



רשומות

# קובץ התקנות

27 בנובמבר 2023

10921

י"ד בכסלו התשפ"ד

עמוד

תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים

ושירותי האחסון), התשפ"ד-2023 ..... 618

## תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים דיגיטליים ושירותי האחסון), התשפ"ד-2023

בתוקף סמכותה לפי סעיף 39 לחוק-יסוד: הממשלה<sup>1</sup>, מתקינה הממשלה תקנות שעת חירום אלה:

הגדרות

### 1. בתקנות שעת חירום אלה –

"ידיעה או מסמך" – לרבות העתק חומר מחשב;

"חומר מחשב" ו"מחשב" – כהגדרתם בחוק המחשבים;

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995<sup>2</sup>;

"חוק להסדרת הביטחון" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998<sup>3</sup>;

"מלמ"ב" – הממונה על הביטחון במערכת הביטחון כמשמעותו בסעיף 21 לחוק להסדרת הביטחון;

"מנהל מוסמך" – אחד מאלה או ממלא מקומו, לפי העניין:

(1) ראש מחלקה בחטיבת איומי סייבר בשב"כ;

(2) ראש מרכז תגובה (IR) במערך הסייבר;

(3) ראש היחידה הטכנולוגית במלמ"ב;

"מערך הסייבר" – מערך הסייבר הלאומי כהגדרתו בחוק להסדרת הביטחון;

"ספק" – אחד מאלה:

(1) מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, ומתקיים חיבור פיזי או לוגי, קבוע או עיתי, או העברת מידע תדירה ממחשבי הספק למחשבי מקבל שירותיו;

(2) מי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי האחסון או שירותים דיגיטליים;

"עובד מוסמך" – כל אחד מאלה:

(1) עובד השירות כהגדרתו בחוק שירות הביטחון הכללי, התשס"ב-2002<sup>4</sup>, שהוסמך בכתב לעניין תקנות שעת חירום אלה בידי ראש חטיבת איומי סייבר בשב"כ או מנהל בשב"כ בדרגת ראש מחלקה הממלא את מקומו;

(2) עובד מערך הסייבר שהוסמך בכתב לעניין תקנות שעת חירום אלה בידי ראש חטיבת ההגנה במערך הסייבר;

(3) עובד מלמ"ב שהוסמך בכתב לעניין תקנות שעת חירום אלה בידי ראש היחידה הטכנולוגית במלמ"ב, לעניין ספק של הגופים המנויים בפרטים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון;

"פעולה להגנת סייבר בחומר מחשב" – מתן הוראות למחשב לצורך הגנת סייבר, ובכלל זה סריקה, עיבוד, הסרה של חומר מחשב הנוגע לתקיפת סייבר, או התקנת סוג תוכנה שפעולתה מוגבלת לרשת הספק בלבד, או חסימה או ניתוק של מחשב או יצירת עותק של חומר המחשב;

<sup>1</sup> ס"ח התשס"א, עמ' 158.

<sup>2</sup> ס"ח התשנ"ה, עמ' 366.

<sup>3</sup> ס"ח התשנ"ח, עמ' 348.

<sup>4</sup> ס"ח התשס"ב, עמ' 179.

"הפעולות הצבאיות המשמעותיות" – הפעולות הצבאיות המשמעותיות שעליהן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה, והודיעה לגביהן לוועדת החוץ והביטחון של הכנסת ביום כ"ג בתשרי התשפ"ד (8 באוקטובר 2023);

"צה"ל" – צבא הגנה לישראל;

"שב"כ" – שירות הביטחון הכללי;

"שירותי אהסון" – שירותי אהסון של מידע שנמסר לשם העלאתו לרשת האינטרנט, שירותי עיבוד ואהסון של נתונים ושירותים לאספקת מידע, תשתית לאהסון או עיבוד נתונים;

"שירותים דיגיטליים" – אחד מאלה:

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

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

(3) שירותי עיבוד, הזנה או שחזור של נתונים, 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;

