תזכיר חוק

א. שם החוק המוצע

חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 3), התשפ"ה-2025

ב. מטרת החוק המוצע, הצורך בו, עיקרי הוראותיו והשפעתו על הדין הקיים

מאז תחילתה של מלחמת "חרבות ברזל", החל מיום 7 באוקטובר 2023, ישנה עלייה בהיקף ובעוצמה של תקיפות הסייבר כנגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלו היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עשויות להוביל לפגיעה בחיי אדם. עמדת גורמי המקצוע בנושא היא שתקיפות אלו הולכות והופכות מתוחכמות ומורכבות יותר.

ספקים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שספקים אלו מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או בהבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום י"ד בכסלו התשפ"ד (27 בנובמבר 2023), את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, ובסמוך לכך, ביום י"ד בטבת התשפ"ד (26 בדצמבר 2023) חוקק החוק אשר החליף את תקנות שעת החירום חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023 (להלן – הוראת השעה).

הוראת השעה הוארכה פעמיים והיא בתוקף עד ליום כ"ו בחשוון התשפ"ו (17.11.2025).

ביום 12 ביוני 2025 החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה על נקיטת פעולות צבאיות משמעותיות נגד איראן. נוכח המערכה נגד איראן והערכת מערך הסייבר הלאומי, שירות הביטחון הכללי והממונה על הביטחון במערכת הביטחון (להלן – מלמ"ב, ויחד – הגופים) ביחס לחומרת איומי הסייבר והסיכונים הנשקפים מהם, כמו גם הצורך המבצעי הדחוף בהקניית כלים חיוניים נוספים כאמור, הותקנו ביום 23 ביוני 2025 תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025 (להלן – תקנות שעת החירום). תקנות שעת החירום בתוקף עד ליום כ"ז בתמוז התשפ"ה (23 ביולי 2025) והן כוללות בעיקרן סמכות של מנהל מוסמך לדרוש ידיעות ומסמכים לטובת הכרעה בשאלה אם תקיפת סייבר היא תקיפת סייבר חמורה; חובת דיווח של ספק במגזר השירותים הדיגיטליים ושירותי האחסון על תקיפת סייבר משמעותית המתרחשת כנגדו בפועל; וחובת ספק נתקף בתקיפה חמורה ליידע על-אודות התקיפה ארגון מקושר אשר עלול להיפגע ממנה באופן ישיר וממשי.

נוכח ההערכות המקצועיות ביחס לחומרת איומי הסייבר העדכניים והסיכונים הנשקפים מהם, עמדת הגופים היא שלאור מאפייניו הייחודיים של מרחב הסייבר הישראלי, הצורך בכלי התמודדות במרחב הסייבר נשמר. לפיכך, הכלים החיוניים, אשר הותקנו בעיקרם במסגרת הוראת השעה ותקנות שעת החירום לצורך התמודדות

עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור והבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור, וזאת אף במנותק מן הלחימה במסגרת מלחמת "חרבות ברזל" ומהמערכה מול איראן.

משכך, מוצע לעגן במסגרת הוראת השעה את הכלים שהותקנו במסגרת תקנות שעת החירום וכן להאריך את תוקפה, נוכח ההערכות המקצועיות כאמור לעיל. בנוסף, מוצע לנתק את הזיקה של הוראת השעה לפעולות הצבאיות המשמעותיות, שעליהן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק יסוד: הממשלה, בסמוך לאחר אירועי ה-7.10.2023 (להלן – הפעולות הצבאיות המשמעותיות), כך שהפעלת הסמכויות מכוח הוראת השעה לא תהיה תלויה במצב הלחימה. זאת, כאמור, לאור הערכת גורמי המקצוע כי במישור הקיברנטי מרחב הלחימה יוסיף להתנהל בעצימות גבוהה, באופן אשר מצדיק את הקניית הסמכויות האמורות גם במנותק ממצב הלחימה במרחב הקינטי, וזאת לתקופה זמנית במסגרת הוראת שעה.

חוק זה בא לתקן את הוראת השעה ולהחליף את ההסדר שנקבע בתקנות שעת החירום.

ג. להלן נוסח תזכיר החוק המוצע ודברי הסבר

תזכיר חוק מטעם משרד ראש הממשלה:

תזכיר חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה) (תיקון מס' 3), תשפ"ה-2025

תיקון שם החוק

1. בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023 (להלן – החוק העיקרי), בשם החוק, המילים "(חרבות ברזל)" – יימחקו.

תיקון סעיף 1

2. בסעיף 1 לחוק העיקרי:

(א) לפני ההגדרה "מחשב" יבוא:

"ארגון מקושר" – ארגון שקיים חיבור, פיזי או לוגי, קבוע או עיתי, בין מחשביו לבין מחשבי הספק, או שמתבצעת העברת חומר מחשב, קבועה או עיתית, ממחשביו למחשבי מקבל שירותיו;";

(ב) בהגדרה "מנהל מוסמך", האמור בסעיף קטן (3) ימחק ובמקומו יבוא:

"(3) ראש יחידת הסייבר במלמ"ב;";

(ג) אחרי ההגדרה "מערך הסייבר" יבוא:

"המרכז הלאומי" – המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר (CERT) שמפעיל מערך הסייבר;

(ד) בהגדרה "עובד מוסמך" בסעיף קטן (3) המילים "היחידה הטכנולוגית" ימחקו ובמקומם יבוא "יחידת הסייבר";

(ה) ההגדרה "הפעולות הצבאיות המשמעותיות" – תימחק.

תיקון סעיף 2

3. בסעיף 2(א) לחוק העיקרי:

(א) ברישא, במקום "או בקיום האספקה והשירותים החיוניים" יבוא "או בהבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור".

