על רציפות תפקודם של השירותים החיוניים, כחלק מביטחונה הלאומי של מדינת ישראל.

פרק א' – הגדרות:

סעיף 1

בסעיף זה מוצע לקבוע הגדרות למונחים בהם נעשה שימוש בחוק המוצע.

מוצע להגדיר "מגזר משק" כמגזר או תת מגזר משק המנוי בטור א' בתוספת הראשונה או השנייה, אשר ביחס אליו פועלת הרשות המוסמכת בהתאם לחוק זה.

מוצע לקבוע בתוספת הראשונה והשנייה את מגזרי המשק אשר בהם בין השאר, יוגדרו ארגונים חיוניים לפי החוק, לרבות הרשות המוסמכת, הגורם המסמיך והגורם המאסדר שיפעלו ביחס לכל מגזר במשק, כפי שיפורט להלן. התוספת השנייה מיוחדת למגזר משרדי הממשלה.

מוצע להגדיר "רשות מוסמכת" כגוף המנוי בטור ג' בתוספת הראשונה או בתוספת השניה. בתוספת השניה נקבע שמערך הדיגיטל יהווה "רשות מוסמכת" לעניין חוק זה, אל מול גופים ממשלתיים, למעט אלה שהוחרגו בהתאם להגדרת "גוף ממשלתי" בסעיף 1, היינו למעט משטרת ישראל, שירות הביטחון הכללי, המוסד למודיעין ולתפקידים מיוחדים, מערך הסייבר הלאומי ומערכת הביטחון באמצעות המלמ"ב וזאת בהתאם לעקרונות החלטת ממשלה 2443, שכותרתה "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" מיום 15.2.2015 (להלן "החלטה 2443"). בהחלטה נקבע שייעוד היחידה להגנת הסייבר בממשלה (יה"ב) להכווין ולהנחות מקצועית בתחום הגנת הסייבר את כלל משרדי הממשלה ויחידות הסמך למעט הגופים המיוחדים.

עוד מוצע להגדיר, בכל רשות מוסמכת:

א. "גורם מאסדר", שהוא השר הממונה על הרשות המוסמכת או גורם אחר האמון על האסדרה של הרשות המוסמכת ביחס למגזר משק המנוי בטור ה' בתוספת הראשונה או השניה;

ב. "גורם מסמיך", שהוא הגורם המנוי בטור ד' בתוספת הראשונה או השנייה, שיסמיך, מבין עובדי הרשות המוסמכת "עובד מוסמך מגזרי" אחד או יותר, ו-"מנהל בכיר ברשות מוסמכת" אחד או יותר.

בנוסף, מוצע להגדיר "מנהל בכיר במערך הסייבר הלאומי" שהוא עובד בכיר במערך הסייבר הלאומי (להלן גם: "מערך הסייבר" או "המערך") אשר דרגתו ראש אגף לפחות שיוסמך לעניין זה על ידי ראש מערך הסייבר הלאומי. כן מוצע להגדיר -"מנהל בכיר ברשות מוסמכת" כעובד בכיר ברשות המוסמכת שדרגתו ראש אגף לפחות אשר הגורם המסמיך הסמיכו לעניין זה.

מנהל בכיר במערך הסייבר הלאומי ומנהל בכיר ברשות מוסמכת, מוסמכים, לפי העניין, לקבל דיווחים של ארגונים חיוניים על תקיפות משמעותיות נגדם בהתאם למוצע בסעיף 11 , לקבוע שתקיפת סייבר היא תקיפה חמורה ולדרוש ידיעות ומסמכים לשם קבלת החלטה אם תקיפה היא תקיפה חמורה בהתאם למוצע בסעיף 14, לפטור ארגון חיוני שנתקף בתקיפה חמורה מהחובה המוצעת בסעיף 15 ליידע ארגון אחר שעלול להפגע מהתקיפה, לקבוע שקיים אינטרס לאומי לסייע לארגון בהתאם למוצע בסעיף 42, לאשר למי שמתקיימים בו התנאים הקבועים בסעיף 48 המוצע לשמש כמומחה חיצוני, ולאשר פרסום פרסום פומבי ברבים של זהות ארגון לפי סעיף 49(ג) המוצע.
כן מוצע להגדיר "עובד מוסמך במערך הסייבר הלאומי", כמשמעותו בסעיף 6(א) המוצע ו-"עובד מוסמך מגזרי", כמשמעותו בסעיף 6(ב) המוצע; עניינם של סעיפים קטנים אלה בהסמכת עובד מוסמך במערך הסייבר הלאומי ועובד מוסמך מגזרי, בהתאמה.

מוצע להגדיר "שירותי אחסון" כשירותי אחסון של חומר מחשב הניתנים בעבור אחר או שירותי אספקת תשתית לאחסון או לעיבוד של חומר מחשב.
עוד מוצע להגדיר "שירותים דיגיטליים" כשירות שהוא אחד מאלה, הניתן עבור אחר:
א. שירותי תכנה, לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח של תכנה;
ב. שירותי ניהול או הפעלה של מערכות מחשבים המשלבות חומרה, תכנה וטכנולוגיות תקשורת;
ג. שירותי עיבוד נתונים, הזנתם או שחזורם, התקנה והגדרת תצורה של מחשבים, התקנת תכנה או שירותי הגנת סייבר;
ד. אספקת או התקנת של מחשבים או ציוד בקרה, המהווים חלק ממכונות וציוד תעשייתי.

בהמשך לכך, מוצע להגדיר "ספק שירותים דיגיטליים או שירותי אחסון" כאחד מאלה:
(1) מי שעיסוקו באספקת שירותי אחסון או שירותים דיגטליים, ומתקיים חיבור פיזי או לוגי, קבוע או עיתי, או שמתבצעת העברת חומר מחשב קבועה או עיתית, ממחשביו למחשבי מקבל השירות;
(2) מי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי אחסון או שירותים דיגטליים;

מוצע לקבוע ש-"נכס מידע משמעותי" הוא מידע או מאגר מידע שתקיפת סייבר נגדו עלולה להוביל לפגיעה בבטחון המדינה או בביטחון הציבור. פגיעה במהימנות או זמינות נכס מידע משמעותי או זליגתו, עלולות להיות בעלות השלכות הרות גורל על בטחון המדינה או ביטחון הציבור. בהתאם, כפי שיפורט בהמשך, חובת ארגון חיוני לדווח על תקיפת סייבר משמעותית לרשות המוסמכת ולמערך הסייבר הלאומי לפי סעיף 11 המוצע תחול בין היתר אם התקיפה עלולה להביא לפגיעה או גישה של גורם שאינו מורשה לנכס מידע משמעותי. בנוסף, בסעיף 14 המוצע, מוצע להגדיר שתקיפת סייבר חמורה היא, בין היתר, תקיפה העלולה לאפשר גישה לגורם שאינו מורשה לנכס מידע משמעותי של ארגון חיוני.

עוד מוצע לקבוע ש-"פגיעות חמורה" היא נקודת תורפה במחשב או בחומר מחשב אשר אפשר לנצל לביצוע תקיפת סייבר שמערך הסייבר הלאומי מצא כי לנוכח מאפייניה היא יוצרת סיכון משמעותי לתקיפת סייבר. כפי שיפורט בהמשך, בסעיף 43 בו מוצע לעגן את פעילות מערך הסייבר הלאומי לאיתור פגיעויות חמורות המוכרות למערך הסייבר הלאומי ולמתן התרעה עליהן.

כן מוצע להגדיר "פעולה להגנת סייבר בחומר מחשב" כמתן הוראות למחשב בשפה קריאת מחשב לשם הגנת סייבר,

ובכלל זה הוראה לסריקה, לעיבוד, להסרה של חומר מחשב הנוגע לתקיפת סייבר, להתקנת סוג תוכנה שפעולתה מוגבלת לרשת הארגון בלבד, לחסימה או לניתוק של מחשב או ליצירת עותק של חומר המחשב. כפי שיפורט בהמשך, הגדרה זו מתייחסת לסמכויות המוצעות בנסיבות בהן נתקף ארגון בתקיפה חמורה, ולא פעל באופן הולם לצורך איתור התקיפה, מניעתה או בלימתה.

מוצע להגדיר "תקיפת סייבר" כפעולה או חשש ממשי לפעולה, שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב השמור בו, לרבות:

א. שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;

ב. מחיקת חומר מחשב, שינויו, שיבושו או הפרעה לשימוש בו;

ג. אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;

ד. חדירה שלא כדין לחומר מחשב כהגדרתה בסעיף 4 לחוק המחשבים, תשנ"ה- 1995;

ה. האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט– 1979;

ו. גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הוצאתו שלא כדין של מידע, לרבות בדרך של העתקתו על-ידי גורם כאמור;

ז. הפרעה או מניעת נגישות של מחשב לרשת תקשורת;

כפי שיפורט בהמשך, הגדרה זו הנה הבסיס להגדרת תקיפת סייבר משמעותית או תקיפת סייבר חמורה לפי החוק המוצע.

מוצע להגדיר "גוף מונחה" כגוף המנוי בפרטים 2 ו-3 בתוספת הראשונה, בתוספת הרביעית או בתוספת החמישית לחוק להסדרת הבטחון בגופים ציבוריים, התשנ"ח-1998 (להלן: "החוק להסדרת הבטחון" או "החוק להסדרת הבטחון הגופים ציבוריים"). הגופים המנויים בתוספות האמורות לחוק להסדרת הבטחון בגופים ציבוריים הם תשתיות מדינה קריטיות וספקים של מערכת הבטחון, המונחים כבר כיום מכח החוק להסדרת הבטחון, על ידי הממונה על הבטחון במערכת הבטחון, שירות הבטחון הכללי ומערך הסייבר הלאומי.

פרק ב' – מערך הסייבר הלאומי:

סעיף 2

מוצע לקבוע בסעיף קטן (א) שמערך הסייבר הלאומי הוא גוף מבצעי-טכנולוגי הפועל כיחידה עצמאית במשרד ראש הממשלה; וכן לקבוע בסעיף קטן (ב) כי השר הממונה על מערך הסייבר הלאומי הוא ראש הממשלה. המערך אחראי על הגנת הסייבר הלאומית, ולשם כך פועל במספר אפיקים ובהם הגנה על המשק מפני מתקפות סייבר וקידום רמת ההגנה והחוסן בשיגרה, תכלול הניהול הלאומי של מאמצי הגנת הסייבר, ועוד.

סעיף 3

הגנת סייבר לאומית אפקטיבית, מבוססת בין השאר על תכלול לאומי של תחום הגנת הסייבר, על מכלול היבטיו, וכלל השותפים הרלוונטיים להבדיל מטיפול מגזרי מבודל. מוצע לקבוע שמערך הסייבר הלאומי יהיה מופקד על קידום, תיאום, הפעלה וביצוע, בהתאם לצורך, של מאמצי הגנת הסייבר הלאומית, לרבות טיפול באיומי סייבר ובאירועי סייבר בזמן אמת, ריכוז מחקר ומודיעין ועבודה עם הגופים המיוחדים. הכל, מבלי לפגוע בתפקידי מערך הסייבר הלאומי שנקבעו מכח כל דין, לרבות החוק להסדרת הבטחון בגופים ציבוריים, וכן בתפקידים שנקבעו בהחלטות הממשלה, לרבות החלטת ממשלה מספר 2444 שכותרתה "קידום ההיערכות הלאומית להגנת הסייבר" מיום 15.2.2015 (להלן "החלטה 2444") והחלטה 2443, לרבות תפקידו של מערך הסייבר כנקודת ממשק מרכזית

בין גופי הביטחון לבין הגורמים במשק.

בכלל האמור יפעל מערך הסייבר הלאומי לביצוע התפקידים הבאים:

א. ליזום ולקדם מדיניות ואסטרטגיה לאומית בתחום הגנת הסייבר.

ב. לרכז תמונת מצב של רמת הגנת הסייבר הלאומית, בראיה לאומית וסקטוריאלית.

ג. לחזק את החוסן הלאומי בהגנת סייבר ולקדם את ההתמודדות עם תקיפות סייבר, לרבות באמעות הובלת בניין הכוח הלאומי.

ד. לפעול להעלאת המודעות בציבור להתנהגות בטוחה במרחב הסייבר ולפרסם התרעות והמלצות לציבור להעלאת רמת הגנת הסייבר.

ה. לקדם ולעודד מחקר ופיתוח של תחום הגנת הסייבר, לרבות פיתוח התעשייה והגנה על מוצרים.

ו. לקדם בחינת והטמעת טכנולוגיות מתפתחות להגנת סייבר; תפקיד זה נדרש לנוכח קצב התפתחות הטכנולוגיה שמשפיע על יכולות ואופני התקיפות בסייבר, והצורך 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.

ז. לקדם שיתוף פעולה בתחום הגנת הסייבר במישור הבינלאומי ולערוך הסכמי שיתוף פעולה בתחום הגנת הסייבר.

ח. לייעץ לראש הממשלה ולממשלה בתחום הגנת הסייבר.

עוד מוצע, לשם ביצוע תפקידיו של מערך הסייבר הלאומי, לעגן את פעילות המרכז לאומי לסיוע בהתמודדות עם אירוע סייבר (ה-CERT הלאומי), הכולל מרכז הלאומי לקבלת דיווחים על תקיפות סייבר ופניות לעניין הגנת סייבר ולסיוע בהתמודדות עם אירועי סייבר ואת מרכז השליטה והבקרה הלאומי למול איומי סייבר (ה-SOC הלאומי), המרכזים מופעלים כיום מכוח החלטה 2444 והחלטה 2443 ובהתאם לעקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר.