"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) אהסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;

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

(5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט-1979<sup>5</sup>;

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

(7) הפרעה או מניעה של חיבור של מחשב לרשת תקשורת;

"תקיפת סייבר חמורה" – תקיפת סייבר שמנהל מוסמך מצא כי בשל חשש ממשי להיותה בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף ולנוכח מאפייניה, לרבות מתאר התקיפה או זהות התוקף, וכן בשל התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות, יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים, ובכלל זה תקיפת סייבר שראש חטיבת הגנה בסייבר בצה"ל מצא כי יש בה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל.

<sup>5</sup> ס"ח התשל"ט, עמ' 118.

2. התעורר חשש ממשי לתקיפת סייבר חמורה כנגד ספק והודיע עובד מוסמך לספק על קיומו של חשש כאמור, לאחר שהזדהה לפניו, יחולו הוראות אלה:
- (1) העובד המוסמך יפרט לפני הספק את התשתית העובדתית והמקצועית לקיומו של חשש כאמור, אם אין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים;
- (2) העובד המוסמך ייתן לספק הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה או בלימתה בפרק זמן סביר שאין בו כדי לפגוע בטיפול בתקיפת הסייבר החמורה, והכול בהתחשב במאפייני תקיפת הסייבר;
- (3) הספק יעדכן את העובד המוסמך בדבר הפעולות שביצע לצורך איתור התקיפה, מניעתה או בלימתה או ימסור לעובד המוסמך תצהיר בנוסח שבתוספת בדבר אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800-53 Security and Privacy Controls for Information Systems and Organizations, והכול בתוך פרק זמן סביר כאמור בפסקה (2);
- (4) לא מסר הספק תצהיר כאמור בפסקה (3) ומצא העובד המוסמך כי הספק הנתקף לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה של תקיפת הסייבר החמורה כאמור בפסקה (2), רשאי העובד המוסמך, אם הדבר חיוני לצורך איתור התקיפה, מניעתה או בלימתה, לאחר שהודיע לספק על כוונתו ונתן לו הזדמנות להשמיע את טענותיו, לתת לספק הוראות, בכתב או בעל פה, ובכלל זה הוראות הנוגעות לחומר מחשב שיהיו רק פעולות להגנת סייבר בחומר מחשב, או הוראות למסירת ידיעה או מסמך לידי העובד המוסמך;
- (5) במתן הוראות לפי פסקה (4), ישקול העובד המוסמך את השפעתן האפשרית על הזכות לפרטיות, על פעילות הספק ועל צד שלישי, לרבות על העלות הכלכלית המוערכת של יישום ההוראה ועל הרציפות התפקודית של הספק; העובד המוסמך יורה לנקוט אמצעי שפגיעתו פחותה לצורך איתור התקיפה, מניעתה או בלימתה; העובד המוסמך יפרט את המועד האחרון לביצוע ההוראה;
- (6) התקבלה הוראה מעובד מוסמך לפי פסקה (4), יפעל הספק בהתאם לה ועד המועד האחרון שנקבע לביצועה כאמור בפסקה (5), וידווח על אופן ביצועה לעובד המוסמך עד למועד האמור.
3. עובד מוסמך יתעד בכתב את ההוראות שנתן לספק לפי תקנה 2 וימסור לו נוסח כתוב של ההוראות שאינו מכיל מידע מסווג בתוך פרק זמן סביר ממתן ההוראה; לעניין זה, "מידע מסווג" – מידע שסיווגו הביטחוני נקבע בידי מערך הסייבר, שב"כ, צה"ל או מלמ"ב, לפי העניין, כסיווג ברמת 'שמור' ומעלה.
4. (א) אדם שקיבל מידע שהתקבל מספק לפי תקנות שעת חירום אלה, ישמור אותן בסוד, לא יגלה אותן לאחר ולא יעשה בו כל שימוש, אלא לצורך איתור תקיפת סייבר חמורה, מניעתה או בלימתה.
- (ב) מידע שהתקבל מספק במסגרת פעולה לפי תקנות שעת חירום אלה, יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, למעט מידע שקבע מנהל מוסמך שהוא חיוני לזיהוי מאפייני תקיפת הסייבר; מידע שנקבע לגביו כאמור יישמר בהיקף המזערי הנדרש.
- (ג) בתקנת שעת חירום זאת, "מידע" – למעט מידע על התוקף, התקיפה, מאפייני התקיפה או אמצעי הטיפול בה.