(ב) סעיף 2(א)(1) ימחק, וסעיפים 2(א)(2) ו-2(א)(3) יסומנו "2(א)(1) ו2(א)(2)", בהתאמה;

(ג) אחרי סעיף (א) יבוא:

"(א1) היה למנהל מוסמך יסוד סביר להניח כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי היא עומדת להתרחש, היא תקיפת סייבר חמורה נגד ספק או תקיפה כאמור הנעשית באמצעות ספק, רשאי הוא להנחות עובד מוסמך לדרוש מהספק להציג לו כל ידיעה או מסמך, לרבות פלט, כדי להבטיח את ביצועו של חוק זה או להקל על ביצועו";

(ד) בסעיף (ב), בסופו, במקום "בפסקאות (1) עד (3) של אותו סעיף קטן" יבוא "בפסקאות (1) ו- (2) של אותו סעיף קטן".

הוספת סעיף 2א

4. אחרי סעיף 2 לחוק העיקרי יבוא סעיף 2א:

חובת דיווח 2א.

(א) נודע לספק על כך שמתרחשת נגדו, בפועל, תקיפת סייבר, ידווח על כך למנהל המוסמך באמצעות המרכז הלאומי, בהתאם להוראות סעיף קטן (ב), אם מתקיים לגביה אחד מאלה:

(1) יש חשש ממשי שהיא אינה מוגבלת לספק הנתקף;

(2) היא עלולה לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות השירות של הספק, בהתחשב, בין השאר, באלה:

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

(ב) סוג הפגיעה והיקפה;

(ג) משך הפגיעה;

(ב) ספק ידווח לפי סעיף קטן (א), לפי אחד מאלה:

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

(א) פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;

(ב) מועד תחילת תקיפת הסייבר ומועד גילוייה;

(ג) מידע לגבי מאפייני תקיפת הסייבר והשפעתה על הספק;

(ד) מידע הנוגע לאפשרות השפעת התקיפה על ארגון מקושר.

(2) (א) הספק יגיש דיווח ראשוני ללא דיחוי מתחייב ולא יאוחר מ- 24 שעות מהמועד בו נודע לספק על תקיפת הסייבר, תוך פירוט הפרטים שלהלן, אם הם ידועים לו:

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

(2) מידע בסיסי על תקיפת הסייבר, ובכלל זה כל מידע הידוע לספק, שיש בו כדי לסייע בהערכת חומרת התקיפה והשלכותיה.

(ב) הספק יגיש דיווח עיקרי ללא דיחוי ולא יאוחר מ-72 שעות מהמועד שבו נודע לספק על תקיפת הסייבר, תוך פירוט הפרטים שלהלן, אם הם ידועים לו:

(1) עדכון ביחס למידע שנמסר בדיווח הראשוני כאמור בפסקה (1), לרבות מידע הנוגע להערכת חומרת התקיפה, השפעותיה והשלכותיה על הספק ועל ארגון מקושר;

(2) מידע הנוגע למאפייני תקיפת הסייבר ולמזהי התקיפה.

(ג) מנהל מוסמך רשאי להנחות עובד מוסמך לדרוש מן הספק דיווח ביניים לעדכון מידע הנוגע לתקיפת הסייבר ולהתמודדות עמה, במועד שיקבע המנהל המוסמך.

(ד) הספק יגיש דיווח מסכם על הפעולות שבוצעו לטיפול בתקיפת הסייבר לא יאוחר מ-30 ימים מהמועד שבו נודע לספק על תקיפת הסייבר תוך פירוט הפרטים שלהלן:

(1) מידע נוסף אודות תקיפת הסייבר, לרבות חומרתה, השפעתה והשלכותיה על הספק ועל ארגון מקושר;

(2) נסיבות ומתווה התקיפה, ככל שהם ידועים לספק;

(3) אופן הטיפול בתקיפה, לרבות פירוט אודות אמצעים אשר עודם ננקטים;

(ה) אם לא הסתיים הטיפול בתקיפת הסייבר בתוך 30 ימים, הספק יגיש במועד זה דיווח אודות התקדמות הטיפול בתקיפת הסייבר, הכולל את הפרטים לפי פסקה (4), ככל שהם ידועים לספק. עם סיום הטיפול בתקיפה, הספק יגיש דיווח מסכם לפי פסקה (4).

(ג) דיווח לפי סעיף זה יכול שיוגש באופן מקוון באתר האינטרנט של מערך הסייבר הלאומי, בהודעה טלפונית למרכז הלאומי או בדרך אחרת שהורה עליה ראש מערך הסייבר הלאומי ופורסמה באתר האינטרנט כאמור.

(ד) על אף האמור בסעיף קטן (ג), ספק של גוף מהגופים המנויים בפרטים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון, יגיש את הדיווח לפי סעיף זה למלמ"ב, באופן שיורה לו ראש המלמ"ב.

תיקון סעיף 3

5. בסעיף 3 לחוק העיקרי:

(א) האמור בו יסומן "(א)" וברישא, לאחר המלים "נגד ספק" יבוא "או באמצעותו".

(ב) בסעיף קטן (א)(3) המילים החל מ"בנוסח שפרסם" – יימחקו, ובמקומן יבוא "לפי הוראות סעיף 3א, והכל בתוך פרק זמן סביר כאמור בפסקה (2)";

(ג) אחרי סעיף קטן (א) יבוא:

"(ב) (1) מסר העובד המוסמך לספק הודעה כאמור בסעיף קטן (א), ימסור הספק, בלא דיחוי, עדכון בדבר התקיפה החמורה לכל ארגון מקושר אשר עלול להיפגע ממנה ישירות ובאופן ממשי, וידווח על כך בכתב לעובד המוסמך, והכול אלא אם כן הורה העובד המוסמך אחרת.

(2) המנהל המוסמך רשאי, לפי בקשה בכתב מאת הספק, אם שוכנע כי קיימות נסיבות חריגות המצדיקות זאת, לפטור את הספק מחובת היידוע כאמור בפסקה (1) או לדחות את מועד היידוע."