בנוסף, ובמסגרת עיגון האסדרה הלאומית, מוצע לעגן ולקבוע שלשם ביצוע תפקידיו, מערך הסייבר הלאומי ינחה מקצועית את היחידות המגזריות במשרדי הממשלה לקידום הגנת הסייבר, לרבות לעניין אופן יישום שנתי ורב שנתי של מדיניות ואסטרטגיית הסייבר הלאומית לצורך שיפור רמת ההגנה בסייבר במגזר ולעניין התמודדות עם תקיפות סייבר חמורות במגזר. בכלל האמור, יפעל מערך הסייבר הלאומי לשתף עם היחידות המגזריות, בהתאם לכל דין והסכם, ובכפוף לשיקול דעתו:

א. תמונת מצב של רמת הגנת הסייבר הלאומית, כאמור בסעיף 3(א)(2) המוצע.

ב. הערכות מקצועיות של מערך הסיבר הלאומי ומידע, ובכלל זה מידע מודיעני, אשר המערך מצא כי הם נדרשים להגנת הסייבר במגזר. זאת, לרבות מידע על תקיפות סייבר והתרעות, לרבות מידע הנוגע לפגיעויות חמורות.

ג. אמצעים טכנולוגיים העומדים לרשות מערך הסייבר הלאומי אשר לפי שיקול דעת המערך נדרשים להגנת הסייבר במגזר.

סעיף 4

מוצע לקבוע בסעיף קטן (א) שראש מערך הסייבר הלאומי ימונה על ידי הממשלה, לפי הצעת ראש הממשלה, בהתאם להוראות חוק שירות המדינה (מינויים), תשי"ט-1959.

חוק זה בא להוסיף על החלטת ממשלה 3270 מיום 17.12.2017 (להלן "החלטת ממשלה 3270"), בה נקבע בין השאר כי ראש מערך הסייבר הלאומי יהיה בעל מומחיות, רקע וניסיון בתחומים הנוגעים לענייני הסייבר של מדינת

ישראל. כן נקבע בהחלטת ממשלה 3270 פטור מחובת המכרז הפומבי למשרת ראש המערך, בהתאם לסעיף 21 לחוק שירות המדינה (מינויים), התשי"ט-1959, 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 מס' 345 מיום 14 בספטמבר 1999 שכותרתה "משרות שהמינוי להן נעשה על-ידי הממשלה או באישורה - פטור ממכרז לפי סעיף 21 לחוק שירות המדינה (מינויים), התשי"ט-1959".

כמו כן, מוצע לקבוע בסעיף קטן (ב) שראש המערך יהיה מופקד על ניהול המערך ועל ביצוע תפקידיו, ויהיו לו כל הסמכויות הנתונות לפי חוק זה לעובדי המערך. עוד מוצע לקבוע בסעיף קטן (ג) שראש המערך יהיה רשאי לאצול את סמכויותיו לפי חוק זה למנהל בכיר במערך הסייבר הלאומי, וזאת פרט לסמכות לתת, בנסיבות מסוימות, הוראות מקצועיות שעניינן הגנת סייבר בארגונים חיוניים, המוצעת בסעיף 10(ה).

פרק ג' – יחידה מגזרית ועובדים מוסמכים:

סעיף 5

המודל האסדרתי הממשלתי הקיים בישראל בתחום הגנת הסייבר, המבוסס בעיקרו על החלטה 2443, הוא במהותו מודל מבוזר, המקנה אחריות לרגולטורים בקידום הגנת הסייבר במגזר המשק. הניסיון הנצבר מאז התקבלה החלטה 2443 בשנת 2015, מלמד שקיימת שונות רבה בין התשומות, המשאבים, היכולות והכלים שהרגולטורים השונים משקיעים בתחום הגנת הסייבר ושונות זו מביאה, בין היתר, לפערים ניכרים במצב ההגנה במגזרים שונים במשק.

במהלך עבודת המטה שנערכה במסגרת גיבוש הצעת החוק עלו חלופות: האחת, מעבר למודל לאומיי ריכוזי מובהק, שבו כלל הסמכויות נתונות בידי מערך הסייבר הלאומי; והשניה, עיגון המודל הקיים תוך מתן מענה לפערים הקיימים והדגש על הצורך בתכלול לאומי בתחום הגנת הסייבר. בשים לב להיכרות המעמיקה של הרגולטורים המגזריים עם מגזרי המשק שהם מאסדרים, הוחלט לשמר ולעגן בחוק את המודל המבוזר מהחלטת ממשלה 2443, תוך שימור, עיגון וחידוד מודל ההנחייה הלאומי, לרבות ההנחיה המקצועית של מערך הסייבר את היחידות המגזריות, בשים לב לכך שמערך הסייבר הלאומי הוא הגורם המדינתי בעל המיומנות והידע בתחום הגנת הסייבר, המחזיק בתמונה הלאומית הכוללת בתחום.

בהתאמה, במסגרת האסדרה הלאומית של תחום הגנת הסייבר, מוצע לעגן בין השאר בחוק את ההסדר הקבוע בעיקרו בהחלטה 2443, לפיו ברשות מוסמכת תפעל יחידה לקידום הגנת הסייבר במגזר המשק (להלן "יחידה מגזרית"), בהתאם להנחיה מקצועית של מערך הסייבר הלאומי. עוד מוצע לחדד ולקבוע שבין תפקידי היחידה המגזרית:

א. לפעול לשיפור רמת ההגנה במגזר המשק בהתאם למדיניות ואסטרטגיית הגנת הסייבר הלאומית שיקבעו לפי סעיף 3(א)(1) המוצע, לרבות באמצעות קידום אסדרה ייעודית למגזר המשק או חלק ממנו, והנחיות מקצועיות מגזריות.

ב. למפות באופן שוטף את הארגונים החיוניים במגזר המשק.

ג. לרכז את נתוני רמת ההגנה בסייבר בארגונים החיוניים במגזר המשק, ולשתפה עם מערך הסייבר הלאומי באופן שוטף, ולכל הפחות אחת לרבעון.

ד. לוודא פיקוח ואת קיומו של מנגנון אכיפה לפי חוק זה במגזר המשק. יובהר, שסמכויות הפיקוח והאכיפה המוסדרות לפי חוק זה, אפשר שיופעלו בפועל ברשות מוסמכת על ידי עובד מוסמך כפי שיקבע הגורם המסמיך גם אם אינו עובד ביחידה המגזרית והדבר נתון לשיקול דעת הגורם המסמיך.

ה. לפעול להנחיית ארגונים חיוניים במגזר המשק בטיפול בתקיפות סייבר חמורות בהתאם להוראות חוק זה.

ו. לפעול לקידום תהליכי שיתוף מידע וידע הנוגע להגנת סייבר במגזר המשק, בין היתר מול מרכז השליטה והבקרה הלאומי (NSOC), וזאת לרבות מידע אודות אירועים, איומים, חולשות, פוגענים ונוזקות למרכז לסיוע בהתמודדות עם איומי סייבר. עוד מוצע לעגן את אפשרות היחידה המגזרית להפעיל לשם כך מרכז שליטה ובקרה מגזרי מול איומי סייבר (SOC מגזרי).

ז. לפעול לקידום העלאת המודעות לסיכוני הסייבר במגזר המשק, ולפרסם התרעות והמלצות להעלאת רמת הגנת הסייבר במגזר בהתייעצות עם מערך הסייבר הלאומי.

ח. להכין תכנית עבודה שנתית או רב שנתית בהתאם לדגשי מערך הסייבר הלאומי ולאחר היוועצות עמו, שתובא לאישור הגורם המסמיך, ותוצג לאחר מכן למערך הסייבר הלאומי.

ט. להכין עדכון מסכם אחת לשנה, שיועבר למערך הסייבר הלאומי, ויכלול בין השאר את מיפוי הארגונים החיוניים במגזר המשק, נתוני רמת ההגנה בארגונים חיוניים במגזר המשק, נתונים בדבר פיקוח ואכיפה ופעולות להטלת עיצומים על ארגון חיוני, פעולות לקידום תהליכי שיתוף המידע והידע הנוגע להגנת סייבר במגזר, לרבות אל מול ה-NSOC והפעלת SOC מגזרי, ככל שמופעל, נתונים בדבר פעולות לקידום העלאת המודעות לסיכוני הסייבר במגזר המשק ופרסום התרעות והמלצות להעלאת רמת הגנת הסייבר במגזר, נתונים אודות תקיפות סייבר חמורות, כמשמעותן בסעיף 14(א) המוצע, שהתרחשו במגזר המשק ומתן הוראות להתמודדות עם תקיפת סייבר חמורה לארגונים חיוניים לפי סעיפים 15 או 16 המוצעים.

סעיף 6

מוצע לקבוע שהגורם המסמיך ברשות מוסמכת יהיה רשאי להסמיך מבין עובדי הרשות המוסמכת עובד אחד או יותר, שיהיו נתונות לו סמכויות הנתונות לעובדים מוסמכים מגזריים, לפי חוק זה, כולן או חלקן. העובדים יוכלו להפעיל את סמכויותיהם רק לתכלית של ביצוע הוראות חוק זה, במגזר המשק.

הסמכויות הנתונות לעובד מוסמך מגזרי כוללות את הנדרשות לשם ביצוע חוק זה במגזר המשק: סמכות דרישת ידיעות ומסמכים שיש בהם כדי להבטיח את ביצועו של חוק זה או להקל על ביצועו לפי סעיף 12 המוצע; סמכות כניסה למקום לפי סעיף 13 המוצע - לשם פיקוח על עמידה בהוראות סעיף 10 המוצע שעניינו רמת הגנת סייבר ובהוראות סעיף 11 המוצע שעניינו דיווח על תקיפת סייבר משמעותית; וסמכות לתת הוראות לארגון חיוני בעת תקיפת סייבר חמורה בהתאם לסעיף 15 או 16 המוצעים לפי העניין. מובהר כי במסגרת המודל הלאומי המבוזר, פעולות הפיקוח, כמו גם הטלת עיצומים, ייעשו על ידי עובדים מוסמכים ברשויות המוסמכות בלבד.

בנוסף, מוצע לקבוע שראש מערך הסייבר הלאומי יהיה רשאי להסמיך מבין עובדי המערך, עובד אחד או יותר שיהיו לו הסמכויות הנתונות לעובד מוסמך במערך הסייבר הלאומי לפי חוק זה, כולן או חלקן, לשם ביצוע הוראות חוק זה. לעובד מוסמך במערך הסייבר הלאומי, יהיו נתונות סמכות מתן הוראות לארגון חיוני בעת תקיפת סייבר חמורה בהתאם לסעיף 15 או 16 המוצעים, לפי העניין. סמכות מתן הוראות כאמור תהיה נתונה לעובד מוסמך במערך הסייבר הלאומי כשמתקיימים התנאים הקבועים בסעיף 17 המוצע.

סעיף 7

על מנת להבטיח שהסמכויות בחוק המוצע יופעלו בידי עובדים כשירים ומיומנים להפעלתן, מוצע לקבוע שלא יוסמך עובד מוסמך מגזרי או עובד מוסמך במערך הסייבר הלאומי, אלא אם מתקיימים בו כל התנאים הבאים:

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

ב. הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה. ראש מערך הסייבר הלאומי יקבע הוראות בדבר תוכן והיקף ההכשרה המתאימה לעניין הסמכויות לפי סעיף זה.

ג. הגורם המסמיך מצא שהוא בעל ההכשרה, הידע, הכישורים והניסיון הנדרשים למילוי תפקידו בצורה נאותה, ובכלל זה ידע מעמיק בהגנת סייבר.

פרק ד' – אסדרה לאומית בתחום הגנת הסייבר:

סימן א': ארגון חיוני

סעיף 8

החוק המוצע מבקש להסדיר את פעילות הארגונים החיוניים לפעילות המשק במגזרים השונים בהיבטי הגנת הסייבר. בכלל האמור מבקש החוק המוצע להבטיח כי ארגון חיוני ינקוט את הפעולות הדרושות להבטחת רמת הגנת סייבר בסיסית, ידווח על תקיפות סייבר משמעותיות נגדו ויתמודד כנדרש עם תקיפות כאמור.

בסעיף זה מוצע לקבוע אילו ארגונים יוגדרו כארגונים חיוניים לעניין חוק זה, בחלוקה למגזרי המשק השונים. לצד זאת, מוצע לקבוע מנגנון המאפשר התאמה למצבים חריגים בהם לא נדרש שארגון העומד בתבחין יוגדר כארגון חיוני, או שבהם ארגון שאינו עומד בתבחין נדרש להיות מוגדר כחיוני.

בסעיף קטן (א)(1) מוצע לקבוע שכל גוף ממשלתי המנוי בטור א' בתוספת השניה, לרבות יחידות הסמך שלו, הוא ארגון חיוני. זאת, בתנאי שאינו נמנה על "הגופים המיוחדים" - מערך הסייבר הלאומי, משרד הביטחון, לרבות הממונה על הבטחון במערכת הביטחון, צבא ההגנה לישראל, שירות הביטחון הכללי, המוסד למודיעין ולתפקידים מיוחדים, ומשטרת ישראל; וכן בתנאי שאינו גוף מונחה.

בסעיף קטן (א)(2) מוצע לקבוע שארגון שמתקיימים לגביו התבחינים המגזריים המפורטים בתוספת השלישית לעניין ארגונים מאותו מגזר משק, ושאינו גוף מונחה - הוא ארגון חיוני. במקביל, מוצע לקבוע כי על אף האמור, ארגון כאמור לא יוגדר כארגון חיוני אם קבע הגורם המאסדר באותו מגזר משק, בהתאם לסעיף (ב) המוצע, שהארגון אינו ארגון חיוני.

בסעיף קטן (א)(3) מוצע לקבוע שארגון חיוני הוא גם ארגון שהגורם המאסדר קבע לגביו באופן חריג, שהוא ארגון חיוני אף על פי שאינו עומד בתבחינים המגזריים המפורטים בתוספת השלישית לעניין ארגונים מאותו מגזר משק, בהתאם לתנאי סעיף (ב).