תיעוד

סודיות

5. הפעלת סמכויות כלפי ספק לפי תקנה 2 לעניין תקיפה מסוימת תינתן בידי עובד אופן הפעלת סמכויות מוסמך מקרב גוף אחד בלבד.
6. (א) מערך הסייבר, השב"כ ומלמ"ב ידווחו אחת לשבועיים ליועצת המשפטית דיווח לממשלה ולוועדת החוץ והביטחון של הכנסת בדבר המקרים שבהם ניתנו הוראות לספק בהתאם לתקנה 2(4), הנימוק למתן ההוראות וסוגן.  
(ב) דיווח לפי תקנת שעת חירום זאת יהיה חסוי ופרסומו אסור.
7. בתקופת תוקפן של תקנות שעת חירום אלה, יראו כאילו בחוק בתי משפט לעניינים מינהליים, התש"ס-2000<sup>6</sup>, בתוספת הראשונה, בסופה נאמר:  
"65) החלטה לפי תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023."
8. (א) תקנות שעת חירום אלה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן. שמירת דינים  
(ב) בלי לגרוע מהאמור בתקנת משנה (א), תקנות שעת חירום אלה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת הממשלה או הסכם, ואולם בכל מקרה של סתירה יגברו תקנות שעת חירום אלה.
9. תוקפן של תקנות שעת חירום אלה חודש מיום פרסומן. תוקף

### תוספת

(תקנה 2(3))

#### NIST 800-53 Security and Privacy Controls for Information Systems and Organizations תצהיר ספק על עמידה בתקן

אני ..... מס' זהות ..... נציג חברת ..... לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי/ה לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה בכתב כלהלן:

1. חברת ..... (להלן – החברה) מספקת ללקוחותיה שירותי אחסון או שירותים דיגיטליים, כהגדרתם בתקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון, התשפ"ד-2023, תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800-53 Security and Privacy Controls for Information Systems and Organizations בגרסתו העדכנית ותוך ניהול הסיכונים הרלוונטיים.

2. הגורם הנושא בתפקיד ..... ששמו/ה ..... מס' זהות ..... הוא הגורם המוסמך מטעם החברה לעניין זה.

3. הגורם המוסמך מטעם החברה, כאמור בסעיף 2, יעדכן עובד מוסמך אם יחול שינוי בנוגע לאמור בתצהיר זה בתוך 7 ימים.

אני מצהיר/ה כי השם שלעיל הוא שמי, והחתימה שלמטה היא חתימתי, וכי תוכן תצהירי זה אמת.

.....

תאריך

.....

חתימה

<sup>6</sup> ס"ח התש"ס, עמ' 190.

אישור

אני, ..... עו"ד מרחוב ..... בעיר ..... מאשר/ת בזה כי  
ביום ..... הופיע/ה לפניי מר/גב' ..... המוכר/ת לי באופן אישי/  
שהזדהה/תה לפניי באמצעות תעודת זהות מס' ..... ולאחר שהזהרתיו/ה כי  
עליו/ה לומר את האמת וכי י/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא י/תעשה כן,  
אישר/ה את ההצהרה שלעיל וחתם/מה עליה בפניי.