הוספת סעיף 3א

6. אחרי סעיף 3 לחוק העיקרי יבוא סעיף 3א:

"אי תחולת הוראות מסוימות לגבי ספק שהגיש תצהיר

3א. הוראות סעיפים 2(א1), 3(א)(3) ו-3(ב) לא יחולו לעניין ספק שהגיש לעובד המוסמך תצהיר בנוסח שפרסם ראש מערך הסייבר באתר האינטרנט של מערך הסייבר הלאומי, בדבר אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו של הספק או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור ללקוחותיו של הספק, תוך יישום הנחיות אבטחה בהתאם לתקנים המנויים בתוספת, לעניין כלל השירותים כאמור שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה.

תיקון סעיף 4

7. בסעיף 4 לחוק העיקרי במקום המלים "שנתן לספק לפי סעיף 3" יבוא "שניתנו לפי סעיפים 2(א1) , 2א(ב)(2)(ג) ו- 3".

תיקון סעיף 6

8. בסעיף 6(ב) לחוק העיקרי אחרי המלים "בתקיפת הסייבר החמורה," יבוא "ולעניין תקיפת סייבר שנקבע, לפי הוראות סעיף 2, שהיא אינה תקיפת סייבר חמורה – בסמוך לאחר קבלת החלטה על כך שהתקיפה אינה מהווה תקיפת סייבר חמורה,".

תיקון סעיף 8

9. בסעיף 8 לחוק העיקרי:

(א) בסעיף קטן (1) במקום "סעיף 3(4)" יבוא "סעיף 3(א)(4)";

(ב) בסעיף קטן (1א) במקום "סעיף 3(4)" יבוא "סעיף 3(א)(4)";

(ג) בסעיף קטן (2) במקום "סעיף 3" יבוא "סעיף 3(א)"

(ד) אחרי סעיף קטן (4) יבוא:

"(5) מספר המקרים שבהם דיווח ספק, לפי הוראות סעיף 2א, על כך שמתרחשת נגדו תקיפת סייבר כאמור באותו סעיף;

(6) מספר המקרים שבהם הורה עובד מוסמך לספק שלא למסור לארגון מקושר עדכון בדבר תקיפת סייבר חמורה, לפי הוראות סעיף 3(ב)(1);"

תיקון סעיף 10

10. בסעיף 10 לחוק העיקרי המילים "חרבות ברזל" ימחקו.

תיקון סעיף 11

11. האמור בסעיף 11 לחוק העיקרי יסומן "(א)" ואחריו יבוא

"(ב) תקנות שעת חירום (חרבות ברזל)(סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025 – בטלות."

תיקון סעיף 12

12. בסעיף 12 לחוק העיקרי המלים "עד יום כ"ו בחשוון התשפ"ו (17 בנובמבר 2025)." ימחקו ובמקומן יבוא "עד יום ז' בניסן התשפ"ו (25.3.2026)".

תיקון סעיף 13

13. האמור בסעיף 13 לחוק העיקרי יסומן "(א)" ואחריו יבוא:

"(ב) הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025, לפני כניסתו לתוקף של חוק זה, יראו אותן כאילו נעשו לפי חוק זה והוראותיו יחולו עליהם."

תיקון התוספת הראשונה

14. בתוספת לחוק העיקרי:

(א) בכותרת במקום "סעיף 3(3)" יבוא "סעיף 3א";

(ב) בפרט מספר 1, בסופו יבוא "(High)"

(ג) האמור בפרט 2 ימחק ובמקומו יבוא:

"(2) עמידת הספק באחד משילובי התקנים המפורטים להלן, בצירוף המסמכים הנדרשים לצידם:

1. הספק מיישם את הדרישות לצורך עמידה בשניים מתקני הליבה שלהלן ומצרף לתצהירו אישורים על עמידה בדרישות אותם תקנים, כמפורט לצידם:

- ISO/IEC 27001 או ת"י 27001 – תעודת הסמכה בתוקף
- SOC 2 Type 2 – תעודת הסמכה או דוח Attestation בתוקף
- CMMC Level 3 – תעודת הסמכה או דוח הערכה (Assessment) ע"י DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
- NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate) - באמצעות הצגת מסמך Authorization To Operate (ATO) קבוע ובתוקף, החתום על ידי Authorizing Official (AO) מוסמך מטעם סוכנות

פדרלית, משרד ממשלתי או גוף ציבורי אחר בארצות הברית. המסמך יוגש ללא תנאים מגבילים (ATO with Conditions) וללא פריטי Plan of Action and Milestones (POA&M) , אשר מועד הטיפול בהם פג במועד ההגשה, וזאת בהתאם לרמת Moderate.

2. הספק מקיים את שני אלה:

2.1 הספק מיישם את הדרישות לצורך עמידה בתקן אחד מתקני הליבה שלהלן, ומצורף לתצהירו אישור על עמידה בדרישות אותו תקן, כמפורט לצידו; וכמו כן הספק עומד בדרישות של תקן נוסף מתקני הליבה שלהלן:

- ISO/IEC 27001 או ת"י 27001 – תעודת הסמכה בתוקף
- SOC 2 Type 2 – תעודת הסמכה או דוח אימות תאימות (Attestation) בתוקף
- CMMC Level 3 – תעודת הסמכה או דוח הערכה (Assessment) ע"י DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
- NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate)- באמצעות הצגת מסמך Authorization To Operate (ATO) קבוע ובתוקף, החתום על ידי Authorizing Official (AO) מוסמך מטעם סוכנות פדרלית, משרד ממשלתי או גוף ציבורי אחר בארצות הברית. המסמך יוגש ללא תנאים מגבילים (ATO with Conditions) וללא פריטי Plan of Action and Milestones (POA&M) , אשר מועד הטיפול בהם פג במועד ההגשה, וזאת בהתאם לרמת Moderate