בסעיף קטן (ב) מוצע לקבוע שגורם מאסדר יהיה רשאי לקבוע ביחס לארגון במגזרו, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, כי על אף שמתקיימים לגבי הארגון התבחינים לארגון חיוני במגזר המשק, הארגון אינו ארגון חיוני. קביעה כאמור יכולה להתבצע גם לאחר פניית הארגון החיוני לגורם המאסדר בבקשה להחריגו. עוד מוצע לקבוע שגורם מאסדר יהיה רשאי לקבוע ביחס לארגון במגזרו, בהחלטה מנומקת בכתב ולאחר שנתן לארגון הזדמנות להשמיע את טענותיו, כי הארגון הוא ארגון חיוני גם אם לא מתקיימים לגביו התבחינים לארגון חיוני במגזר המשק, ובתנאי שאינו גוף מונחה. כל זאת, אם מתקיימות נסיבות חריגות המצדיקות קביעה כאמור ביחס לארגון, בהתחשב בסוג הארגון, מאפייני פעילותו והשלכות פגיעת תקיפת סייבר בפעילות הארגון לרבות בהתייחס לביטחון המדינה, בטחון הציבור, חיי אדם, כלכלת המדינה או לרציפות אספקתם של שירותים חיוניים לציבור, ובכלל האמור בהתחשב בחשיבות זמינות השירות של הארגון בהתחשב בחלופות לשירות, למספר המשתמשים התלויים בשירות שהארגון מספק, לנתח השוק של שירות הארגון, לפריסה הגיאוגרפית של השירות שמספק הארגון, ולתלות של ארגונים אחרים בשירות שמספק הארגון.

עוד מוצע לקבוע שגורם מאסדר יידרש, טרם קבלת החלטתו בנושא, לשמוע את עמדת הועדה המייעצת בעניין. בראשות הוועדה יעמוד עובד בכיר ברשות המוסמכת שהסמיך הגורם המאסדר, ויהיו חברים בה נציגי מערך הסייבר הלאומי, משרד האוצר, משרד הביטחון, שירות הביטחון הכללי והיעוץ המשפטי לממשלה, אשר יוכלו לבחון את הנושא מנקודת מבטם וגם בראיית רוחב. הוועדה המייעצת לפי סעיף זה, תעביר את עמדתה לגורם

מאסדר שפנה אליה בתוך 30 יום.
בסעיף קטן (ג) מוצע לקבוע כי אם קבע בהתאם לסעיף (ב) הגורם המאסדר שארגון הוא ארגון חיוני או שאינו ארגון חיוני, יודיע על כך לארגון ויידע את מערך הסייבר הלאומי בתוך 14 ימים תוך פירוט נימוקי ההחלטה. קביעת הגורם המאסדר תיכנס לתוקף במועד מסירת ההודעה לארגון.
בסעיף קטן (ד) מוצע שאם נקבע ארגון כארגון חיוני בהתאם לסעיף (ב), תינתן לו שהות לנקוט בצעדים הנדרשים בכדי לעמוד בדרישות החוק, כך שהחובה לעמוד ברמת ההגנה בהתאם לסעיפים 10(ב) עד 10(ד) תחול בחלוף 12 חודשים ממועד הקביעה בדבר היותו ארגון חיוני, זאת מתוך ההבנה כי נדרש פרק זמן להיערכות כדי לעמוד ברמת ההגנה הנדרשת.
בסעיף קטן (ה) מוצע לקבוע שארגון שעומד בתבחינים להגדרתו כארגון חיוני לפי סעיף קטן (א)(2) ביותר ממגזר משק אחד, רשאי לפנות לגורמים המאסדרים באותם מגזרי משק, לצורך קביעתם, בהתייעצות עם מערך הסייבר הלאומי, את מגזר המשק האחד בו יוגדר הארגון כארגון חיוני לפי חוק זה. זאת, בכדי לייצר וודאות עבור ארגונים במשק באשר לזהות המאסדר שסמכויותיו חלות ביחס אליהם.
בסעיף קטן (ו), בכדי לאפשר גמישות והתאמה של התבחינים המגזריים לשינויי הזמנים והצרכים, מוצע לקבוע שהגורם המאסדר, בהתייעצות עם ראש מערך הסייבר הלאומי ועם שר האוצר, ובאישור ועדה מועדות הכנסת, רשאי לשנות את התבחינים לארגונים חיוניים במגזר המשק, המנויים בתוספת השלישית, ובלבד ששינוי כאמור ייעשה על בסיס כללים ואמות מידה מקצועיים המיושמים במדינות מפותחות עם שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת.

סעיף 9

מתוך ההבנה כי האיומים במרחב הסייבר והסיכונים עבור המגזרים השונים משתנים, ומתוך הרצון לשמר גמישות במקרים הנדרשים, מוצע לקבוע שראש הממשלה, לאחר שקילת המלצת ראש מערך הסייבר הלאומי, בהיוועצות עם הגורם המאסדר ושר האוצר, ובאישור ועדה מועדות הכנסת, יהיה רשאי לשנות את התוספת הראשונה או השניה, לרבות הוספת מגזר משק חדש לגביו יחול חוק זה, הוספת תתי מגזרים, ושינוי רשות המוסמכת, הגורם המסמיך או הגורם המאסדר ביחס למגזר משק מסוים.

סימן ב': הגנת סייבר בארגונים וחובת דיווח

סעיף 10

סעיף זה נועד להסדיר את רמת הגנת הסייבר שעל ארגונים במשק לעמוד בה.
סעיף קטן (א) מבהיר למען הסר ספק, את המצב המשפטי הקיים, במסגרתו כל ארגון, לרבות ארגון חיוני, אחראי להבטחת רמת הגנת הסייבר הראויה בו, בהתאם לסוג ואופי פעילותו ותוך ניהול סיכון הולם.
ביחס לארגון חיוני, לאור חשיבותו להמשך שמירה על הרציפות התפקודית, לצד חובת הארגון הכללית להבטיח רמת הגנת סייבר ראויה בו, מוצע לקבוע בסעיף קטן (ב) חובות פרטניות לעניין רמת הגנה בסיסית שארגון חיוני נדרש לעמוד בהן, המפורטות בחלק א' לתוספת הרביעית. זאת באמצעות עמידה בהוראות הרלוונטיות באחד התקנים המנויים בחלק ב' לתוספת הרביעית תוך הבטחת הלימה לדרישות המפורטות בחלק א' לתוספת הרביעית, וזאת במטרה להקל על יישום הדרישות בתוספת הרביעית על ידי הארגונים החיוניים, ולהתאים את אופן יישום הדרישות בהתאם לאופן הנדרש בתקנים מקצועיים מקובלים בהתאמות הנדרשות. יובהר כי סעיף זה אינו מחייב עמידה מלאה בכל הוראות התקן הנבחר על ידי הארגון החיוני, ככל שהוראות התקן רחבות יותר מהדרישות המנויות בחלק א לתוספת הרביעית, אלא מציע לקבוע שנדרש לעמוד בהוראות הרלוונטיות לדרישות רמת ההגנה המפורטות בתוספת בלבד. הכל, כמפורט לעיל מבלי לגרוע מהחובה הכללית לעמוד ברמת ההגנה הנדרשת. כן מוצע

לקבוע, בכדי להנגיש שינויים בהוראות התקינה לפיהן יש לפעול, כי מערך הסייבר הלאומי יפרסם באתר האינטרנט שלו עדכונים רלוונטיים של התקינה. ההוראות המנויות בתוספת הרביעית נועדו להבטיח רמת הגנה בסיסית באמצעות הוראות הנוגעות למדיניות לניתוח סיכונים והגנה על נכסי סייבר; היערכות והתמודדות עם אירועי סייבר; רציפות תפקודית והמשכיות השירות; הגנת סייבר בשרשרת האספקה; פיתוח ותחזוקה של מערכות, חשיפה וטיפול בפגיעויות ותהליכי רכש; הגיינת מחשב בסיסית והדרכות; הצפנה והסתרת נכסי סייבר; בקרת גישה, ניהול נכסים, וטיפול בגורם האנושי. בכדי לאפשר עדכון של ההוראות המנויות בתוספת הרביעית מעת לעת בכדי להמשיך ולהבטיח הגנת סייבר בסיסית, מוצע לקבוע שראש הממשלה, לאחר שקילת המלצת ראש מערך הסייבר הלאומי, באישור ועדת החוץ והבטחון של הכנסת, רשאי לשנות את התוספת הרביעית.

כדי להשלים ולשפר את רמת ההגנה של ארגונים חיוניים ולאפשר התאמה מירבית של הסטנדרט המקצועי הנדרש למאפיינים היחודיים של כל מגזר משק, מוצע לקבוע בסעיף קטן (ג), שגורם מאסדר רשאי, לאחר התייעצות עם ראש מערך הסייבר הלאומי, לקבוע בתקנות, או בהוראות אחרות שהוא מוסמך לתת לפי דין, דרישות בעניין רמת הגנת הסייבר לארגונים חיוניים במגזר המשק ביחס אליו הוא הגורם המאסדר, שהן נוספות על הדרישות שבתוספת הרביעית.

באופן דומה, וביחס לגופים ממשלתיים, מוצע לקבוע בסעיף קטן (ד) שהשר האמון על מערך הדיגיטל הלאומי, יהיה מוסמך לקבוע, בהתייעצות עם ראש מערך הסייבר הלאומי, הוראות נוספות על הדרישות שבתוספת הרביעית לעניין רמת הגנת הסייבר של גופים אלה.

זאת ועוד, מתוך הראייה הלאומית המתכללת של מערך הסייבר הלאומי בתחום הגנת הסייבר, נוכח רמת האיומים הגבוהה במרחב הישראלי, בסעיף קטן (ה) מוצע לקבוע, שראש מערך הסייבר הלאומי באישור ראש הממשלה יהיה רשאי, בהתקיים סיכון סייבר משמעותי העלול לאפשר תקיפת סייבר חמורה נגד ארגונים חיוניים שונים באופן העלול ליצור סיכון משמעותי במשק, להורות לארגון חיוני, אחד או יותר, לנקוט אמצעים להתמודדות או מניעת הסיכון כאמור אם מצא כי ההוראה נדרשת באופן דחוף. סעיף זה נועד לאפשר לראש מערך הסייבר הלאומי, במקרים חריגים, לתת הוראות לארגונים חיוניים בכדי להתמודד באופן דחוף עם סיכוני סייבר משמעותיים, כדוגמת טיפול ארגונים חיוניים בפגיעויות חמורות העלולות להביא לסיכון משמעותי במשק. בכדי להבטיח שימוש מידתי ומאוזן בסמכות זו, מוצע לקבוע גדרים ברורים להפעלתה. בכלל האמור, מוצע לקבוע כי ההחלטה תתקבל על ידי ראש מערך הסייבר הלאומי באישור ראש הממשלה, וכן לקבוע כי הוראות דחופות למניעת סיכון כאמור, ינתנו רק לאחר שראש מערך הסייבר הלאומי שקל את השפעתן על פעילות הארגון החיוני ועל צד שלישי, לרבות הזכות לפרטיות, ואת העלות הכלכלית המועדכת של יישום הוראות והשפעתן האפשרית על הרציפות התפקודית של הארגון החיוני, למיטב ידיעתו ומצא כי אין בה לפגוע במידה העולה על הנדרש בנסיבות העניין. כן מוצע לקבוע שהוראות כאמור ייקבעו לתקופה שאינה עולה על 30 ימים וראש המערך יהיה רשאי להאריכה לתקופה אחת נוספת שאינה עולה על 30 ימים אם מצא שההוראה עדיין נדרשת מאותם נימוקים. עוד מוצע לקבוע שההוראה תועבר לארגונים החיוניים, ככל הניתן בנסיבות העניין באמצעות הרשות המוסמכת.

מוצע לקבוע שבמקרים בהם קיים צורך דחוף, בגינו לא ניתן לפנות תחילה לקבל אישור ראש הממשלה, יהיה רשאי ראש מערך הסייבר הלאומי לתת את ההוראה ולקבל את אישור ראש הממשלה עד 48 שעות לאחר שניתנה, ואולם אם לא ינתן אישור ראש הממשלה 48 שעות לאחר נתינתה, יראו את ההוראה כאילו לא ניתנה והארגון החיוני יעודכן על כך.

במסגרת עיגון חובת ארגון חיוני לעמוד ברמת הגנה נדרשת וכדי לאפשר בקרה על עמידה בחובה זו, מוצע לקבוע בסעיף קטן (ו) שעל ארגון חיוני תחול חובה לשמור מסמכים המעידים על עמידתו ברמת הגנה, בין בהתאם לתוספת הרביעית ובין בהתאם להוראות או תקנות נוספות שייקבעו בעניין.

בנוסף, מוצע להתוות את שיקול הדעת, ולקבוע בסעיף קטן (ז) שהוראות בהתאם לסעיפים 10(ב) עד 10(ד) כאמור,

יקבעו על בסיס כללים ואמות מידה מקצועיים, המיושמים במדינות מפותחות עם שווקים משמעותיים, אלא אם כן מתקיימות נסיבות המצדיקות אחרת, לרבות בשל מגבלות או חלופות מצומצמות למתן השירותים, צרכים תפעוליים ייחודיים, הערכת איומים וסיכונים לרבות היערכות למצב חירום או תנאי שוק יחודיים.

סעיף 11

כל אדם רשאי למסור הודעה למערך הסייבר הלאומי לעניין תקיפת סייבר.