.....  
חותמת

.....  
חתימה

י"ד בכסלו התשפ"ד (27 בנובמבר 2023)  
(חמ 6618-3)

בנימין נתניהו  
ראש הממשלה









רשומות

# ספר החוקים

26 בדצמבר 2023

3135

י"ד בטבת התשפ"ד

עמוד

חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון  
(הוראת שעה – חרבות ברזל), התשפ"ד–2023 ..... 410

תיקונים עקיפים:

חוק בתי משפט לעניינים מינהליים, התש"ס–2000 – מס' 140

תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים  
הדיגיטליים ושירותי האחסון), התשפ"ד–2023 – ביטול

# חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים דיגיטליים שירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023\*

הגדרות

1. בחוק זה –

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

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995;

"חוק להסדרת הביטחון" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998;

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

"מנהל מוסמך" – אחד מאלה או ממלא מקומו:

(1) ראש יחידת המודיעין וההכוונה בחטיבת איומי סייבר בשב"ב;

(2) ראש מרכז תגובה (IR) במערך הסייבר;

(3) ראש היחידה הטכנולוגית במלמ"ב;

"מערך הסייבר" – מערך הסייבר הלאומי כהגדרתו בחוק להסדרת הביטחון;

"ספק" – אחד מאלה:

(1) מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, ומתקיים חיבור

פיזי או לוגי, קבוע או עיתי, או שמתבצעת העברת חומר מחשב קבועה או עיתית, ממחשבו למחשבי מקבל שירותיו;

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

"עובד מוסמך" – כל אחד מאלה:

(1) עובד השירות כהגדרתו בחוק שירות הביטחון הכללי, התשס"ב-2002;

שראש חטיבת איומי סייבר בשב"ב או ממלא מקומו הסמיך בכתב לעניין חוק זה;

(2) עובד מערך הסייבר שראש חטיבת ההגנה במערך הסייבר הסמיך בכתב לעניין חוק זה;

(3) לעניין ספק של הגופים המנויים בפרטים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון – עובד המלמ"ב שראש היחידה הטכנולוגית במלמ"ב הסמיך בכתב לעניין חוק זה;

"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 הספק בלבד, לחסימה או לניתוק של מחשב, או ליצירת עותק של חומר המחשב;

"הפעולות הצבאיות המשמעותיות" – הפעולות הצבאיות המשמעותיות שעליהן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה<sup>4</sup>, והודיעה לגביהן לוועדת החוץ והביטחון של הכנסת ביום כ"ג בתשרי התשפ"ד (8 באוקטובר 2023);

\* התקבל בכנסת ביום י"ג בטבת התשפ"ד (25 בדצמבר 2023); הצעת החוק ודברי הסבר פורסמו בהצעות חוק הממשלה – 1688, מיום כ"ג בכסלו התשפ"ד (6 בדצמבר 2023), עמ' 358.

<sup>1</sup> ס"ח התשנ"ה, עמ' 366.

<sup>2</sup> ס"ח התשנ"ח, עמ' 348.

<sup>3</sup> ס"ח התשס"ב, עמ' 179.

<sup>4</sup> ס"ח התשס"א, עמ' 158.

"צה"ל" – צבא הגנה לישראל;

"שב"כ" – שירות הביטחון הכללי;

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

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

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

(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;

"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 לחומר מחשב כהגדרתה בסעיף 4 לחוק המחשבים;

(5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט-1979<sup>5</sup>;

(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 מניעה של חיבור של מחשב לרשת תקשורת.

(א) מנהל מוסמך רשאי לקבוע כי תקיפת סייבר שמתרחשת או שיש חשש ממשי כי עומדת להתרחש היא תקיפת סייבר חמורה, אם מצא כי יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים, ובשל כל אלה (בחוק זה – תקיפת סייבר חמורה):

(1) התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות;

(2) קיומו של חשש ממשי שהיא בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף;

(3) מאפייניה, לרבות מיתאר התקיפה או זהות התוקף.