2.2 הספק מיישם את הדרישות לצורך עמידה בתקן אחד מהתקנים המשלימים שלהלן ומצורף לתצהירו אישור על עמידה בדרישות אותו תקן, כמפורט לצידו:

תקן ISO/IEC 27017 – תעודת הסמכה

תקן ISO/IEC 27018 – תעודת הסמכה

תקן ISO/IEC 27034 – תעודת הסמכה

- תקן ISO/IEC 27035 – תעודת הסמכה
- תקן ISO/IEC 27701 – תעודת הסמכה
- תקן NIST SP 800-161 – תעודת הסמכה
- תקן PCI DSS – תעודת הסמכה
- תקן IEC 62443 – תעודת הסמכה
- תקן ISO 22301 - תעודת הסמכה
- תקן SOC 2 Type 1 – תעודת הסמכה
- תקן "רב מגן" ברמה 2 – אישור בכתב מאת משרד הביטחון
- תקן CIS – Critical Security Control (IG 3) - דוח אימות תאימות מאת CIS Securesuite Members

3. הספק מקיים את כל אלה:

3.1 הספק מיישם את הדרישות לצורך עמידה בתקן שלהלן, ומצרף לתצהירו אישור על עמידה בדרישות אותו תקן, כמפורט לצדו:

- CMMC Level 3 – תעודת הסמכה או דוח הערכה (Assessment) ע"י DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
- NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate)

באמצעות הצגת מסמך Authorization To Operate (ATO) קבוע ובתוקף, החתום על ידי Authorizing Official (AO) מוסמך מטעם סוכנות פדרלית, משרד ממשלתי או גוף ציבורי אחר בארצות הברית. המסמך יוגש ללא תנאים מגבילים (ATO with Conditions) וללא פריטי Plan of Action and Milestones (POA&M) , אשר מועד הטיפול בהם פג במועד ההגשה, וזאת בהתאם לרמת Moderate

3.2 הספק עומד בדרישות של תקן אחד מתקני הליבה שלהלן:

- ISO/IEC 27001 או ת"י 27001

- SOC 2 Type 2

3.3 הספק עומד בדרישות תקן אחד מהתקנים המשלימים שלהלן:

- תקן ISO/IEC 27017
- תקן ISO/IEC 27018
- תקן ISO/IEC 27034
- תקן ISO/IEC 27035
- תקן ISO/IEC 27701
- תקן NIST SP 800-161
- תקן NIST SP 800-218
- תקן PCI DSS
- תקן IEC 62443
- תקן ISO 22301
- תקן SOC 2 Type 1
- תקן "רב מגן" ברמה 2
- תקן CIS – Critical Security Control (IG 3) - דוח אימות תאימות מאת CIS Securesuite Members"

דברי הסבר

כללי מאז תחילתה של מלחמת "חרבות ברזל", החל מיום 7 באוקטובר 2023, ישנה עלייה בהיקף ובעוצמה של תקיפות הסייבר כנגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלו היא לפגוע, כחלק מהמתקפה המשולבת המכוונת כלפי חוסנה של מדינת ישראל, במרחב הסייבר הישראלי, בכלכלה ובתפקודו התקין של המשק הישראלי, והן אף עשויות להוביל לפגיעה בחיי אדם. עמדת גורמי המקצוע בנושא היא שתקיפות אלו הולכות והופכות מתוחכמות ומורכבות יותר.

ספקים של שירותי אחסון ושל שירותים דיגיטליים מהווים יעד מועדף לתקיפות סייבר, בין השאר, מאחר שספקים אלו מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי. בשים לב לאמור, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה בביטחון המדינה, בביטחון הציבור או בהבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור.

כדי להתמודד עם הצורך המתואר לעיל, התקינה הממשלה, ביום י"ד בכסלו התשפ"ד (27 בנובמבר 2023), את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, ובסמוך לכך, ביום י"ד בטבת התשפ"ד (26 בדצמבר 2023) חוקק החוק אשר החליף את תקנות שעת החירום חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023 (להלן – הוראת השעה).

הוראת השעה מסמיכה מנהל מוסמך במערך הסייבר הלאומי, בשירות הביטחון הכללי או בממונה על הביטחון במערכת הביטחון (מלמ"ב) (להלן – הגופים), וכן מסמיכה את ראש חטיבת ההגנה בצה"ל, לקבוע כי תקיפת סייבר היא תקיפת סייבר חמורה, ככל שיש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים; ובהמשך לכך – נתונה לעובד מוסמך באחד הגופים הסמכות להודיע לספק על קיומו של חשש לתקיפת סייבר חמורה כנגדו. ככל שהספק לא הגיש תצהיר לפי הוראת השעה, וכן לא פעל באופן הולם ובתוך פרק זמן סביר שניתן לו לטיפול בתקיפת הסייבר החמורה, מסמיכה הוראת השעה את העובד המוסמך לתת לספק הנתקף הוראות לצורך איתור התקיפה, מניעתה או בלימתה, תוך שהוראת השעה קובעת תנאים למתן ההוראות כאמור.

הוראת השעה הוארכה פעמיים והיא עומדת בתוקף עד ליום כ"ו בחשוון התשפ"ו (17.11.2025).

ביום 12 ביוני 2025 החליטה ועדת השרים לענייני ביטחון לאומי על נקיטת פעולות צבאיות משמעותיות נוכח המערכה נגד איראן לפי סעיף 40 לחוק-יסוד: הממשלה.

נוכח המערכה נגד איראן והערכת הגופים ביחס לחומרת איומי הסייבר והסיכונים הנשקפים מהם, והצורך המבצעי הדחוף בהקניית כלים חיוניים נוספים כאמור, הותקנו ביום 23 ביוני 2025 תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025 (להלן – תקנות שעת החירום). תקנות שעת החירום בתוקף עד ליום כ"ז בתמוז התשפ"ה (23 ביולי 2025) והן כוללות בעיקרן סמכות מנהל מוסמך לדרוש ידיעות ומסמכים מספק במגזר השירותים הדיגיטליים ושירותי האחסון לטובת הכרעה בשאלה אם תקיפת סייבר היא תקיפת סייבר חמורה; חובת דיווח של ספק למנהל מוסמך על תקיפת סייבר משמעותית כנגדו; וחובת ספק נתקף בתקיפה חמורה ליידע ארגון מקושר אשר עלול להיפגע מן התקיפה באופן ישיר וממשי.