באשר לתקיפות נגד ארגונים חיוניים או באמצעותם, קבלת דיווח מיידי על תקיפות משמעותיות נגד ארגונים אלה, היא חיונית לצורך מאמצי ההגנה על המשק. בשים לב לאמור מוצע לקבוע שארגון חיוני יהיה חייב למסור באופן מיידי דיווח על תקיפת סייבר משמעותית המתרחשת נגדו בפועל, למנהל בכיר במערך הסייבר הלאומי ולמנהל בכיר ברשות המוסמכת של מגזר המשק אליו משתייך הארגון החיוני. יובהר שבהתאם להסדר המוצע, הארגון החיוני יגיש דיווח אחד שיוגש במקביל לרשות המוסמכת ולמערך הסייבר הלאומי.

מוצע לקבוע כי תקיפה משמעותית בגינה תחול חובת הדיווח לפי סעיף זה היא תקיפה שמתקיים לגביה לפחות אחד מהבאים:

א. תקיפת הסייבר עלולה לפגוע באופן משמעותי בזמינות, רציפות או מהימנות השירות שהארגון החיוני מספק, לרבות בבטיחות של מערכת או תהליך חיוניים בארגון, בהתחשב בין השאר במספר או סוג המשתמשים בשירות, שעלולים להיות מושפעים מהתקיפה; סוג הפגיעה והיקפה; ומשך הפגיעה;

ב. תקיפת הסייבר עלולה להביא לפגיעה או גישה של גורם שאינו מורשה לנכס מידע משמעותי, ובכלל זה בדרך של פגיעה בתהליך הזדהות, שינויו, או הוצאה שלא כדין של מידע לרבות בדרך של העתקתו על ידי גורם כאמור;

ג. יש חשש ממשי שהתקיפה אינה מוגבלת לארגון הנתקף.

מוצע לקבוע שהדיווח המיידי לפי סעיף זה יכלול כל מידע שיש בו כדי לסייע להערכת חומרתה של תקיפת הסייבר והשלכותיה ובכל מקרה יכלול לכל הפחות את הפרטים שלהלן, ככל שהם ידועים לארגון:

(1) פרטי הארגון והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו, לרבות שם איש קשר בארגון, מספר טלפון, כתובת למשלוח הודעות וכתובת דואר אלקטרוני ומספר ח.פ. (אם קיים);

(2) מועד תחילת תקיפת הסייבר ומועד גילויה;

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

(4) מידע הנוגע לאפשרות שתקיפת הסייבר עלולה לפגוע ישירות ובאופן ממשי בארגון אחר.

יובהר, כי בעוד ההחלטה אם תקיפה היא "תקיפה חמורה" כהגדרתה בסעיף 14 המוצע, כרוכה בבחינת שיקולים שרק לרשות מנהלית יש את היכולת לשקול, הגדרת "תקיפה משמעותית" גובשה כך שארגון חיוני יוכל להפעיל את שיקול דעתו ולבחון האם מדובר בתקיפה משמעותית שחלה עליו חובה לדווח עליה בהתאם לסעיף זה. יצוין כי בכוונת מערך הסייבר הלאומי לפרסם גילוי דעת בדבר דוגמאות לתקיפות סייבר משמעותיות עליהן נדרש לדווח לפי סעיף זה.

בכדי להקל על ארגונים חיוניים, ולהבטיח שידרשו להגיש דיווח ראשוני אחד בלבד, מוצע לקבוע כי הדיווח יוגש למרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר (CERT) שמפעיל מערך הסייבר הלאומי, באופן מקוון באתר האינטרנט של מערך הסייבר הלאומי, בהודעה טלפונית למרכז הלאומי או בדרך אחרת שהורה עליה ראש מערך הסייבר הלאומי ופורסמה באתר האינטרנט של המערך, לאחר ההגשה, הדיווח יועבר לרשות המוסמכת באופן מקוון או על ידי מערך הסייבר הלאומי.

לצד זאת, בכדי לאפשר התאמה מירבית לאופן ההתנהלות של רשויות מוסמכות אל מול מגזר המשק הרלוונטי,

מוצע לקבוע שהגורם המסמיך יוכל לקבוע, לאחר יידוע של מערך הסייבר הלאומי, כי הדיווח יוגש בדרך אחרת לרשות המוסמכת ויועבר על ידה באופן מיידי למערך הסייבר הלאומי.

בנוסף, מוצע לקבוע שארגון חיוני ימסור למנהל בכיר במערך הסייבר הלאומי ולמנהל בכיר ברשות המוסמכת, בסמוך לאחר הטיפול בתקיפת הסייבר, דיווח מסכם, באותו אופן בו הגיש את הדיווח הראשוני. הדיווח המסכם יכלול תיאור מפורט על אודות תקיפת הסייבר, לרבות חומרתה והשלכותיה; סוג תקיפת הסייבר והגורמים שהיוו מקור להתרחשותה, למיטב ידיעתו של הארגון; אופן הטיפול בתקיפת הסייבר, לרבות פירוט בדבר האמצעים שננקטו או שעדיין ננקטים לשם כך, ולמעט סוד מסחרי הנוגע ישירות לאופן הטיפול בתקיפת הסייבר ולאמצעים כאמור. תכלית הדיווח המסכם היא לאפשר, בין השאר, למערך הסייבר הלאומי ולרשות המוסמכת לוודא שהאינטרסים הציבוריים שעלולים להפגע כתוצאה מתקיפת סייבר משמעותית מוגנים וכן להבטיח שמערך הסייבר הלאומי והרשות המוסמכת מחזיקים בתמונת מצב מלאה ככל האפשר של רמת ההגנה במשק ובמגזר לפי העניין.

סימן ג': סמכויות פיקוח

סעיף 12

מוצע לקבוע שלשם פיקוח על ביצוע הוראות 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 ביצועו של חוק זה או להקל על ביצועו. זאת לרבות לשם פיקוח על עמידת ארגון חיוני במגזר המשק ברמת ההגנה הנדרשת לפי סעיף 10 המוצע, לשם פיקוח על עמידת ארגון חיוני בחובת הדיווח על תקיפות סייבר משמעותית כמוצע בסעיף 11, או לשם בחינה האם ארגון הוא ארגון חיוני במגזר המשק לפי סעיף 8 המוצע.

סעיף 13

מוצע לקבוע שלשם פיקוח על עמידת ארגון חיוני ברמת ההגנה הקבועה בסעיף 10 המוצע ועל חובת הדיווח על תקיפה משמעותית לפי סעיף 11 המוצע, עובד מוסמך מגזרי יהיה רשאי להיכנס למקום, ובלבד שלא יכנס למקום המשמש למגורים, אלא על פי צו של בית משפט. יודגש, כי סמכות הכניסה למקום של העובד המגזרי אינה כוללת סמכות לבצע פעולות בחומר מחשב. בכדי להבטיח שימוש מידתי בסמכות, מוצע לקבוע שעובד מוסמך מגזרי לא יעשה שימוש בסמכויות הנתונות לו לפי סעיף זה, אלא בעת מילוי תפקידו וכשיש בידו תעודה החתומה בידי הגורם המסמיך, המעידה על תפקידו וסמכויותיו של העובד המוסמך המגזרי, שאותה יציג לפי דרישה. עם זאת, מוצע לקבוע שחובת ההזדהות האמורה לא תחול אם קיומה עלול לגרום לסיכול הכניסה למקום על ידי העובד המוסמך או אם קיומה עלול לפגוע בביטחון העובד המוסמך המגזרי או בביטחון אדם אחר. בחלוף הנסיבה כאמור בגינה לא קיים העובד המוסמך המגזרי את חובת ההזדהות, יזדהה העובד המוסמך בהתאם למפורט בסעיף, מוקדם ככל האפשר.

סימן ד': תקיפת סייבר חמורה

הכלל אותו מבקשת הצעת החוק לעגן, הוא חובת התמודדות ארגון עם תקיפת סייבר חמורה. במקביל, לשם הבטחת התמודדות הולמת עם תקיפות סייבר חמורות כלפי או באמצעות ארגון חיוני או ספק שירותים דיגיטליים ושירותי אחסון, בהתחשב בנזק הפוטנציאלי החמור שעלול להגרם כתוצאה מתקיפה כאמור, מוצע, לצד חובות הארגונים, להסדיר את הסמכויות והפעולות אשר יוקנו לגופי המדינה השונים כלפי אותם ארגונים, לצורך לאיתור, מניעה או בלימה של תקיפות חמורות.

יצוין כי סעיפים דומים במהותם נחקקו במסגרת חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים

הדיגטליים ושירותי האחסון (הוראת שעה), תשפ"ד-2023 (להלן: "הוראת השעה"), ביחס למגזר האמור, והובילו לשיפור ניכר בהגנת המשק הישראלי בסייבר. ההסדר המוצע מבקש בעיקרו לעגן הסדרים דומים הנדרשים ביחס למגזר השירותים הדיגטליים ושירותי האחסון וביחס לארגונים חיוניים השייכים לכלל מגזרי המשק בהתבסס, בין היתר, על הנסיון המצטבר ביישום הוראת השעה.

סעיף 14

מוצע לקבוע שתקיפת סייבר חמורה היא תקיפת סייבר שהיה למנהל בכיר ברשות מוסמכת חשש ממשי כי מתקיימים ביחס אליה אחד או יותר מהתנאים הבאים:

א. תקיפת הסייבר עלולה לפגוע ברציפות התפקודית של ארגון חיוני לרבות בבטיחות של מערכת או תהליך חיוניים בארגון;

ב. תקיפת הסייבר עלולה לפגוע בזמינות, רציפות או מהימנות השירות שארגון חיוני מספק;

ג. תקיפת הסייבר עלולה לאפשר גישה לגורם שאינו מורשה לנכס מידע משמעותי של הארגון החיוני;

ד. לתקיפת הסייבר בארגון חיוני מאפיינים (או שיש חשש קיומם של מאפיינים) המעידים על חומרה מיוחדת, לרבות מיתאר התקיפה או זהות התוקף;

ה. תקיפת הסייבר בארגון חיוני עלולה לפגוע בבטחון המדינה, בביטחון הציבור או לפגוע באופן חמור ברציפות אספקתם של שירותים חיוניים לציבור בשל מאפייני התקיפה (לרבות מתאר התקיפה או זהות התוקף) וקיומו של חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לארגון הנתקף.

בנוסף, מוצע לקבוע שאם למנהל בכיר ברשות מוסמכת היה יסוד סביר להניח כי תקיפת סייבר שמתרחשת או שקיים חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה נגד ארגון חיוני במגזר המשק או תקיפה כאמור הנעשית באמצעות הארגון החיוני, הוא יהיה רשאי, בעצמו או באמצעות עובד מוסמך מגזרי, לדרוש מהארגון החיוני להציג לו כל ידיעה או מסמך, לרבות פלט, הנדרשים בכדי להבטיח או להקל את ביצועו של סעיף זה לקביעה אם התקיפה האמורה היא תקיפה חמורה. יובהר, שפניית רשות מוסמכת לארגון לצורך דרישת ידיעות ומסמכים מכח סעיף זה, תבוצע באופן מצומצם והדרגתי ככל הניתן, בשים לב לנתונים הקיימים בידי הרשות ולמידע הנדרש לבחינת חומרת תקיפת הסייבר המסוימת. כך לדוגמא, ככל שלצורך החלטה אם התקיפה הנבחנת היא תקיפת סייבר חמורה, נדרש למנהל המוסמך מידע בנוגע לקישוריות הארגון לארגונים אחרים לצורך הערכת הסיכון הנגזר מן התקיפה, תתמקד דרישת המידע הראשונית במידע הנוגע לכך. עוד להמחשה, במקרה בו קיים ספק באשר למאפיינים הטכנולוגיים של התקיפה לשם הבנת חומרתה, תתמקד הפניה, ככל האפשר, בדרישה ממוקדת לקבלת המאפיינים הטכנולוגים הנדרשים לצורך הבחינה האמורה.

סעיף 15

סעיף זה נועד להסמיך עובד מוסמך מגזרי לפי התוספת הראשונה, לתת הוראות לארגון חיוני במגזרו להתמודדות עם תקיפת סייבר חמורה או חשש ממשי לה, בנסיבות בהן נמצא צורך לכך. מוצע לקבוע תנאים למתן הוראות מחייבות לארגון חיוני בנסיבות בהן הארגון אינו מתמודד באופן הולם עם חשש ממשי לתקיפת סייבר חמורה. תכלית הוראות אלה היא לוודא שהארגון החיוני פועל כנדרש לאיתור התקיפה, מניעתה או בלימתה וזאת בכדי לצמצם את נזקי התקיפה, ובכלל האמור כדי להגן על האינטרס הציבורי העלול להיפגע כתוצאה מתקיפת סייבר חמורה כנגד ארגון כאמור. כמו כן, הסעיף מבקש לקבוע הליך מנהלי סדור המגלם את האיזונים בין הצורך להגן מפני תקיפת הסייבר החמורה והאינטרס הציבורי לבין הצורך להגן על האינטרסים של הארגון ועל זכויות וצדדים שלישיים דוגמת עובדי הארגון, ובעלי עניין נוספים.

בהתאמה, מוצע לקבוע בסעיף קטן (א) שאם קבע מנהל בכיר ברשות מוסמכת שמתרחשת או עומדת להתרחש נגד או באמצעות ארגון חיוני, תקיפת סייבר חמורה הדורשת את מעורבותו, יודיע על כך עובד מוסמך מגזרי לארגון החיוני, לאחר שהזדהה בפניו, ויפרט בהודעתו לארגון החיוני את התשתית העובדתית והמקצועית לקביעה כאמור, ככל שאין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים. יובהר, כי לא בכל מצב בו מתקיימת תקיפה חמורה תידרש מעורבות הרשות המוסמכת, ובהתאם לא בכל מצב תימסר לארגון הודעה כאמור. הצפייה היא כי ארגון חיוני יתמודד עם תקיפות סייבר חמורות באופן הולם, ולכן למשל, במצב בו נהיר כי הארגון מודע לתקיפה ומתמודד עמה באופן הולם, לא בהכרח תימסר לארגון הודעה של העובד המוסמך המגזרי כאמור. לצד זאת, מסירת הודעה כאמור לארגון היא תנאי להפעלת הסמכויות לפי הסעיף המוצע.
עוד מוצע, כי לאחר מתן ההודעה לארגון החיוני שמתרחשת או שקיים חשש ממשי כי עומדת להתרחש תקיפת סייבר חמורה, נגד או באמצעות הארגון, תינתן לארגון החיוני הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה, לרבות מניעתה מבעוד מועד או מניעת הישנותה, או בלימתה לאחר שהחלה, והכל בתוך פרק זמן סביר שיימסר לארגון החיוני על ידי העובד המוסמך המגזרי, בהתחשב במאפייני תקיפת הסייבר החמורה.
בהמשך לכך מוצע לקבוע כי הארגון החיוני יידרש לעדכן את העובד המוסמך המגזרי בדבר הפעולות שביצע לצורך איתור התקיפה, מניעתה או בלימתה, בתוך פרק הזמן שהוגדר.

