



רשומות

ספר החוקים

14 באוגוסט 2025

3453

כ' באב התשפ"ה

עמוד

חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון
(הוראת שעה – חרבות ברזל) (תיקון מס' 3), התשפ"ה-2025 798

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

1. תיקון שם החוק
בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023¹ (להלן – החוק העיקרי), בשם החוק, במקום "(הוראת שעה – חרבות ברזל)" יבוא "(הוראת שעה)".
2. תיקון סעיף 1
בסעיף 1 לחוק העיקרי –
(1) לפני ההגדרה "'חומר מחשב", "מחשב", "פלט" ו"תוכנה"' יבוא:
"ארגון מקושר" – ארגון שקיים חיבור, פיזי או לוגי, קבוע או עיתי, בין מחשבו לבין מחשבי הספק, או שמתבצעת העברת חומר מחשב, קבועה או עתית, בין מחשבי הספק למחשבו;
(2) בהגדרה "מנהל מוסמך", במקום פסקה (3) יבוא:
(3) לעניין ספק של הגופים המנויים בפרטים 2 ו-3 בתוספת הראשונה לחוק להסדרת הביטחון – ראש יחידת הסייבר במלמ"ב;
(3) אחרי ההגדרה "מערך הסייבר" יבוא:
"המרכז הלאומי" – המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר (CERT), שמפעיל מערך הסייבר;
(4) בהגדרה "עובד מוסמך", בפסקה (3), במקום "היחידה הטכנולוגית" יבוא "יחידת הסייבר";
(5) ההגדרה "הפעולות הצבאיות המשמעותיות" – תימחק.
3. בסעיף 2 לחוק העיקרי –
(1) בסעיף קטן (א) –
(א) ברישה, במקום "בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים" יבוא "בביטחון המדינה או בביטחון הציבור, או לפגוע באופן חמור בריציפות אספקתם של שירותים חיוניים לציבור";
(ב) פסקה (1) – תימחק;
(2) אחרי סעיף קטן (א) יבוא:
"א" (1) 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, בעצמו או באמצעות עובד מוסמך, לדרוש מהספק להציג לו כל ידיעה או מסמך לרבות פלט, כדי להבטיח או להקל את ביצועו של סעיף זה; הוראות סעיף קטן זה לא יחולו לעניין ספק שהגיש תצהיר כאמור בסעיף 3(א)(3).
(3) בסעיף קטן (ב), במקום "בפסקאות (1) עד (3)" יבוא "בפסקאות (2) ו-(3)".

* התקבל בכנסת ביום י"ט באב התשפ"ה (13 באוגוסט 2025); הצעת החוק ודברי הסבר פורסמו בהצעות חוק הממשלה – 1888, מיום י"ט בתמוז התשפ"ה (15 ביולי 2025), עמ' 984.
¹ ס"ח התשפ"ד, עמ' 410; התשפ"ה, עמ' 426.

"חובת דיווח 2א. (א) נודע לספק על כך שמתרחשת נגדו, בפועל, תקיפת סייבר משמעותית שמתקיים לגביה אחד מהמפורטים להלן, ידווח על כך למנהל המוסמך, בהתאם להוראות סעיף קטן (ב):

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

(ב) סוג הפגיעה והיקפה;

(ג) משך הפגיעה.

(ב) לשם מילוי חובת הדיווח כאמור בסעיף קטן (א), יפעל ספק באחת הדרכים שבפסקאות (1) או (2) להלן, בציון הדרך שבה בחר לפעול:

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

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

(ב) מועד תחילתה של תקיפת הסייבר ומועד גילויה;

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

(ד) מידע הנוגע לאפשרות שתקיפת הסייבר תשפיע באופן ממשי על ארגון מקושר;

(2) יגיש את הדיווחים בהתאם למפורט להלן:

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

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

(ג) יגיש, לפי דרישה מאת המנהל המוסמך, בעצמו או באמצעות עובד מוסמך, ובמועד שיקבע המנהל המוסמך, דיווח ביניים הכולל עדכון לגבי המידע שנמסר לפי פסקאות משנה (א) או (ב);

(ד) יגיש, לא יאוחר מחלוף 30 ימים מהמועד שבו הגיש את הדיווח לפי פסקת משנה (ב), דיווח הכולל את הפרטים שלהלן (להלן – דיווח מסכם):