נוכח ההערכות המקצועיות ביחס לחומרת איומי הסייבר העדכניים והסיכונים הנשקפים מהם, עמדת הגופים היא שלאור מאפייניו הייחודיים של מרחב הסייבר, הצורך בכלי התמודדות במרחב הסייבר הישראלי נשמר. לפיכך, הכלים החיוניים, אשר הותקנו בעיקרם במסגרת הוראת השעה ותקנות שעת החירום לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור והבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור, וזאת אף במנותק מן הלחימה במסגרת מלחמת "חרבות ברזל" ומהמערכה מול איראן. משכך, מוצע לעגן במסגרת הוראת השעה את הכלים שהותקנו במסגרת תקנות שעת החירום וכן להאריך את תוקפה נוכח ההערכות המקצועיות, כאמור לעיל.

בנוסף, מוצע לנתק את הזיקה של הוראת השעה לפעולות הצבאיות המשמעותיות, שעליהן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק יסוד: הממשלה, בסמוך לאחר אירועי ה-7.10.2023 (להלן – הפעולות הצבאיות המשמעותיות), כך שהפעלת הסמכויות מכוח הוראת השעה לא תהיה תלויה במצב הלחימה. זאת, כאמור, לאור הערכת גורמי המקצוע כי במישור הקיברנטי מרחב הלחימה יוסיף להתנהל בעצימות גבוהה, באופן אשר מצדיק את הקניית הסמכויות האמורות גם במנותק ממצב הלחימה במרחב הקינטי, וזאת לתקופה זמנית במסגרת הוראת שעה.

חוק זה בא להחליף את ההסדר שנקבע בתקנות שעת החירום ומוצע לבטלן.

סעיף 1 כאמור, מגמת העלייה בהיקף ומורכבות תקיפות הסייבר, בייחוד כלפי מגזר השירותים הדיגיטליים ושירותי האחסון, התחדדה עם פרוץ מלחמת חרבות ברזל. בהתאם, נקבע ההסדר שבהוראת השעה כהסדר שחל במהלך מלחמת חרבות ברזל. בפרט, הגדרתה של תקיפת סייבר כתקיפת סייבר חמורה, מותנית כיום, בין היתר, בהתרחשותה במהלך תקופות הפעולות הצבאיות המשמעותיות. לצד זאת כאמור, עמדת הגופים היא שבהתאם להערכות המקצועיות ביחס לחומרת איומי הסייבר העדכניים והסיכונים הנשקפים מהם ולאור מאפייניו

הייחודיים של מרחב הסייבר הישראלי, הצורך בכלי התמודדות במרחב הסייבר נשמר אף בהיעדר לחימה במרחב הקינטי. לפיכך, הכלים החיוניים, אשר הותקנו בעיקרם במסגרת הוראת השעה ותקנות שעת החירום לצורך התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, נדרשים לשם שמירה על ביטחון המדינה, בטחון הציבור והבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור, וזאת אף במנותק מן הלחימה במסגרת מלחמת "חרבות ברזל" ומהמערכה הקינטית מול איראן. על כן, מוצע לקבוע שההסדר הקבוע בהוראת השעה יחול ללא תלות בהימשכות הפעולות הצבאיות המשמעותיות. בהתאם, מוצע לשנות את שמו של החוק ולהסיר ממנו את המלים "חרבות ברזל".

סעיף 2 מוצע להוסיף לסעיף 1 בהוראת השעה הגדרות נוספות שייעשה בהם שימוש.
בתוך כך, מוצע לקבוע בסעיף 3(ב) את חובת ספק נתקף בתקיפה חמורה לידע ארגון מקושר אשר עלול להיפגע ממנה באופן ישיר וממשי. לעניין זה, מוצע להגדיר "ארגון מקושר" כארגון שקיים חיבור, פיזי או לוגי, קבוע או עיתי, בין מחשביו לבין מחשבי הספק, או שמתבצעת העברת חומר מחשב, קבועה או עיתית, ממחשביו למחשבי מקבל שירותיו. כלומר, ארגון מקושר הוא ארגון שקיימת חיבוריות בין מחשביו למחשבי הספק בגינה קיימת סכנה להתפשטות התקיפה מהספק לארגון.
כמו כן, מוצע להגדיר את "המרכז הלאומי", באמצעותו ידווח ספק על תקיפת סייבר משמעותית בהתאם לסעיף 2א כמרכז הלאומי לסיוע התמודדות עם איומי סייבר (CERT) שפועל במערך הסייבר הלאומי, וכן לתקן את הגדרת המנהל המוסמך במלמ"ב.
בנוסף, מוצע למחוק את הגדרת "הפעולות הצבאיות המשמעותיות" מסעיף 1, וזאת עקב ניתוק הוראת השעה מהזיקה לפעולות הצבאיות המשמעותיות, כאמור לעיל.