בהמשך לכך, מוצע שאם מצא העובד המוסמך כי הארגון החיוני הנתקף לא פעל באופן הולם לאיתור תקיפת הסייבר החמורה, מניעתה או בלימתה, יהיה רשאי העובד המוסמך להודיע לארגון החיוני על כוונתו לתת לו הוראות, ולארגון תינתן הזדמנות להשמיע את טענותיו לעניין הכוונה לתת לו הוראות מחייבות. יודגש, כי לא יינתנו הוראות מכוח סעיף קטן א(4) המוצע לארגון חיוני אשר טיפל באופן הולם באיתור התקיפה, מניעתה או בלימתה.

לאחר שמיעת טענות הארגון החיוני, אם לא השתכנע העובד המוסמך אחרת, יהיה רשאי, העובד המוסמך המגזרי בהתייעצות עם מערך הסייבר הלאומי, לתת לארגון הוראות, בכתב או בעל פה, ככל שהדבר חיוני לצורך איתור התקיפה, מניעתה או בלימתה. במסגרת סמכותו לפי סעיף זה, מוצע שהעובד המוסמך יהיה רשאי לתת לארגון החיוני, בין היתר, הוראות הנוגעות לחומר מחשב שיהיו פעולות להגנת סייבר בחומר מחשב, כלומר להורות לארגון לתת הוראות למחשב בשפת קריאת מחשב לשם הגנת סייבר. בכלל זה יהיה רשאי העובד המוסמך להורות לארגון החיוני לבצע סריקה, עיבוד, הסרה של חומר מחשב הנוגע לתקיפת סייבר, התקנת סוג תוכנה שפעולה מוגבלת לרשת הארגון בלבד, חסימה או ניתוק של מחשב או יצירת עותק של חומר מחשב. כמו כן, יכול העובד המוסמך המגזרי לתת סוגי הוראות נוספים מכח סעיף זה, ובכלל זה הוראות למסירת ידיעה או מסמך, לרבות עותק חומר מחשב הנדרש לאיתור, מניעת או בלימת תקיפת סייבר חמורה, לידי העובד המוסמך המגזרי.

יובהר, שבהתאם להנחיית היועצת המשפטית לממשלה מספר 1.2500 מיום 10 באוקטובר 2019 שכותרתה "כללים מנחים לגיבוש הסדרים דיגיטליים", לפיה "הסדר דיגיטלי לא יעדיף ככל הניתן אמצעי טכנולוגי אחד על פני אמצעי טכנולוגי אחר, אם שניהם מגשימים את השימושים והמטרות של אותו ההסדר", מוצע לקבוע שהעובד המוסמך יהיה רשאי להורות על התקנת סוג תוכנה ולא על התקנת תוכנה מסוימת, מקום בו יש יותר מתוכנה אחת המגשימה את אותם השימושים והמטרות. זאת ועוד, מתן הוראה מחייבת על ידי עובד מוסמך לפי חוק זה להתקנת תוכנה, תהיה לסוג תכנה שפעולתה מוגבלת לרשת הספק בלבד.

מוצע להתוות את שיקול הדעת של העובד המוסמך המגזרי ולקבוע שבמתן הוראות לפי סעיף זה הוא ישקול את

השפעתן האפשרית על פעילות הארגון החיוני ועל צד שלישי, לרבות הזכות לפרטיות ובכלל זה מידע על לקוחות ועובדים, וכן את העלות הכלכלית המוערכת של יישום ההוראות ואת השפעתן האפשרית על הרציפות התפקודית של הארגון החיוני, למיטב ידיעתו של העובד המוסמך המגזרי או בהתחשב בהערכה שמסר הארגון לעניין זה, אם מסר.
כמו כן, מוצע להדגיש את חובת העובד המוסמך לפעול במידתיות ולקבוע שהוא יורה לנקוט באמצעי שפגיעתו פחותה לצורך איתור התקיפה, מניעתה או בלימתה. יובהר בהקשר זה שבמרבית המקרים, המידע המתקבל בהקשר הגנת סייבר הוא מידע טכנולוגי שאינו מכיל מידע אישי.
בנוסף, מוצע לקבוע שבעת מתן ההוראה, העובד המוסמך המגזרי יפרט את המועד האחרון לביצועה ועד למועד זה הארגון יפעל בהתאם להוראה שקיבל וידווח על אופן ביצועה לעובד המוסמך המגזרי.

בנוסף, לנוכח הצורך למנוע התפשטות תקיפות סייבר חמורות וצמצום השלכותיהן, מוצע לקבוע בסעיף קטן (ב) כי אם מסר עובד מוסמך מגזרי לארגון חיוני הודעה על קיומה של תקיפה חמורה בהתאם לסעיף קטן (א), ימסור הארגון בלא דיחוי עדכון בדבר תקיפת הסייבר החמורה לכל ארגון העלול להפגע מהתקיפה ישירות ובאופן ממשי, וידווח על כך בכתב לעובד המוסמך המגזרי. הכל אלא אם כן הורה העובד המוסמך המגזרי, בהתייעצות עם מערך הסייבר הלאומי, אחרת. כמו כן, בהתקיימן של נסיבות חריגות המצדיקות זאת, מוצע לקבוע שמנהל בכיר ברשות מוסמכת יהיה רשאי, לפי בקשה בכתב מאת ארגון חיוני, בהתייעצות עם מערך הסייבר הלאומי, לפטור את הארגון החיוני מחובת יידוע ארגונים העלולים להפגע כאמור, או לדחות את מועד היידוע.

סעיף 16

לעניין תקיפה חמורה נגד או באמצעות גוף ממשלתי כהגדרתו בחוק, מוצע לקבוע באופן דומה להסדר ביחס לארגונים חיוניים שאינם גופים ממשלתיים, שאם מנהל בכיר במערך הדיגיטל מצא שמתרחשת או עומדת להתרחש נגד או באמצעות ארגון חיוני שהוא גוף ממשלתי תקיפת סייבר חמורה הדורשת את מעורבותו והודיע על כך לגוף הממשלתי, רשאי עובד מוסמך מגזרי, לאחר שהודיע על כך לגוף, לתת לו הוראות, בהתייעצות עם מערך הסייבר הלאומי, בכתב או בעל פה והגוף הממשלתי יפעל בהתאם להוראות שינתנו כאמור. כן מוצע, להתוות את שיקול הדעת של העובד המוסמך המגזרי ולקבוע כי במתן הוראות ישקול את השפעתן האפשרית על פעילות הגוף הממשלתי ועל צד שלישי, לרבות הזכות לפרטיות, ויורה לנקוט באמצעי שפגיעתו פחותה לאיתור התקיפה, מניעתה או בלימתה. יובהר שביחס לגופים ממשלתיים, בסעיף 15 לא מוצע לקבע את המדרג המוצע טרם מתן הוראות ביחס לארגונים חיוניים שאינם ממשלתיים. זאת בשל אופיים הייחודי של גופים ממשלתיים והציפייה המוגברת מהם לפעול באופן מיידי לטיפול בתקיפות סייבר חמורות בהתאם להנחיות הרשות המוסמכת.

סעיף 17

כמפורט לעיל, הכלל אותו מבקשת הצעת החוק לעגן, הוא התמודדות הארגון החיוני עם תקיפה חמורה, וזאת במידת הנדרש בליווי היחידה המגזרית ברשות המוסמכת הרלוונטית. במקביל, בשים לב לכך שמערך הסייבר הלאומי הוא הגוף הלאומי בעל ראיית הרוחב והמחזיק בכלים נוספים להתמודדות, נקודת המוצא היא כי בראייה לאומית בנסיבות מסוימות נדרשת מעורבות ישירה של מערך הסייבר הלאומי בליווי ההתמודדות עם תקיפות חמורות. בשים לב לאמור, מוצע לקבוע בסעיף זה את הנסיבות בהן תידרש התערבות המערך בהקשר זה.
בסעיף קטן (א) מוצע לקבוע כי למנהל בכיר במערך הסייבר הלאומי יהיו נתונות הסמכויות לקבוע כי תקיפת סייבר היא תקיפה חמורה בהתאם לסעיף 14 המוצע, וכי עובד מוסמך במערך הסייבר הלאומי יוכל לנקוט בפעולות לפי סעיפים 15 ו-16 המוצעים לפי העניין, לרבות מתן הוראות להתמודדות עם תקיפת סייבר חמורה הן ביחס לארגון

חיוני בנסיבות הקבועות בסעיף, והן ביחס לספק שירותים דיגיטליים ושירותי אחסון. ביחס לספק שירותים דיגטליים או שירותי אחסון מוצע כי הסמכות למתן הוראות להתמודדות עם תקיפת סייבר חמורה, תחול באופן כולל ולא רק ביחס לארגונים חיוניים במגזר זה. הצעה זו נדרשת בשל המאפיינים היחודיים של מגזר משק זה, החיבוריות הגבוהה של ספקי שירותי אחסון וספקי שירותים דיגיטליים העלולה להיות מנוצלת על ידי תוקפים לגרימת נזק רחב היקף, ופוטנציאל הנזק למשק הגלום בתקיפת סייבר חמורה נגד ארגונים במגזר זה גם אם אינם ארגונים חיוניים. יודגש כי בהוראת השעה מוקנית סמכות זו למערך הסייבר הלאומי ביחס למגזר האמור, והנסיון מיישום הוראת השעה מלמד כי הסמכות חיונית להגנת הסייבר במגזר משק זה נוכח המאפיינים המתוארים לעיל. ביחס לארגון חיוני שאינו שייך למגזר אשר מערך הסייבר הלאומי הוא הרשות המוסמכת ביחס אליו, מוצע לקבוע בסעיף קטן (ב) שעובד מוסמך במערך הסייבר הלאומי ינקוט בפעולות לפי סעיפים 15 ו-16 המוצעים רק בנסיבות המפורטות בו, היינו:

-אם קבע ראש מערך הסייבר הלאומי שיש מקום להיענות לבקשת רשות מוסמכת לסיוע בהפעלת סמכויותיה כלפי ארגון חיוני לפי סעיפים 15 או 16 המוצעים. בקשה זו עשויה לנבוע, למשל, מהצורך להסתייע ביכולות שמצויות בידי מערך הסייבר הלאומי ולא בידי הרשות המוסמכת.

-בנסיבות בהן קבע ראש המערך שקיים חשש כי תקיפת סייבר חמורה תתפשט במהירות לארגונים רבים, תתפשט ליותר ממגזר משק אחד או תפגע בבטחון המדינה או בבטחון הציבור. מדובר בנסיבות בהן נדרשת מעורבות ישירה של מערך הסייבר הלאומי בליווי הלאומי של ההתמודדות עם תקיפות חמורות נגד ארגונים חיוניים.

במקביל, כדי להבטיח תיאום וסנכרון למול הארגון החיוני, מוצע לקבוע בסעיף קטן (ג) כי משהחליט מנהל בכיר במערך הסייבר הלאומי על הפעלת סמכות לעניין ארגון חיוני בהתאם לסעיף קטן (ב) המוצע, יידע בעניין את הרשות המוסמכת, והסמכויות לעניין תקיפת הסייבר נגד הארגון החיוני יופעלו בהוראת עובד מוסמך של מערך הסייבר הלאומי בלבד, וזאת ככל הניתן בנסיבות העניין, באמצעות הרשות המוסמכת.

סעיף 18

מוצע לקבוע בסעיף קטן (א) שסמכות מנהל בכיר להכריז על תקיפת סייבר חמורה בהתאם לסעיף 14 המוצע, תהיה נתונה גם לראש חטיבת ההגנה בסייבר בצה"ל, וזאת ביחס לתקיפת סייבר חמורה שהוא מצא שמתרחשת או שקיים חשש ממשי שהיא עומדת להתרחש כנגד ארגון חיוני, כנגד ארגון חיוני למערכת הביטחון או כנגד ספק שירותים דיגיטליים או שירותי אחסון, אם מצא כי יש חשש ממשי שיש בה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל בשל הנסיבות המפורטות בסעיף 14 המוצע.

עוד מוצע לקבוע בסעיף קטן (ב) שאם קבע ראש חטיבת ההגנה בצה"ל שמתקיימת תקיפת סייבר חמורה כאמור בסעיף קטן (א), יראו את הקביעה כקביעת מנהל בכיר במערך הסייבר הלאומי, ולעניין ארגון חיוני למערכת הביטחון כקביעת מנהל בכיר במלמ"ב.

סימן ה': ארגון חיוני למערכת הביטחון

סעיף 19

מוצע לקבוע הגדרות שישמשו בסימן זה.

במסגרת כך מוצע לקבוע שגוף מונחה מלמ"ב יהיה גוף המנוי בפרטים 2 ו-3 לתוספת הראשונה לחוק הסדרת הבטחון בגופים ציבורים. בנוסף, מוצע להגדיר בסימן זה "מערכת הביטחון" ככוללת את צה"ל, משרד הביטחון, מלמ"ב וגופים מונחי מלמ"ב לפי חוק הסדרת הבטחון בגופים ציבוריים.