(ב) הסמכות הנתונה למנהל מוסמך לפי סעיף קטן (א) תהיה נתונה לראש חטיבת הגנה בסייבר בצה"ל, לעניין תקיפת סייבר שהוא מצא שמתרחשת או שיש חשש ממשי כי עומדת להתרחש, אם מצא כי יש חשש ממשי שיש בה כדי לפגוע ברציפות התפקוד המבצעי של צה"ל, בשל האמור בפסקאות (1) עד (3) של אותו סעיף קטן.

2. תקיפת סייבר חמורה

<sup>5</sup> ס"ח התשל"ט, עמ' 118.

קבע מנהל מוסמך או ראש חטיבת הגנה בסייבר בצה"ל לפי הוראות סעיף 2 כי תקיפת סייבר שמתרחשת או עומדת להתרחש, נגד ספק, היא תקיפת סייבר חמורה, והודיע על כך עובד מוסמך לספק, לאחר שהזדהה לפניו, יחולו הוראות אלה:

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

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

(3) הספק יעדכן את העובד המוסמך בדבר הפעולות שביצע לאיתור התקיפה, מניעתה או בלימתה או ימסור לעובד המוסמך תצהיר בנוסח שפרסם ראש מערך הסייבר באתר האינטרנט של מערך הסייבר בדבר אספקת שירותי האחסון או השירותים הדיגיטליים ללקוחותיו או בדבר אספקת שירותי תחזוקה, ניהול או בקרה של שירותים כאמור, תוך יישום הנחיות אבטחה בהתאם לתקן המנוי בתוספת או לפיה, לעניין כלל השירותים שהוא מספק, או לעניין השירותים כאמור שנגדם בוצעה התקיפה, והכול בתוך פרק זמן סביר כאמור בפסקה (2);

(4) לא מסר הספק תצהיר כאמור בפסקה (3), ומצא העובד המוסמך כי הספק לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה, כאמור בפסקה (2), רשאי העובד המוסמך אם מצא שהדבר נדרש לאיתור התקיפה, מניעתה או בלימתה, ולאחר שהודיע לספק על כוונתו לתת לו הוראות לפי פסקה זו ונתן לו הזדמנות להשמיע את טענותיו, לתת לספק הוראות, בכתב או בעל פה, שיבצע הספק, ובכלל זה הוראות לביצוע פעולות להגנת סייבר בחומר מחשב או הוראות למסירת ידיעה או מסמך, לרבות העתק מחומר מחשב, לידי העובד המוסמך;

(5) במתן הוראות לספק לפי פסקה (4) –

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

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

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

(6) נתן עובד מוסמך לספק הוראה לפי פסקה (4), יפעל הספק בהתאם לה עד המועד האחרון שנקבע לביצועה כאמור בפסקה (5)(ג), וידרוח על אופן ביצועה לעובד המוסמך עד המועד האמור.

עובד מוסמך יתעד בכתב את ההוראות שנתן לספק לפי סעיף 3 וימסור לו נוסח כתוב של ההוראות שאינו מכיל מידע מסווג, בהקדם האפשרי לאחר מתן ההוראה; בסעיף זה, "מידע מסווג" – מידע שסיווגו הביטחוני נקבע בידי מערך הסייבר, שב"כ, צה"ל או מלמ"ב, לפי העניין, כסיווג ברמת 'שמור' ומעלה.

הסמכויות לפי סעיף 3 לעניין תקיפת סייבר מסוימת נגד ספק, או לעניין כמה תקיפות כאמור המתרחשות באותו מועד, יופעלו כלפי הספק בידי עובד מוסמך מקרב גוף אחד בלבד.