סעיף 3 כמפורט לעיל, ולאור מאפייניו הייחודיים של מרחב הסייבר, מוצע לקבוע שההסדר יחול ללא תלות בהימשכות הפעולות הצבאיות המשמעותיות. בהתאם, מוצע לתקן את העילה לפיה יקבע מנהל מוסמך שיש חשש ממשי לתקיפת סייבר חמורה. כך, לפי הנוסח המוצע, המנהל המוסמך יידרש לבחון אם יש בתקיפה חשש ממשי "לפגיעה בביטחון המדינה בביטחון הציבור או בהבטחת רציפות אספקתם הנאותה של שירותים החיוניים לציבור".
במקביל, מוצע למחוק מרשימת התבחינים להגדרתה של תקיפת סייבר כתקיפת סייבר חמורה על ידי המנהל המוסמך בהתאם לסעיף 2 להוראת השעה, את התבחין הקבוע בסעיף 2(א)(1) לפיו על התקיפה להתרחש במהלך תקופת הפעולות הצבאיות המשמעותיות.
בנוסף, מוצע להוסיף להוראת השעה את סעיף 2(א1) ולקבוע בו שכאשר למנהל מוסמך יש יסוד סביר להניח שתקיפת סייבר שמתרחשת, או שקיים חשש ממשי כי עומדת להתרחש, נגד ספק או באמצעות הספק, היא תקיפה חמורה, הוא יהיה רשאי להנחות עובד מוסמך לדרוש מהספק להציג לו ידיעות או מסמכים, לרבות פלט מחשב, וזאת כדי להבטיח את ביצועו של חוק זה או להקל על ביצועו. זאת, לצורך בחינת התקיימותם של התנאים לקביעה שתקיפת סייבר שמתרחשת או שיש חשש ממשי שעומדת להתרחש היא תקיפה חמורה לפי סעיף 2(א) להוראת השעה. כמו כן, בהתאם לסעיף 4 להוראת השעה, הדרישה להעברת ידיעות או מסמכים תתועד בכתב ויימסר לספק נוסח כתוב של הדרישה שאינו מכיל מידע מסווג, בהקדם האפשרי לאחר הדרישה. יובהר, שפניית מנהל מוסמך לספק לצורך דרישת ידיעות ומסמכים, תבוצע באופן מצומצם והדרגתי ככל הניתן, בשים לב לנתונים הקיימים בידי המנהל המוסמך ולמידע המינימלי הנדרש לבחינת חומרת תקיפת הסייבר המסוימת. כך לדוגמא, ככל שלטובת החלטה אם התקיפה הנבחנת היא תקיפת סייבר חמורה, נדרש למנהל המוסמך מידע בנוגע לקישוריות הספק 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 הראשונית של המנהל המוסמך, ככל האפשר, בדרישה ממוקדת לקבלת המאפיינים הטכנולוגים הנדרשים לצורך הבחינה האמורה.

סעיף 4 מוצע להוסיף להוראת השעה את סעיף 2א ולקבוע, שספק ידווח באופן מיידי למנהל מוסמך אם נודע לו על תקיפת סייבר המתרחשת נגדו בפועל, אשר יש חשש ממשי שאינה מוגבלת לספק הנתקף, או תקיפה העלולה לפגוע באופן משמעותי בזמינות, ברציפות או במהימנות שירותי הספק. לצורך בחינת התקיימותו של התנאי השני, הספק ישקול שיקולים שונים, ובהם את כמות או סוג המשתמשים העלולים להיות מושפעים מהתקיפה, סוג והיקף הפגיעה וכן את משך הפגיעה.
עוד מוצע לקבוע שדיווח לפי סעיף זה יכול שיוגש באופן מקוון באתר האינטרנט של מערך הסייבר הלאומי, בהודעה טלפונית למרכז הלאומי או בדרך אחרת שיורה ראש מערך הסייבר הלאומי ותפורסם באתר האינטרנט האמור.
ספק של הגופים המנויים בסעיף 2 ובסעיף 3 לתוספת הראשונה לחוק להסדרת הביטחון, התשנ"ח-1998, כלומר - משרד הביטחון, מפעלי מערכת הביטחון ומפעלים המייצרים מוצרים עבור מערכת הביטחון שהוגדרו בצו על ידי שר הביטחון, ימסור את ההודעה על תקיפת סייבר נגדם למלמ"ב, באופן שיורה לו ראש מלמ"ב.

מוצע לקבוע כי הספק יבצע את הדיווח באחת משתי דרכים, לבחירתו:
א. <u>חלופת דיווח ראשונה</u>: דיווח מיידי, הכולל את הפרטים שלהלן, ככל שהם ידועים לספק, וכל מידע אחר שיש בו כדי לסייע להערכת חומרתה של תקיפת הסייבר והשלכותיה:
(1) פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;
(2) מועד תחילת תקיפת הסייבר ומועד גילוייה;
(3) מידע לגבי מאפייני תקיפת והשפעתה על הספק;
(4) מידע הנוגע לאפשרות השפעת התקיפה על ארגונים מקושרים, כלומר ארגון שקיים קישור לוגי או פיזי בינו לבין הספק, קבוע או עיתי, או שמתבצעת העברת חומר מחשב קבועה או עיתית, ממחשביו למחשבי מקבל שירותיו;
ב. <u>חלופת דיווח שניה</u>: דיווח הדומה לחובת הדיווח הקבועה בדירקטיבת האיחוד האירופי (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for High Common Level of Cybersecurity Across the Union) (להלן – דירקטיבת NIS2), אשר כיום ספקים שונים ממילא נדרשים למסור בהתאם לדירקטיבה האמורה. בדומה לקבוע בדירקטיבת NIS2, מוצע לקבוע בחלופת דיווח זו שספק יגיש ללא דיחוי ובתוך 24 שעות מהמועד בו נודע לו על התקיפה דיווח ראשוני שיכלול את הפרטים הבאים, ככל שהם ידועים לו:
(א) פרטי הספק והשירותים שהוא מספק, ובכלל זה פרטי קשר שלו;
(ב)מידע בסיסי על תקיפת הסייבר, ובכלל זה כל מידע הידוע לספק, שיש בו כדי לסייע בהערכת חומרת התקיפה והשלכותיה.
עוד מוצע לקבוע במסגרת חלופה זו, בהתאם לקבוע בדירקטיבת NIS2, שספק יגיש דיווח עיקרי ללא דיחוי ולא יאוחר מ- 72 שעות מהמועד שבו נודע לו על תקיפת הסייבר, שיכלול, ככל שהפרטים ידועים לו, עדכון ביחס למידע שנמסר בדיווח הראשוני, לרבות מידע הנוגע להערכת חומרת התקיפה, השפעותיה והשלכותיה על ארגונים מקושרים ומידע הנוגע למאפייני ומזהי תקיפת הסייבר (למשל סוג התקיפה, מאפיינים טכנולוגיים של התקיפה ואופן התקיפה).
בנוסף, בדומה לקבוע בדירקטיבת NIS2, מוצע לקבוע שמנהל מוסמך יהיה רשאי להנחות עובד מוסמך לדרוש מן

הספק דיווח ביניים לעדכון מידע הנוגע לתקיפת הסייבר והתמודדות עמה במועד שיקבע המנהל המוסמך.