סעיף 20

מוצע לקבוע בסעיף קטן (א) ששר הביטחון, לפי המלצת ראש מלמ"ב, רשאי לקבוע שארגון הוא ארגון חיוני למערכת הביטחון, אם מצא כי הארגון מנוי ברשימת הספקים של מערכת הביטחון ובלבד שהארגון אינו גוף מונחה, וכן מצא שהארגון מספק למערכת הביטחון מוצרים, שירותים או טכנולוגיות וכן מספק או מחזיק ידע, שהם חיוניים לפעילות ביטחונית או מבצעית של מערכת הביטחון, אשר פגיעה בזמינותם ותפקודם עקב תקיפת סייבר עלולה לגרום לפגיעה משמעותית בביטחון המדינה או ברציפות התפקוד של מערכת הביטחון.
בנוסף, מוצע לקבוע שאם הארגון הוא ארגון חיוני בהתאם לסעיף 8 המוצע, יקבע שר הביטחון שארגון הוא חיוני למערכת הביטחון רק בהסכמת הגורם המאסדר באותו מגזר משק, וזאת בתנאי שמצא, כי אין די בהגדרת הארגון כארגון חיוני לצורך מענה לסיכון האמור לפגיעה המשמעותית בביטחון המדינה או ברציפות התפקוד של מערכת הביטחון. כמו כן, מוצע לקבוע כי החלטת שר הביטחון תינתן רק לאחר שניתנה לארגון הזדמנות להשמיע טענותיו לעניין זה. בנוסף, כדי להבטיח שהגדרת ארגון כארגון חיוני למערכת הביטחון תתבצע לאחר שיישקלו שיקולים רוחביים הקשורים בהגנת הסייבר הלאומית, מוצע לקבוע בסעיף קטן (ב) שהמלצת ראש מלמ"ב לפי סעיף קטן (א) המוצע, תינתן לאחר שקיים התייעצות עם הרמכ"ל וכן לאחר שקיבל את הסכמת ראש מערך הסייבר הלאומי.
מוצע לקבוע כי אם לא נתן ראש מערך הסייבר הלאומי הסכמתו לקביעה שארגון הוא ארגון חיוני למערכת הביטחון, רשאי יהיה ראש מלמ"ב להביא את הסוגייה להכרעה בפני ראש המטה לביטחון לאומי.
כמו כן, מוצע לקבוע בסעיף קטן (ג) תהליך יידוע לפיו, אם קבע שר הביטחון לפי סעיף זה, שארגון הוא ארגון חיוני למערכת הביטחון או קבע שאין עוד צורך בהגדרת ארגון כארגון חיוני למערכת הביטחון, יודיע על כך לארגון ויידע בכך את מערך הסייבר הלאומי, צה"ל וגורם מאסדר עימו התייעץ לפי סעיף זה ככל שהיה כזה, בתוך 14 ימים. קביעת שר הביטחון תיכנס לתוקף במועד מסירת ההודעה על הקביעה לארגון. בסעיף קטן (ד) מוצע לקבוע שרשימת הארגונים החיוניים למערכת הביטחון לא תפורסם לציבור. בסעיף קטן (ה) מוצע לקבוע שאם נקבע ארגון כארגון חיוני למערכת הביטחון, לא יוגדר כארגון חיוני לפי סעיף 8 לחוק עם קביעת שר הביטחון וכל עוד לא בוטלה.

סעיף 21

מוצע לקבוע בסעיף קטן (א) שסמכות הנתונה לפי חוק זה לגורם מסמיך ברשות מוסמכת, למנהל בכיר ברשות מוסמכת, לעובד מוסמך מגזרי ולממונה, תהיה נתונה בהתאם לעובדי מלמ"ב, בשינויים המחוייבים, כלפי ארגון חיוני למערכת הביטחון. בסעיף קטן (ב) מוצע לקבוע שסמכות הנתונה לפי חוק זה לגורם מאסדר תהיה נתונה לשר הביטחון כלפי ארגון חיוני למערכת הביטחון.

סעיף 22

מוצע לקבוע שארגון שנקבע כארגון חיוני למערכת הביטחון, יחולו לגביו הוראות החוק החלות על ארגון חיוני בהתאמות הנדרשות, למעט הוראות סעיף 17 המוצע. עם זאת החובה החלה על ארגונים חיוניים מכח חוק זה לעמוד בדרישות רמת ההגנה הבסיסית המנויות בתוספת הרביעית, תחול על ארגון חיוני למערכת הבטחון בתום 6 חודשים ממועד הקביעה כי ארגון הוא ארגון חיוני למערכת הבטחון.

פרק ה': עיצום כספי

סימן א': עיצום כספי

בכדי לתמרץ את הארגונים החיוניים ואת ספקי שירותים דיגיטליים ושירותי אחסון לציית לחובות הקבועות בחוק זה, שאי הציות להן עלול להוביל לפגיעה באינטרסים ציבוריים דוגמת בטחון המדינה, בטחון הציבור ולפגיעה חמורה ברציפות אספקת שירותים חיוניים לציבור, מוצע לקבוע בפרק זה את סמכות הרשויות המוסמכות להטיל עיצומים כלפי ארגון בעקבות הפרה של חובות מרכזיות בחוק, כפי שיפורט להלן.

סעיף 23

מוצע להגדיר את "הממונה" בסעיף 1 המוצע, כעובד בכיר ברשות מוסמכת אשר דרגתו ראש אגף לפחות ושהוסמך על ידי הגורם המסמיך להטיל עיצומים לפי חוק זה. הממונה יהיה במידת האפשר אותו גורם שכבר מוסמך להטיל עיצומים ברשות המוסמכת מכח דינים אחרים, ככל שיש כזה. תכליתה של הסנקציה המינהלית היא תכלית הרתעתית־מניעתית. גובה הסכום של העיצום הכספי נועד למנוע את התמריץ הכלכלי להפר את החוק, קרי לנטרל את קיומה של "ההפרה היעילה". במקביל, גובה הסכום של העיצום הכספי נקבע כך שיהיה מידתי ולא יסכן את המשך פעילותו הכלכלית של המפר, שכן מטרת הסנקציה המינהלית היא החזרת המפוקח למשטר ציות ולא לגרום בפועל להפסקת פעילותו.

מוצע לקבוע שהממונה יהיה רשאי להטיל עיצום כספי על ארגון חיוני, למעט ארגון חיוני שהוא גוף ממשלתי או רשות מקומית, וכן בהיבטים מסוימים להטיל עיצום כספי על ספק שירותים דיגיטליים ושירותי אחסון גם אם אינו ארגון חיוני, כמפורט להלן:

א. הטלת עיצום בגין הפרת דרישות רמת ההגנה המחייבות ארגון חיוני לפי סעיף 10(ב), המנויות בתוספת הרביעית. ביחס לכל דרישה שהופרה, ניתן יהיה להטיל עיצום בסכום הקבוע בטור ב' בתוספת השישית.

ב. הטלת עיצום בסך 300,000 ₪ בגין הפרת הוראה מקצועית שניתנה על ידי ראש מערך הסייבר הלאומי לפי סעיף 10(ה);

ג. הטלת עיצום בסך 300,000 ₪ בגין הפרת החובה למסור לעובד מוסמך מגזרי בכתב מידע או מסמך שהיה עליו לשמור בהתאם להוראות סעיף 10(ו) המוצע, לפי דרישה שנמסרה לארגון בכתב, במועד או באופן שנקבעו בדרישה, וזאת בניגוד להוראות לפי סעיף 12 המוצע.

ד. הטלת עיצום בסך 300,000 ₪ בגין הפרת חובת הדיווח על תקיפת סייבר שחלה על ארגון חיוני לפי סעיפים קטנים 11(א) עד 11(ג) המוצעים , או אי מסירת דיווח מסכם בהתאם לחובה המוצעת בסעיף 11(ד).

ה. הטלת עיצום בסך 300,000 ₪ בגין הפרת הוראה להתמודדות עם תקיפת סייבר חמורה שניתנה לפי סעיפים 15(א)(4) או 17 המוצעים, שניתנה בכתב, הנדרשת לשם איתור תקיפת סייבר חמורה, מניעתה או בלימתה. עוד מוצע, שעיצום בגין הפרת הוראה כאמור יוכל להיות מוטל על כל ארגון במגזר השירותים הדיגיטליים ושירותי האחסון ולא רק על ארגונים חיוניים במגזר זה. זאת, מפני שסמכות מתן ההוראות להתמודדות עם תקיפות חמורות חלה כלפי כלל הארגונים במגזר האמור כלפי כלל הארגונים בו בשל מאפייניו היחודיים, בדגש על החיבוריות הגבוהה של ארגונים בו לארגונים רבים במשק.

לחלק מהרשויות המוסמכות קיימת כיום סמכות להטיל עיצומים גם מכוח חקיקה אחרת במסגרת הרגולציה שמתבצעת על ידם במגזר המשק. בכדי לייצר וודאות למשק ולמנוע כפל ענישה, מוצע לקבוע בסעיף קטן (ד) שעל מעשה אחד המהווה הפרה של הוראות לפי חוק זה וכן מהווה הפרה לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד.

סעיפים 24-26

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

בסעיף 24 המוצע, מעוגן השלב הראשון בהפעלת הסמכות כלפי ארגון לפי סעיף 23 המוצע. מוצע כי כאשר יש יסוד

סביר להניח כי ארגון הפר את הוראות החוק וקיימת כוונה להטיל עיצום כספי, תשלח הודעה על כוונת חיוב על-ידי הממונה. מטרת הודעה זו להבהיר לארגון מה המעשה או המחדל המהווה את ההפרה, מה סכום העיצום הכספי שצפוי להיות מוטל על המפר בשל ביצוע ההפרה האמורה ומה התקופה שבה נדרש לשלם. כן מוצע שבהודעה תצויין זכותו של המפר לטעון את טענותיו בפני הממונה.

בסעיף 25 המוצע מעוגנת זכות הטיעון של הארגון לפני הממונה, כמקובל בהליך מינהלי. לפי אותו סעיף, מוצע שמפר שנמסרה לו הודעה על כוונת חיוב כאמור, יהיה רשאי לטעון את טענותיו בכתב לפני הממונה, הן לעניין הכוונה 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 בת 30 ימים.

בסעיף 26 מוצע לקבוע כי רק לאחר ששקל הממונה את טענות הארגון לפי סעיף 25 המוצע, יחליט אם יש להטיל עיצום כספי ומה גובהו. החליט הממונה להטיל עיצום כספי, ישלח לארגון דרישת תשלום 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, 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 27

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

סעיפים 28-33

בסעיף 28, 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 שבשלם ניתן יהיה להטיל עיצום כספי בסכום הנמוך מהסכומים המוצעים בסעיף 23 ובתוספת החמישית, ובשיעורים שיקבע. הממונה לא יהיה רשאי להטיל עיצום כספי בסכום נמוך מהסכומים המוצעים בסעיף 23, אלא לפי הוראות תקנות ההפחתה האמורות. בתקנות ההפחתה, רשאי הגורם המאסדר להביא בחשבון נסיבות ושיקולים 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 באמצעים למניעת הישנות ההפרה או לתקן את הנזקים שנגרמו בשלה. כמו כן, במסגרת תקנות ההפחתה ראוי אף להתחשב במחזור עסקאותיו של הארגון, ככל שמידע אודותיו נמסר לממונה על ידי הארגון, ולהפחית את סכום העיצום הכספי במקרים שבהם קיים חשש להמשך פעילותו הכלכלית של הארגון. זאת, מאחר שמטרת העיצום הכספי, כאמור, היא להשיב את הארגון למשטר ציות מבלי לסכן את המשך רציפותו התפקודית.
בסעיף 29 מוצע לקבוע את מנגנון ההצמדה של סכום העיצום הכספי.

בסעיף 30, מוצע לקבוע שארגון ישלם את העיצום הכספי בתוך 30 ימים מיום מסירת דרישת התשלום כאמור בסעיף 26. עוד מוצע בסעיף 31 לקבוע, שאם לא שילם ארגון עיצום כספי במועד, יתווספו על העיצום הכספי, לתקופת הפיגור, הפרשי הצמדה וריבית כהגדרתם בחוק פסיקת ריבית והצמדה, תשכ"א-1961, עד לתשלומו.
בסעיף 32 מוצע לקבוע את סמכות הממונה לפרוס את התשלום על העיצום הכספי בהתחשב בסכומו ובנסיבות מיוחדות אחרות שיצדיקו פריסה כאמור.
בנוסף, בסעיף 33 מוצע לקבוע, כי עיצום כספי ייגבה לאוצר המדינה ועל גבייתו יחול חוק המרכז לגביית קנסות, אגרות והוצאות, התשנ"ה-1995.

סימן ב': התראה מנהלית

סעיף 34

סעיף מוצע זה מעגן את האפשרות לעשות שימוש בכלי אכיפתי נוסף - ההתראה המינהלית. זהו כלי אכיפה המקל עם הארגון, 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, למרות 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 המשק 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.

סעיפים 35-36

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 35 מוצע לאפשר לארגון החיוני לתקוף את החלטת הממונה באמצעות הגשת בקשה לביטול ההתראה בשל אחד מהטעמים האלה:
א. הארגון לא הפר את הוראות חוק זה כאמור בהתראה המנהלית.
ב. המעשה שביצע הארגון, המפורט בהתראה, לא מהווה הפרה של הוראות חוק זה.
מוצע לקבוע בסעיף קטן (ג) שבהמשך להגשת הבקשה, הממונה רשאי לבטל את ההתראה או לדחות את הבקשה ולהותיר את ההתראה על כנה. החלטת הממונה תינתן למפוקח בכתב בצירוף נימוקי ההחלטה .
יובהר, כי אם הארגון לא הגיש בקשה לביטול ההתראה לפי סעיף זה בתוך 30 ימים מקבלת התראה מנהלית, 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.
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 24 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.