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

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

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

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

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

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

תיקון סעיף 3 5. בסעיף 3 לחוק העיקרי –

(1) האמור בו יסומן "(א)" ובו –

(א) ברישה, אחרי "נגד ספק" יבוא "או באמצעותו";

(ב) בפסקה (3), במקום "בהתאם לתקן המנוי בתוספת או לפיה" יבוא "בהתאם לאמור בטור א' לתוספת" ואחרי "שנגדם בוצעה התקיפה" יבוא "ואם בטור ב' לתוספת מנוי לצידו מסמך – בצירוף המסמך";

(2) אחרי סעיף קטן (א) יבוא:

"(ב) (1) מסר העובד המוסמך לספק הודעה כאמור בסעיף קטן (א), ימסור הספק, בלא דיחוי, עדכון בדבר תקיפת הסייבר החמורה לכל ארגון מקושר אשר עלול להיפגע ממנה ישירות ובאופן ממש, וידווח על כך בכתב לעובד המוסמך, והכול אלא אם כן הורה העובד המוסמך אחרת; הוראות סעיף קטן זה לא יחולו לעניין ספק שהגיש תצהיר כאמור בסעיף קטן (א)(3).
(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."

6. בסעיף 4 לחוק העיקרי, במקום "שנתן לספק לפי סעיף 3" יבוא "שניתנו לספק לפי סעיפים 2(א1), 2(ב2)(ג) או 3".

7. בסעיף 6(ב) לחוק העיקרי, אחרי "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 תקיפת סייבר חמורה".

8. בסעיף 8(א) לחוק העיקרי –

(1) בפסקאות (1) ו־1א), במקום "סעיף 3(4)" יבוא "סעיף 3(א)(4)";

(2) בפסקה (2), במקום "סעיף 3" יבוא "סעיף 3(א)";

(3) אחרי פסקה (4) יבוא:

"(5) מספר הספקים שנדרשו להציג למנהל מוסמך ידיעה או מסמך לפי הוראות סעיף 2(א1);

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

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

9. בסעיף 10 לחוק העיקרי, המתקן את חוק בתי משפט לעניינים מינהליים, התש"ס-2000,² בפרט 65 לתוספת הראשונה לחוק האמור המובא בו, במקום "(הוראת שעה – חרבות ברזל)" יבוא "(הוראת שעה)".

10. בסעיף 12 לחוק העיקרי, במקום "כ"ו בחשוון התשפ"ו (17 בנובמבר 2025)" יבוא "י"ג בשבט התשפ"ו (31 בינואר 2026)".

11. במקום התוספת לחוק העיקרי יבוא:

"תוספת"

(סעיף 3(א)(3))

² ס"ח התש"ס, עמ' 190.

טור א' התקן	טור ב' המסמך
1. הספק מיישם את הדרישות לצורך עמידה בתקן NIST 800-53 Security and Privacy Controls for Information Systems and Organizations (high)	
2. הספק מיישם את הדרישות לצורך עמידה בשניים מתקני הליבה שלהלן:	
(1) ISO/IEC 27001 או ת"י 27001	תעודת הסמכה בתוקף
(2) SOC 2 Type 2	תעודת הסמכה או דוח Attestation בתוקף
(3) CMMC Level 3	תעודת הסמכה או דוח הערכה (Assessment) על ידי DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
(4) NIST 800-53 Security and Privacy Controls for Information Systems and Organizations (Moderate)	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, ומצורף בלי תנאים מגבילים (ATO) (with Conditions) ובלי פריטי Plan of Action and Milestones (POA&M), שמועד הטיפול בהם חלף במועד הגשת התצהיר, וזאת בהתאם לרמת Moderate
3. הספק מקיים את שני אלה:	
(1) הספק מיישם את הדרישות לצורך עמידה בתקן אחד מתקני הליבה שלהלן ומצורף אישור כמפורט לצידו, וכמו כן הספק מקיים את הבקורות הנדרשות בהתאם לתקן נוסף מתקני הליבה שלהלן:	
(א) ISO/IEC 27001 או ת"י 27001	תעודת הסמכה בתוקף
(ב) SOC 2 Type 2	תעודת הסמכה או דוח אימות תאימות (Attestation) בתוקף