כמו כן, בדומה לקבוע בדירקטיבת NIS2, מוצע לקבוע שהספק יגיש דיווח מסכם על הפעולות שבוצעו לטיפול בתקיפת הסייבר לא יאוחר מ-30 ימים מהמועד שבו נודע לספק על תקיפת הסייבר שיכלול את הפרטים שלהלן:

(א) מידע נוסף אודות תקיפת הסייבר, לרבות חומרתה, השפעתה והשלכותיה על הספק ועל ארגונים מקושרים;

(ב) נסיבות ומתווה התקיפה ככל שהם ידועים לספק;

(ג) אופן הטיפול בתקיפה לרבות פירוט אודות אמצעים אשר עודם ננקטים.

עוד מוצע לקבוע שאם לא הסתיים הטיפול בתקיפת הסייבר בתוך 30 ימים, הספק יגיש במועד זה, דיווח אודות התקדמות הטיפול בתקיפת הסייבר, הכולל את הפרטים הידועים לספק מתוך הפרטים שעליו לדווח במסגרת הדיווח המסכם, ועם סיום הטיפול בתקיפה, יגיש גם דיווח מסכם.

סעיף 5 מוצע להבהיר ברישא של סעיף 3(א), שהוראות החוק ביחס לתקיפה חמורה, חלות כשתקיפת סייבר מתרחשת או עומדת להתרחש נגד ספק וגם כשתקיפה כאמור מתקיימת באמצעותו.

עוד מוצע לקבוע, כי הוראות הסעיף לא יחולו על ספק אשר יגיש תצהיר לפי הוראות סעיף 3א לחוק והתוספת לחוק, אותה מוצע להרחיב, כפי שיפורט להלן.

כמו כן, בשים לב לחיבוריות הגבוהה במגזר המשק הרלוונטי ולנוכח הצורך למנוע התפשטות תקיפות חמורות, מוצע להוסיף את סעיף 3(ב) ולקבוע בו שעם קבלת הודעת העובד המוסמך לספק כי תקיפת סייבר שמתרחשת או עומדת להתרחש נגדו היא תקיפת סייבר חמורה, יידע הספק בלא דיחוי ארגון מקושר שעלול להיפגע ישירות ובאופן ממשי מהתקיפה, וידווח על כך לעובד המוסמך. עוד מוצע לקבוע, כי חובת היידוע לפי סעיף זה, לא תחול אם הורה על כך העובד המוסמך, או שהמנהל המוסמך מצא כי קיימות נסיבות המצדיקות זאת, לבקשת הספק.

סעיף 6 בהתאם לסעיף 3(א)(3) להוראת השעה, באפשרות הספק למסור תצהיר, כמפורט בתוספת להוראת השעה, בדבר יישום הנחיות אבטחה בהתאם לתקן הבינלאומי NIST 800-53 Security and Privacy Controls for Information Systems and Organizations

מוצע להרחיב את האמור ולקבוע בסעיף 3א, שספק אשר יצהיר על אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו של הספק או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור ללקוחותיו של הספק, תוך יישום הנחיות אבטחה בהתאם לתקנים המנויים בתוספת, ובכלל האמור שילוב בין התקנים כמפורט בתוספת, לעניין כלל השירותים כאמור שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה לא יידרש למסור ידיעות או מסמכים לבחינת התקיימותה של תקיפת סייבר חמורה בהתאם לסעיף 2(א1) המוצע, לא יינתנו לו הוראות לפי סעיף 3(א)(4) לחוק וכן הוא יהיה פטור מן החובה לעדכן ארגון מקושר על תקיפות סייבר חמורות בהתאם לסעיף 3(ב) המוצע. מדובר בתקנים בין-לאומיים מקצועיים שיש בהם כדי ליתן מענה לתקיפות מורכבות. עמידה בדרישות המפורטות בתקנים אלו – שהם מוכרים ונגישים במגזר השירותים הדיגיטליים ושירותי האחסון – מעידה על יכולת התמודדות טובה עם איומי סייבר, המביאה לצמצום משמעותי של הסיכון הנשקף מתקיפה אצל ספק העומד בדרישות תקנים אלו.

רשימת התקנים, והשילובים ביניהם, נבחרו מאחר שלגופים העומדים בהם יש נהלים, מדיניות ארגונית ותהליכים ארגוניים שמבטיחים טיפול הולם בתקיפות חמורות. ספק המוסמך לפי אחד או יותר מתקני הליבה המנויים בתצהיר מפגין רמה יחסית גבוהה של מוכנות ניהולית ותהליכית בהתמודדות עם איומי סייבר. הסמכה כאמור מעידה על כך שהארגון מיישם גישה שיטתית לזיהוי ולניהול סיכונים, מחזיק במדיניות סדורה, מבצע מיפוי תהליכים ונכסים, ומפעיל בקרות להגנה, זיהוי, תגובה ושיקום. בנוסף, קיימת התמקדות בהגברת המודעות

הארגונית ובהטמעת תהליכים מבוססי Best Practices, תוך שילוב אחריות הנהלה גבוהה. העמידה בתקנים אלה מבטאת יישום של עקרונות חוסן דיגיטלי והיערכות מקצועית להתמודדות עם תרחישים מורכבים. תקנים אלו מהווים מסגרת יציבה ואמינה ליצירת מערך אבטחת מידע והגנת סייבר מודרנית, והם תומכים ביישום רציף של שיפור ותחזוקה של מערך הסייבר הארגוני – הן ברמה הניהולית והן ברמה האופרטיבית. לצד אלו, התקנים המשלימים המנויים בתוספת משמשים כחיזוק נקודתי במרחבי סיכון ייחודיים- פיתוח מאובטח, אבטחת ענן, פרטיות, ICS, שרשרת אספקה ותגובה לאירועים. שילוב בין תקן ליבה ותקן משלים מספק כיסוי רוחבי סביר ועומק הגנתי המהווים יחדיו מענה טוב לתקיפות סייבר חמורות.