בנוסף, מוצע לקבוע כי אם נמסרה למפר התראה מנהלית 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 24, 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 24, בשינויים המחויבים.

סימן ג': שונות

סעיפים 37-38

מוצע לקבוע בסעיף 37 שעל מעשה אחד המהווה הפרה של הוראות החוק פי ההפרות המנויות בסעיף 23 המוצע, אשר מהווה הפרה גם לפי חוק אחר, לא יוטל יותר מעיצום כספי אחד, וזאת כדי ליצור וודאות וסופיות דיונית, בייחוד ביחס לארגונים שהרשות המוסמכת ביחס למגזר המשק אליו הם משתייכים מוסמכת להטיל עיצומים גם מכח חוקים אחרים.

כן מוצע להבהיר בסעיף 38 שאין בהגשת עתירה לבית משפט לעניינים מינהליים על החלטת הממונה, כדי לעכב את ביצוע החלטתו, אלא אם כן הסכים לכך הממונה, או שבית המשפט שאליו הוגשה העתירה הורה על כך.

סעיף 39

בסעיף 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 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.

בסעיף קטן (ב) מוצע לקבוע כי אם הוגשה עתירה לבתי משפט לעניינים מנהליים 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.

בסעיף 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. הממונה 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. בנוסף, על אף חשיבותו של הפרסום כמפורט לעיל, הרי שכדי למנוע פגיעה מעבר לנדרש בארגון כתוצאה מהפרסום האמור, מוצע להגביל את תקופת הפרסום לארבע שנים.

סעיף 40

מוצע לקבוע בסעיף קטן (א) שתשלום עיצום כספי או מסירת התראה מנהלית, לא יגרעו מאחריותו הפלילית של אדם (לרבות ארגון) בשל הפרת הוראה מהוראות לפי חוק זה, לפי פרק ז'. עם זאת, מוצע לקבוע בסעיף קטן (ב) 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. כמו כן, הוגש נגד אדם (לרבות ארגון) כתב אישום בשל עבירה המהווה הפרה, לא ינקוט נגדו הממונה הליכים לפי פרק זה בשל ההפרה.

סעיף 41

בסעיף קטן (א) מוצע לקבוע שגורם מאסדר אשר קבע תקנות לעניין דרישות רמת הגנה נוספות בהתאם לסעיף 10(ג), רשאי, בהתייעצות עם ראש מערך הסייבר הלאומי, בהסכמת שר המשפטים ובאישור ועדת החוץ והביטחון בכנסת, להוסיף הפרות נוספות לתוספת החמישית ביחס למגזרו, שביחס אליהן יוטל עיצום כספי, ובלבד שסכום העיצום הכספי שיקבע בטור ב' לתוספת ביחס להפרות שהוסיף לא יעלה על 640,000 ₪.

פרק ו': סיוע להגנת סייבר

סעיף 42

מערך הסייבר הלאומי מסייע בהקשרים ובתנאים שונים לאנשים ולגופים במשק 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, להגדיר את התנאים הנדרשים למתן סיוע של עובד מערך הסייבר הלאומי או מי מטעמו, להגנת סייבר לארגון המעוניין בכך, בעקבות פניית מערך הסייבר הלאומי לארגון או לבקשת הארגון, ככל שבמסגרת סיוע זה עלול מערך הסייבר הלאומי להחשף למידע אישי. לשם הבהירות, יודגש שבמרבית המקרים, פעולות הסיוע של מערך הסייבר הלאומי אינן כרוכות בקבלת מידע אישי, וכן גם במקרים בהם עלול מערך הסייבר הלאומי להיחשף למידע אישי אגב מתן סיוע, מדובר בתוצר נלווה לפעולת הסיוע ולא במטרתה. עוד יובהר, כי אין בהוראות סעיף מוצע זה כדי להגביל מתן סיוע בנסיבות אחרות, אם אותו סיוע אינו כרוך בחשיפה למידע אישי. עוד יובהר, שמתן הסיוע כרוך בהשקעת משאבים ציבוריים ועל כן מתן הסיוע האמור בסעיף לא יינתן לכל ארגון אלא יתבצע בכפוף לשיקול דעת מערך הסייבר הלאומי. כמו כן, מוצע לקבוע שמתן סיוע בהגנת הסייבר לפי סעיף זה לארגון במגזר המשק המנוי בחוק על ידי מערך הסייבר הלאומי יבוצע לאחר התייעצות עם הרשות המוסמכת לגבי עצם מתן הסיוע.

מוצע להגדיר "סיוע בהגנת סייבר" לעניין סעיף זה כפעולות לצורך סיוע במניעת, איתור או התמודדות עם תקיפת סייבר, לרבות פעולות הכרוכות בקבלת מידע בעל ערך הגנתי באופן חד פעמי או רציף, או בקבלת גישה למחשב או לחומר מחשב; יובהר שסיוע בהגנת סייבר אפשר שיינתן לא רק במסגרת התמודדות עם תקיפת סייבר פעילה אלא גם לשם מניעתה, לרבות סיוע בפעולות העלאת חוסן בשגרה.

עוד מוצע להגדיר שארגון אשר לו יוכל מערך הסייבר הלאומי לתת סיוע בהגנת סייבר הכרוך בקבלת מידע אישי לפי סעיף זה, יהיה ארגון אשר ראש מערך הסייבר הלאומי קבע כי קיים אינטרס לאומי בסיוע לו לפי סעיף זה, או ארגון שמנהל בכיר במערך הסייבר הלאומי קבע כי קיים אינטרס לאומי לסייע לו לפי סעיף זה אגב תקיפת סייבר נגדו או באמצעותו. לגבי גופים ממשלתיים, יובהר כי המגבלות המוצעות בסעיף לא יחולו ביחס אליהם, מאחר ומדובר בפעילות משולבת של מערך הסייבר הלאומי עם גוף ממשלתי אחר.

מוצע לקבוע שבמסגרת סיוע בהגנת סייבר של מערך הסייבר הלאומי העלול להיות כרוך בקבלת מידע אישי, לארגון המעוניין בכך, רשאי עובד המערך לבצע פעולות סיוע הכרוכות בקבלת מידע אישי, בהתאם להוראות הסעיף, ובכלל

האמור לאחר שהוסברו לנציג הארגון הטעם המקצועי לסיוע, הפעולות שיתבצעו כחלק מהסיוע וזכותו של הארגון שלא להסכים לקבל סיוע. כמו כן, 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 בתוך זמן קצר מהודעתו ובהקדם האפשרי.

כדי לצמצם את הפגיעה האפשרית בזכויות מוצע לקבוע שסיוע לפי סעיף זה יינתן לארגון רק אם לארגון יש מדיניות בנוגע לגישה ועיבוד מידע אישי במסגרתה הובהרה האפשרות להעביר מידע אישי לצרכי הגנת הסייבר. אולם, אם נדרש סיוע דחוף לארגון שאין לו מדיניות כאמור, ניתן לתת סיוע אם הארגון התחייב ליידע את עובדיו בדבר קבלת הסיוע בהגנת סייבר כאמור, וכן התחייב לפרסם מדיניות כאמור סמוך ככל הניתן לאחר קבלת הסיוע. 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 להגנת סייבר שאינה במוקד הסיוע להגנת סייבר, בכדי להבטיח הגנה מירבית על הזכות לפרטיות, מוצע לקבוע שלא יעובד מידע אישי בהתאם לסעיף זה אלא במידה הנדרשת לשם ביצוע 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 זה שימוש בטכנולוגיות ובשיטות פעולה באופן שיצמצם ככל האפשר את חשיפתו למידע אישי. בכלל האמור, מידע העלול לכלול מידע אישי לא יעובד על ידי אדם אלא אם קבע מנהל מוסמך כי אופי פעולת הסיוע מחייב עיבוד על ידי אדם, ובכלל זה אם קיים חשש לתקיפת סייבר אשר המידע נדרש לבחינתה, או אם נדרש לבצע מבדק חדירות למערכות הארגון. עיבוד על ידי אדם במקרים כאמור יבוצע על ידי מורשי גישה בלבד אשר עברו הכשרה לעניין הגנה על מידע אישי כפי שיקבע ראש מערך הסייבר הלאומי, ויתועד באופן שיאפשר פיקוח ובקרה על אופן ביצועה, על מועד ביצועה ועל זהות מבצע הפעולה. התיעוד האמור יישמר לשלוש שנים לפחות על ידי מערך הסייבר הלאומי.

עוד מוצע שככלל, פעולה בחומר מחשב במסגרת סיוע וולנטרי לפי סעיף זה, למעט פעולה בהעתק חומר מחשב שנמסר למערך הסייבר הלאומי, תתבצע על ידי נציג הארגון. 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 במסגרת האיזונים הקבועים בסעיף זה, אפשר שפעולה בהעתק חומר מחשב כאמור תתבצע על ידי עובד במערך הסייבר הלאומי. פעולת סיוע להגנת סייבר בחומר מחשב לפי סעיף זה, תתבצע על ידי מערך הסייבר הלאומי רק מטעמים מיוחדים ובאישור ראש מערך הסייבר הלאומי, לבקשת הארגון בכתב ובנוכחות נציג הארגון.

להשלמת התמונה, מוצע להבהיר שארגון יוכל למסור מידע העלול לכלול מידע אישי במסגרת קבלת סיוע לפי סעיף זה והדבר לא יחשב לפגיעה בפרטיות לפי חוק הגנת הפרטיות.

בנוסף, מוצע שרשות מוסמכת תוכל לתת סיוע בהתאם להוראות, לאיזונים ולבלמים שנקבעו בסעיף זה, לשם הפעלת מרכז שליטה ובקרה ענפי (SOC), כחלק מגיבוש תמונת מצב שוטפת בהיבטי הגנת הסייבר והטיפול באירועי סייבר במגזר. יובהר שמשרדי הממשלה רשאים להפעיל SOC ממשלתי במסגרת תנאי ההעסקה של עובדי המדינה ואין בסעיף זה כדי לפגוע או להשפיע על כך.

סעיף 43

מוצע לעגן את פעילות מערך הסייבר הלאומי, לאיתור פגיעויות חמורות המוכרות למערך הסייבר, ולמתן התרעה עליהן. פעילות כאמור תתבצע בהתאם לשיקול דעתו של המערך. בהקשר זה, מוצע להתוות את שיקול דעת עובד מערך הסייבר ולקבוע שפעילות עובד המערך לאיתור פגיעויות כאמור, תתבצע במטרה לאתר את הפגיעויות בארגונים, באופן שאינו מאפשר גישה למערכות מחשוב שיש הגבלה על נגישותן לציבור מרשת האינטרנט או מרשת ציבורית אחרת, באופן שלא צפויה להיות לו השפעה משמעותית על תפקוד מחשב שביחס אליו מאותרת הפגיעות

החמורה ותוך מיקוד במידע הטכנולוגי המצומצם ביותר המאפשר לזהות את קיומה או היעדרה של הפגיעות החמורה ותוך ניסיון שלא להיחשף למידע אישי וללא איסוף מידע אישי.

פרק ז': עונשין

סעיפים 44-46

נוכח האינטרס הציבורי העלול להיפגע כתוצאה מהפרה של הוראות חוק זה מוצע להטיל אחריות פלילית על ארגון שלא קיים הוראה מבצעית שתכליתה הגנה על הציבור מפני תקיפות סייבר. בהתאם, בסעיף 44 מוצע לקבוע בסעיף קטן (א) שארגון שלא נקט, בניגוד לסעיף 10(ה) המוצע באמצעים להתמודדות או מניעת סיכון משמעותי במשק הנדרשים באופן דחוף, עליהם הורה ראש מערך הסייבר הלאומי, או ארגון שלא מילא הוראה להתמודדות עם תקיפת סייבר חמורה שניתנה על-ידי עובד מוסמך מגזרי או עובד מוסמך מטעם מערך הסייבר הלאומי, לפי העניין, בניגוד לסעיפים 15(א)(4), 16(א) ו- 17(ב) המוצעים, דינו יהיה מאסר שנתיים או קנס כאמור בסעיף 61(א)(4) לחוק העונשין.

כמו כן, מוצע שככל שמדובר בעבירה נמשכת, נוסף על העונש האמור, יוטל קנס נוסף, כאמור בסעיף 61(ג) לחוק העונשין לכל יום שבו נמשכת ההפרה.

בנוסף, בסעיף 45 מוצע לקבוע שנושא משרה בתאגיד, 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 קטן (א) בידי תאגיד או בידי עובד בתאגיד ; המפר הוראה זו, דינו – קנס כאמור בסעיף 61(א)(3) לחוק העונשין. כמו כן, מוצע לקבוע חזקה לפיה אם נעברה עבירה לפי סעיף קטן (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.

זאת ועוד, בסעיף 46 מוצע לקבוע שאדם שגילה מידע אישי שהתקבל מארגון לפי חוק זה או עשה שימוש במידע אישי שהתקבל מארגון לפי חוק זה, בניגוד להוראות הסודיות, הגבלת השימוש והמחיקה המוצעות בסעיף 49, דינו מאסר שלוש שנים.

פרק ח': הוראות שונות

סעיף 47

בכדי לייצר וודאות עבור הארגונים החיוניים באשר לעמידתם בדרישות המחייבות בתחום הגנת הסייבר, מוצע לקבוע, שארגון חיוני יוכל לפנות לרשות מוסמכת לקבלת חוות דעת מקדמית על התאמת אופן יישום דרישה המנויה בתוספת הרביעית לעניין רמת הגנת סייבר בסיסית. בכדי לאפשר לרשות המוסמכת לגבש את חוות הדעת המקדמית על בסיס כלל המידע הנדרש לצורך כך, תהיה רשאית רשות מוסמכת לדרוש ידיעות ומסמכים נוספים הדרושים לה לצורך מתן חוות הדעת המקדמית.