6. סודיות, הגבלת שימוש ומחיקה
- (א) אדם שהגיע לידי מידע שהתקבל מספק לפי חוק זה ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לאיתור תקיפת סייבר חמורה, מניעתה או בלימתה.
- (ב) מידע שהתקבל מספק לפי חוק זה יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, אלא אם כן קבע מנהל מוסמך שהמידע כאמור חיוני לזיהוי מאפייני תקיפת הסייבר; מידע שנקבע לגביו כאמור יישמר בהיקף המזערי הנדרש.
- (ג) פרסום פומבי ברבים של זהות הספק, שהתקבלה לפי חוק זה, יהיה באישור מנהל מוסמך לאחר שנתן לספק הזדמנות להשמיע את טענותיו.
- (ד) בסעיף זה, "מידע" – למעט מידע על התוקף, התקיפה, מאפייני התקיפה או אמצעי הטיפול בה.
7. עונשין
- אדם שגילה מידע שהתקבל מספק לפי חוק זה או עשה שימוש במידע שהתקבל מספק לפי חוק זה, תוך כדי מילוי תפקידו או במהלך מילוי תפקידו, בניגוד להוראות סעיף 6(א), דינו – מאסר שלוש שנים.
8. דיווח
- (א) מערך הסייבר, שב"כ ומלמ"ב ידווחו ליועץ המשפטי לממשלה ולוועדת החוץ והביטחון של הכנסת, אחת לחודש, על כל אלה:
- (1) המקרים שבהם ניתנו הוראות לספק לפי סעיף 3(4), הנימוק למתן ההוראות וסוגן, ומספר המקרים שבהם ספק לא מילא אחר הוראות כאמור;
- (2) מספר המקרים שבהם העובר המוסמך סייע לספק במילוי ההוראות שניתנו לו לפי סעיף 3;
- (3) סוגי הספקים שמנהל מוסמך קבע כי תקיפתם היא תקיפת סייבר חמורה לפי סעיף 2(א);
- (4) מספר המקרים שבהם מנהל מוסמך קבע כי תקיפת סייבר היא תקיפת סייבר חמורה לפי סעיף 2(א), בפילוח בשל פגיעה בביטחון המדינה, פגיעה בביטחון הציבור או פגיעה בקיום האספקה והשירותים החיוניים.
- (ב) דיווח לפי חוק זה יהיה חסוי ופרטומו אסור.
9. שמירת דינים
- (א) הוראות חוק זה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן.
- (ב) בלי לגרוע מהוראות סעיף קטן (א), הוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת הממשלה או הסכם, אולם במקרה של סתירה, יגברו הוראות חוק זה.
10. תיקון חוק בתי משפט לעניינים מינהליים – הוראת שעה – מס' 140
- תיקון חוק בתי משפט לעניינים מינהליים – הוראת שעה – מס' 140
- בתקופת תוקפו של חוק זה, כאמור בסעיף 12, יקראו את חוק בתי משפט לעניינים מינהליים, התש"ס-2000, כך שבתוספת הראשונה, בסופה יבוא:
- "65. החלטה של רשות לפי חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), התשפ"ד-2023".
11. ביטול תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023 – בטלות.

<sup>6</sup> ס"ח התש"ס, עמ' 190; התשפ"ד, עמ' 216.

<sup>7</sup> ס"ח התשפ"ד, עמ' 410.

<sup>8</sup> ק"ת התשפ"ד, עמ' 618.

12. סעיפים 1 עד 10 לחוק זה יעמדו בתוקפם עד תום שבעה חודשים מיום פרסומו.
13. הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד–2023, לפני יום תחילתו של חוק זה, יראו אותן כאילו נעשו לפי חוק זה והוראותיו יחולו עליהן.

### תוספת

(סעיף 3(3))

1. תקן NIST 800–53 Security and Privacy Controls for Information Systems and Organizations
2. תקן שראש מערך הסייבר, בהסכמת ראש השב"כ ומלמ"ב, פרסם ברשומות ובאתר האינטרנט של מערך הסייבר, אם פרסם תקן כאמור, ובלבד שיש בו כדי להבטיח ברמת סבירות גבוהה את הגבלת השפעתה של תקיפת סייבר חמורה מעבר לספק הנתקף וטיפול הולם בתקיפות סייבר חמורות.

בנימין נתניהו  
ראש הממשלה

אמיר אוחנה  
יושב ראש הכנסת

יצחק הרצוג  
נשיא המדינה