סעיף 7 סעיף 4 להוראת השעה קובע שעובד מוסמך יתעד בכתב את ההוראות שניתנו לפי סעיף 3 וימסור נוסח כתוב לספק של ההוראות, שאינו מכיל מידע מסווג, וזאת בהקדם האפשרי לאחר מתן ההוראה. מוצע להוסיף חובת תיעוד דומה על ידי העובד המוסמך ביחס לדרישת ידיעות ומסמכים של המנהל המוסמך לפי סעיף 2(א1) ולסעיף 2א(ב)(2)(ג).

סעיף 8 במסגרת ההסדר הקיים, סעיף 6(ב) להוראת השעה קובע שמידע שהתקבל מספק לפי הוראת השעה יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, אלא אם כן קבע מנהל מוסמך שהמידע כאמור חיוני לזיהוי מאפייני תקיפת הסייבר. מוצע לתקן את סעיף 6(ב) ולהוסיף שלעניין תקיפת סייבר שנקבע לפי הוראות סעיף 2שהיא אינה תקיפת סייבר חמורה, יימחק המידע בסמוך לאחר קבלת החלטה על כך שהתקיפה אינה מהווה תקיפת סייבר חמורה, אלא אם כן קבע מנהל מוסמך שהמידע חיוני לזיהוי מאפייני תקיפת הסייבר. מידע שנקבע לגביו כאמור, יישמר בהיקף המזערי הנדרש.

סעיף 9 לשם קיום פיקוח ובקרה שוטפים על פעולותיהם של הגורמים המוסמכים לפי תקנות אלו, מוצע לקבוע כי תורחב חובת הדיווח ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, הקבועה בסעיף 8 להוראת השעה, כך שתתווסף חובת דיווח לעניין מספר המקרים שבהם דיווח ספק, לפי הוראות סעיף 2א, על כך שמתרחשת נגדו תקיפת סייבר כאמור באותו סעיף וכן לעניין מספר המקרים שבהם הורה עובד מוסמך לספק שלא למסור לארגון מקושר עדכון בדבר תקיפת סייבר חמורה, לפי הוראות סעיף 3(ב)(1);

סעיף 10 במסגרת התיקון המוצע לשם החוק, מוצע לעדכן גם את ההפניה שבסעיף.

סעיף 11 חוק זה בא להחליף את ההסדר שנקבע בתקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ״ה-2025 ומוצע לבטלן.

סעיף 12 לנוכח האיומים והערכות של גורמי המקצוע בגופים, כמתואר לעיל, כמו גם הצורך במתן פרק זמן שיאפשר לבחון את אופן יישומם של ההסדרים החדשים המוצעים, מוצע להאריך את תוקפה של הוראת השעה עד ליום ז׳ בניסן התשפ״ו (25.3.2026).

סעיף 13 לצד ביטול תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ״ה-2025, וכדי להבטיח את רציפות הדין בין תקנות שעת החירום לבין תיקון החוק המוצע, מוצע לקבוע הוראת מעבר לפי הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת

החירום האמורות, כאילו נעשו לפי חוק זה, והוראותיו יחולו עליהן.

סעיף 14 כאמור, בתיקון המוצע להוספת סעיף 3א להוראת השעה, מוצע לקבוע כי ספק שיגיש תצהיר בדבר אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו של הספק או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור ללקוחותיו של הספק, תוך יישום הנחיות אבטחה בהתאם לתקנים המנויים בתוספת, לפי העניין, לעניין כלל השירותים כאמור שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה, יהיה פטור מן הדרישה למסור ידיעות או מסמכים לבחינת התקיימותה של תקיפת סייבר חמורה בהתאם לסעיף 2(א1) המוצע, לא יינתנו לו הוראות לפי סעיף 3(א)(4) וכן יהיה פטור מהחובה לעדכן ארגון מקושר על תקיפות סייבר חמורות בהתאם לסעיף 3(ב) המוצע.
בהתאם, מוצע לתקן את התוספת ולהוסיף לרשימת התקנים המנויים בה גם את החלופה של עמידה בשילובי תקנים, לצד צירוף המסמכים הנדרשים כמפורט בתוספת. חלופה נוספת זו תחליף את פרט 2 לתוספת כך שתימחק האפשרות לקבוע תקינה נוספת באמצעות תיקון התוספת.
בנוסף, מוצע להוסיף את המונח High לפרט 1 בתוספת להוראת השעה, שעניינו ברמה הגבוהה של התקן המנוי בה NIST 800–53 Security and Privacy Controls for Information Systems and Organizations. גוף המיישם קו בסיס אבטחה גבוה (High), נערך באופן מיטבי להתמודד עם תקיפות סייבר חמורות. שכן, הוא מיישם סט מקיף של אמצעי הגנה, שנועדו להגן על סודיות, שלמות וזמינות המידע והמערכות, לנהל סיכוני אבטחה באופן פרואקטיבי ושיטתי, ולספק יכולת להגן על פעולות ונכסים קריטיים וחיוניים, באופן שמקים בסיס איתן לעמידות המערכות גם בפני האיומים החמורים ביותר.