סעיף 48

מוצע לקבוע בסעיף קטן (א) שלצורך הפעלת סמכות עובד מוסמך מגזרי, עובד מוסמך במערך הסייבר הלאומי לפי החוק, וכן סמכות עובד לפי סעיפים 42 ו- 43 המוצעים (בסעיף זה- עובד מוסמך), רשאי העובד מוסמך להסתייע במומחה, לרבות מומחה שאינו עובד מדינה, שהוא בעל ניסיון, ידע או אמצעים יחודיים הדרושים להפעלת הסמכות. בכדי להבטיח שגם כאשר סמכויות מופעלות על ידי מומחה כאמור, יחולו כלל המגבלות, האיזונים והבלמים החלים בהפעלת סמכות על ידי עובד מדינה, מוצע לקבוע בסעיף קטן (ב) שהעובד המוסמך יפקח על ביצוע הפעולות על ידי המומחה. בכל מקרה שיקול הדעת שניתן לרשות מוסמכת או לעובדיה או למערך הסייבר הלאומי או לעובדיו, במסגרת הפעלת סמכויותיו לפי החוק, לא יופעל על ידי המומחה החיצוני. עוד מוצע לקבוע בסעיף קטן (ג) שמומחה

הנכנס למקום לפי סעיף 13 המוצע ללא עובד מוסמך מגזרי שנוכח במקום, תיעשה בתנאים בסעיף 13 המוצע וכן בתנאי שניתנה הסכמה בכתב של מחזיק המקום לכניסת מומחה למקום, לאחר שניתן לו הסבר על מטרת הכניסה ועל זכותו לסרב לכניסת המומחה ולחזור בו מהסכמתו עד לתחילת בחינת המומחה.

עוד מוצע לקבוע בסעיף קטן (ד) שמנהל בכיר ברשות מוסמכת או מנהל בכיר במערך הסייבר הלאומי לפי העניין (בסעיף זה "הגורם המאשר") יהיו רשאים לתת אישור לשמש מומחה חיצוני למי שהוא בעל ניסיון, ידע ומומחיות המתאימים לתפקיוד ולא הורשע בעבירה שמפאת מהותה, חומרתה או נסיבותיה הוא אינו ראוי לשמש מומחה חיצוני או הוגש נגדו כתב אישום בעבירה כאמור. בנוסף, מוצע לקבוע בסעיף קטן (ה) תנאים שיבטיחו שהמומחה החיצוני לא יהיה מצוי בניגוד עניינים.

בסעיף קטן (ו) מוצע לקבוע שהרואה עצמו נפגע מפעולת מומחה חיצוני יהיה רשאי לפנות בתלונה מנומקת בכתב למנהל בכיר ברשות המומכת או למנהל בכיר במערך הסייבר הלאומי, לפי העניין.

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

מוצע לקבוע בסעיף קטן (ח) שמגבלות על עיסוקיו של המומחה החיצוני לאחר סיום ההתקשרות עימו יקבעו במידת הצורך, בחוזה ההתקשרות עמו, ובכלל זה הוראות לעניין פרק הזמן שבו לא יעבוד המומחה חיצוני אצל גוף המתחרה בגוף שטיפל בענייני כמומחה חיצוני ולא יתן שירות לגוף כאמור או יקבל זכות או טובת הנאה ממנו, והכל אם הדבר נדרש.

סעיף 49

על מנת להגן על הזכות לפרטיות של אדם שמידע אישי לגביו הגיע לידי אדם אחר לפי חוק זה, מוצע לקבוע בסעיף קטן (א) שככל שאדם קיבל מידע אישי שהתקבל לפי חוק זה, הוא ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא למטרת ביצוע סמכות של האדם להגנת סייבר לפי דין, או לפי צו בית משפט.

כן מוצע לקבוע בסעיף קטן (ב) שמידע אישי שהתקבל לפי חוק זה ישמר בהיקף המזערי הנדרש, וימחק לאחר שנתיים לכל היותר מעת קבלתו, אלא אם הוא חיוני לזיהוי מאפייני תקיפת סייבר או להתמודדות עם תקיפת סייבר או חשש לה או שהוא נדרש להליכי הטלת עיצומים לפי פרק ה' לחוק או לשם העמדה לגין בגין ביצוע עבירות לפי פרק ז' לחוק.

יובהר כי לעניין חוק זה כתובת IP לא תחשב מידע אישי.

בסעיף קטן (ג) מוצע לקבוע שפרסום ברבים של זהות ארגון, לרבות ארגון חיוני או ספק שירותים דיגיטליים או שירותי אחסון, שהתקבלה לפי חוק זה, יהיה באישור מנהל בכיר במערך הסייבר הלאומי או מנהל בכיר ברשות מוסמכת לאחר שנתן לארגון הזדמנות להשמיע את טענותיו.

סעיף 50

כדי לשמור על כללי המנהל התקין של רשויות מנהליות הפעולות מכח חוק זה, מוצע לקבוע במפורש שעובד מוסמך מגזרי או עובד מוסמך במערך הסייבר הלאומי יתעד בכתב הוראות להתמודדות עם תקיפת סייבר חמורה שניתנו לארגון לפי סעיפים 15, 16 או 17 המוצעים וימסור לארגון נוסח כתוב של ההוראות בהקדם האפשרי לאחר מתן ההוראה. הנוסח הכתוב לא יכיל מידע מסווג , בסיווג ברמת "שמור" ומעלה, כלומר מידע שסיווגו הביטחוני נקבע בידי רשות המוסמכת בהתאם לכללי סיווג מידע לפי דין.

סעיף 51

לשם יצירת אחידות בעבודה הממשלתית הנוגעת להגנת סייבר ותכלול כלל הפעילות הממשלתית בנושא בידי מערך

הסייבר הלאומי, מוצע לקבוע שאסדרה שיש לה השפעה משמעותית על הגנת סייבר, תיקבע לאחר התייעצות עם ראש מערך הסייבר הלאומי.

סעיף 52

מוצע לקבוע שארגון חיוני המנוי בתוספת השישית, אשר הגיש תצהיר בדבר יישום הנחיות הגנת סייבר בהתאם לתקן NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (control baseline for Moderate or High impact) לעניין פעילות הליבה של הארגון בצירוף אישור המנוי בתוספת השישית, לא יחולו עליו החובות החלות על ארגון חיוני לפי חוק זה, למעט החובה לדווח על תקיפת סייבר משמעותית לפי סעיף 11 המוצע, וזאת לתקופה של שנתיים החל מיום מסירת התצהיר. כמו כן, מוצע לקבוע כי ספק שירותים דיגטליים ושירותי אחסון, שאינו ארגון חיוני, שהגיש למנהל בכיר ברשות מוסמכת תצהיר בדבר אספקת שירותי האחסון, השירותים הדיגיטליים, או אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור, תוך יישום הוראות התקן האמור לעניין שירותי הליבה אותם מספק או לעניין השירותים כאמור שנגדם בוצעה התקיפה בצירוף אישור המנוי בתוספת השישית, לא יחולו עליו הוראות סעיף 17 לעניין מתן הוראות להתמודדות עם תקיפה חמורה לתקופה של שנתיים החל מיום מסירת התצהיר.

תקן NIST 800-53 ברמה בינונית וגבוהה, אליו מפנה הסעיף הוא תקן בין-לאומי מקצועי הנותן מענה לרמת הגנה ולתקיפות בעלות רמת מורכבות ועוצמה גבוהה אשר שחקני תקיפה מתקדמים, עתירי משאבים ונחושים (APT), עשויים לעשות בהן שימוש. התקן כולל הוראות שיש בהן כדי להביא לצמצום משמעותי של התקיפה מארגון הנתקף למקבלי שירותיו, הוא מכיל, בין היתר, בקרות ברזולוציה מפורטת, וכולל, בין השאר, הוראות לעניין ניטור עצמי רציף של חברות, עמידה ברמת הגנה בסייבר והתמודדות עם אירועים. על כן, קיימת הצדקה לפטור מחובות מרכזיות מכח חוק זה כאמור ארגונים העומדים בתקן זה. יצויין שמדובר בתקינה מוכרת ונגישה, וניתן למצוא מידע אודותיה באתר מכון התקנים האמריקאי. כמו כן, על מנת להנגיש את המידע ביתר קלות, תתווסף הפנייה לתקן זה באתר מכון התקנים האמריקאי באתר מערך הסייבר הלאומי.

יובהר שהחובה החלה על כל ארגון במשק ובכלל האמור על ארגון חיוני לעמוד ברמת הגנה נאותה בהתאם לאופי הפעילות ולניהול הסיכון, תמשיך לחול גם על ארגון חיוני שיגיש תצהיר כאמור. עוד יובהר שהגשת תצהיר לא תעצור בדיעבד הליכי פיקוח או הליכים לפי פרק ה' לעניין הטלת עיצומים שהחלו טרם הגשת התצהיר על ידי ארגון.

סעיף 53

החוק מבקש לשפר את הגנת הסייבר הלאומית, ולשפר את רמת החוסן הלאומית בסייבר של ישראל כגון 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 חוק זה באות להוסיף על חוק שירות הביטחון הכללי, תשס"ב-2002 ועל הוראות כל דין אחר ולא לגרוע מהן. בכלל האמור, אין בחוק זה או בהוראות מכוחו כדי לגרוע מחובת ארגון להבטיח בהתאם לכל דין, לרבות דיני הנזיקין, רמת הגנת סייבר ראויה לפעילות הארגון. עוד מוצע להבהיר שהוראות חוק זה באות להוסיף על החלטות מנהל, החלטות ממשלה, ובכלל זאת החלטות ממשלה 2443 ו-2444, או הסכם קיים או עתידי, בעניין הנוגע להגנת סייבר, אולם במקרה של סתירה, יגברו הוראות חוק זה.

סעיף 54

מוצע להבהיר שקבלת מידע אגבית מתקשורת בין מחשבים אגב ביצוע פעולות לשם הגנת סייבר בחומר מחשב לפי חוק זה, לא תיחשב האזנת סתר לפי חוק האזנת סתר, התשל"ט-1979.

סעיף 55

בכדי להבטיח פיקוח פנים ממשלתי ופיקוח פרלמנטרי על אופן יישום חוק זה, מוצע לקבוע שמערך הסייבר הלאומי יציג לועדת החוץ והביטחון של הכנסת אחת לשנה, דוח על תמונת המצב של רמת הגנת הסייבר הלאומית ועל הפעולות שננקטו על-ידי המערך לצורך חיזוק החוסן הלאומי בהגנת הסייבר וקידום ההתמודדות עם תקיפות סייבר בשנה החולפת. עוד מוצע, שמערך הסייבר הלאומי ידווח ולועדת החוץ והביטחון של הכנסת וליועץ המשפטי לממשלה, אחת לשנה על מספר הארגונים החיוניים שקבע מאסדר כי יוחרגו מהגדרת ארגון חיוני אף שעמדו בתבחינים המגזריים, או שנכללו כארגון חיוני על אף שלא עמדו בתבחינים, לפי סעיף 8(ב) המוצע, בחלוקה למגזרים והנימוק שנקבע לכך ; מספר ההוראות שניתנו לפי סעיף 10(ה) המוצע וסוגי הארגונים להן ניתנו ; וביחס לכל הוראה שניתנה לפי סעיף 10(ה) המוצע, על מהות ההוראה שניתנה והאם ניתן אישור ראש הממשלה בטרם מתן ההוראה וסוגי הארגונים להן ניתנו. עוד מוצע לקבוע שדיווח לפי חוק זה יהיה חסוי ופרסומו אסור.

סעיף 56

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

סעיף 57

מוצע לתקן את חוק בתי משפט לעיינים מנהליים, התש"ס-2000 ולהסמיך את בית המשפט לעניינים מינהליים לדון בעתירות בעניין החלטות לפי חוק זה, למעט החלטות ממשלה לפי החוק, בכדי לאפשר ביקורת שיפוטית ונגישות לערכאות ביחס אליהן.

סעיף 58

מוצע להרחיב את ההחרגה הקיימת בחוק חופש המידע ביחס לפעילות מערך הסייבר הלאומי מכח החוק להסדרת הבטחון בגופים ציבוריים, כך שתחול גם ביחס לפעילות חטיבות מערך הסייבר הלאומי העוסקות בהגנת סייבר מול המשק, בהגנת הסייבר של המערך, חטיבת ההגנה ופעילות יחידת הביטחון במערך הסייבר הלאומי. הסיבה להחרגה הגורפת של יחידות אלו במערך הסייבר הלאומי מתחולת החוק לחופש המידע היא שהנגשת מידע בעניין עבודתן לציבור עלולה לחשוף שיטות ואמצעים מדינתיים להגנת סייבר, וכן לחשוף מידע מסווג הנוגע למצב הגנת הסייבר במשק והחוסן הלאומי בסייבר.

סעיף 59

מוצע לקבוע תחילה מאוחרת לחוק במטרה לתת למשק, ובפרט לארגונים חיוניים ולספקי שירותים דיגיטליים או שירותי אחסון, פרק זמן שיאפשר להם להסתגל ולבצע את ההתאמות הנדרשות בארגון לצורך עמידה בחובות כאמור. בהתאם, מוצע לקבוע שתחילתו של חוק זה 3 חודשים מיום פרסומו. בנוסף מוצע לקבוע שהחובה לעמוד ברמת הגנה לפי סעיפים 10(ב) ו-10(ג), חובת הדיווח על תקיפה משמעותית הקבועה בסעיף 11 וחובת ארגון חיוני או ספק שירותים דיגיטליים לפעול להתמודדות עם תקיפת סייבר חמורה בהתאם לסעיפים 15 ו-17, יחולו 12 חודשים לאחר פרסומו של חוק זה.