טור א' התקן	טור ב' המסמך
(ג) CMMC Level 3	תעודת הסמכה או דוח הערכה (Assessment) על ידי DCMA DIBCAC (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center
(ד) NIST 800–53 Security and Privacy Controls for Information Systems and Organizations (Moderate)	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, ומצורף בלי תנאים מגבילים (ATO with Conditions) ובלי פריטי Plan of Action and Milestones (POA&M), שמועד הטיפול בהם חלף במועד הגשת התצהיר, וזאת בהתאם לרמת Moderate
(2) הספק מיישם את הדרישות לצורך עמידה בתקן אחד מהתקנים המשלימים שלהלן:	
(א) תקן ISO/IEC 27017	תעודת הסמכה
(ב) תקן ISO/IEC 27018	תעודת הסמכה
(ג) תקן ISO/IEC 27034	תעודת הסמכה
(ד) תקן ISO/IEC 27035	תעודת הסמכה
(ה) תקן ISO/IEC 27701	תעודת הסמכה
(ו) תקן PCI DSS	תעודת הסמכה
(ז) תקן IEC 62443	תעודת הסמכה
(ח) תקן ISO 22301	תעודת הסמכה
(ט) תקן SOC 2 Type 1	תעודת הסמכה
(י) תקן "רב מגן" ברמה 2	אישור בכתב מאת המלמ"ב
(יא) תקן CIS – Critical Security Control (IG3)	דוח אימות תאימות מאת CIS Securesuite Members

4. הספק מקיים את כל אלה:

(1) הספק מיישם את הדרישות לצורך עמידה בתקן אחד מהתקנים שלהלן:

טור א' התקן	טור ב' המסמך
(א) CMMC Level 3	תעודת הסמכה או דוח הערכה DCMADIBCAC על ידי (Assessment) (Defense Contract Management Agency – Defense Industrial Base Cybersecurity Assessment Center)
(ב) NIST 800-53 Security and Privacy Controls for Information Systems and Organizations (Moderate)	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, ומצורף בלא תנאים מגבילים ATO Plan of (with Conditions) פריטי (POA&M), Action and Milestones שמועד הטיפול בהם חלף במועד הגשת התצהיר, וזאת בהתאם לרמת Moderate
(2) הספק מקיים את הבקורות הנדרשות בהתאם לתקן אחד מתקני הליבה שלהלן:	
(א) ISO/IEC 27001 או ת"י 27001	
(ב) SOC 2 Type 2	
(3) הספק מקיים את הבקורות הנדרשות בהתאם לתקן אחד מהתקנים המשלימים שלהלן:	
(א) תקן ISO/IEC 27017	
(ב) תקן ISO/IEC 27018	
(ג) תקן ISO/IEC 27034	
(ד) תקן ISO/IEC 27035	
(ה) תקן ISO/IEC 27701	
(ו) תקן NIST SP 800-161	
(ז) תקן NIST SP 800-218	
(ח) תקן PCI DSS	
(ט) תקן IEC 62443	
(י) תקן ISO 22301	
(יא) תקן SOC 2 Type 1	
(יב) תקן "רב מגן" ברמה 2	
(יג) תקן CIS – Critical Security Control (IG3)	דוח אימות תאימות מאת CIS "Securesuite Members".

12. תקנות שעת חירום (חרבות ברזל) (סמכויות נוספות לשם התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ה-2025³ (להלן – תקנות שעת החירום) – בטלות.

ביטול תקנות
שעת חירום
(חרבות ברזל)
(סמכויות נוספות
לשם התמודדות
עם תקיפות
סייבר חמורות
במגזר השירותים
הדיגיטליים
ושירותי האחסון)

13. הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת החירום, לפני תחילתו של חוק זה, יראו אותן כאילו נעשו לפי החוק העיקרי כנוסחו בחוק זה, והוראותיו יחולו עליהן.

בנימין נתניהו
ראש הממשלה

אמיר אוחנה
יושב ראש הכנסת

יצחק הרצוג
נשיא המדינה

³ ק"ת התשפ"ה, עמ' 2318, מיום כ"ז בתמוז התשפ"ה (23 ביולי 2025).

