

## תזכיר חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023

עדכון לקוחות – דצמבר 2023

### לקוחות יקרים,

ביום 28 בנובמבר 2023 פרסם משרד המשפטים את טיוטת תזכיר חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023 ("הטיוטה"). הטיוטה היא למעשה המשך של תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), תשפ"ד-2023, אלא שתוקפן של אלה הוא חודש ממועד התקנתן וכמובן שמעמדן הנורמטיבי שונה מחוק ("התקנות").

ראינו לנכון לסקור בתמצית את עיקרי הטיוטה היות ולדעתנו, ככל שתתקבל, יהיה בחוק משום מתן סמכויות שלא היו קיימות עד היום לגופי מדינה, העתידות להשפיע על סקטורים נכבדים במשק.

נשמח לסייע לארגונכם לבחון ולעמוד בהוראות חוק הגנת הפרטיות ובדיני הגנת הפרטיות החלים עליו לרבות בחינת השפעת הוראות טיוטת תזכיר זה.

### עיקרי הדברים

#### רקע

לפי הטיוטה, גופים המספקים שירותים דיגיטליים ושירותי אחסון (מוגדר בהמשך), מתאפיינים בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות משרדי ממשלה, וגופים ציבוריים, בהם גם גופים ביטחוניים, בתי חולים, תשתיות מדינה קריטיות וארגונים החיוניים לתפקודו של המשק, ועוד. לפיכך, הנזק שנגרם מתקיפה כנגד גופים אלו עלול להתפשט ולהשפיע על חברות רבות במשק, דבר ההופך אותם ליעד ערכי לתקיפות סייבר.

למרות רגישותם וחשיבותם של הגופים האמורים, אין כיום גורם ממשלתי האמון על הסדרת פעילותם ככל שהדבר נוגע להגנת הסייבר, כאשר רק אם גופים אלה מחזיקים או מעבדים מידע אישי, מוסדרת פעילותם על ידי רשות הגנת הפרטיות.

לפי משרד המשפטים במסגרת הלחימה המתמשכת מתחוללת עליה בהיקף ובעוצמת מתקפות הסייבר כנגד גופים אזרחיים במשק הישראלי.

בנסיבות אלה מוצע כי בהתקיים חשש ממשי לתקיפת סייבר חמורה (כפי שמוגדר בהמשך) כנגד ספק שירותי אחסון או שירותים דיגיטליים, יהיה רשאי עובד מוסמך במערך הסייבר, בשירות הביטחון הכללי או במלמ"ב, להודיע לספק על קיומו של חשש כאמור ולהנחות אותו כיצד לפעול (במסגרת המגבלות הקבועות בטיוטה).

## עיקרי הטיוטה

### 1. תקיפת סייבר חמורה.

1.1. "תקיפת סייבר" – הטיוטה מגדירה תקיפת סייבר כפעולה או חשש ממשי לפעולה, שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב השמור בו לרבות לפי הדוגמאות המובאות בטיוטה.<sup>1</sup>

1.2. בהתאמה, "תקיפת סייבר חמורה" היא תקיפת סייבר שמנהל מוסמך<sup>2</sup> מצא שבשל 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 סייבר בצה"ל מצא כי יש בה לפגוע ברציפות התפקוד המבצעי של צה"ל.

1.3. "ספק" הוא (א) מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים<sup>3</sup>, ומתקיים חיבור פיזי או לוגי, קבוע או עתי, או העברת מידע תדירה ממחשבי הספק למחשבי מקבל שירותיו; או (ב) מי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי האחסון או שירותים דיגיטליים.

<sup>1</sup> "חומר מחשב" ו-"מחשב" – כהגדרתם בחוק המחשבים, התשנ"ה-1995.  
<sup>2</sup> ראש מחלקה בחטיבת איומי סייבר בשב"כ, ראש מרכז תגובה (IR) במערך הסייבר, ראש היחידה הטכנולוגית במלמ"ב.  
<sup>3</sup> "שירותי אחסון" מוגדרים כשירותי אחסון של מידע שנמסר לשם העלאתו לרשת האינטרנט, שירותי עיבוד ואחסון נתונים ושירותים לאספקת מידע, תשתית לאחסון או עיבוד נתונים; "שירותים דיגיטליים" – אחד מאלה: (1) שירותי תכנה לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח; (2) שירותי ניהול או הפעלה של מערכות מחשבים המשלבות חומרה, תכנה וטכנולוגיות תקשורת; (3) שירותי עיבוד, הזנת או שחזור נתונים, התקנה והגדרת תצורה של מחשבים, התקנת תכנה או שירותי הגנת סייבר; (4) אספקה או התקנה של מחשבים או של ציוד בקרה, המהווים חלק ממכונות וציוד תעשייתי.

## 2. פעולות והנחיות

סעיף 2 קובע כי אם התעורר חשש ממשי לתקיפת סייבר חמורה כנגד ספק-  
2.1. עובד מוסמך<sup>4</sup> רשאי להודיע לספק על קיומו של חשש ממשי לתקיפת סייבר חמורה,  
ולפרט את התשתית העובדתית והמקצועית לקיומו של חשש כאמור, ככל שאין בכך כדי  
לחשוף מקורות מידע, שיטות או אמצעים.

2.2. העובד המוסמך ייתן לספק הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה  
או בלימתה בפרק זמן סביר, בהתחשב במאפייני תקיפת הסייבר והספק יעדכן את העובד  
המוסמך בדבר הפעולות שביצע לצורך איתור, מניעת ובלימת התקיפה או שימסור 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, והכל תוך פרק זמן  
סביר כאמור לעיל.

2.3. לא מסר הספק תצהיר כאמור בפסקה (2.2) ומצא העובד המוסמך כי הספק לא פעל  
באופן הולם, רשאי העובד המוסמך, ככל שהדבר חיוני, לאחר שהודיע לספק על כוונתו  
ונתן לו הזדמנות להשמיע את טענותיו, לתת לספק הוראות, בכתב או בעל פה.

2.4. במתן הוראות לפי פסקה (2.3), 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.

2.5. נתקבלה הוראה מעובד מוסמך לפי פסקה (2.3), יפעל הספק בהתאם לה ועד המועד  
האחרון שנקבע לביצועה כאמור בפסקה (2.4), וידווח על אופן ביצועה לעובד המוסמך עד  
למועד האמור.

## 3. אופן הפעלת הסמכות

3.1. לעובדים המוסמכים יש חובת תיעוד ומסירת התיעוד לספק לו נתנו הוראות מכח הטיוטה  
(למעט לפיהם לא נדרש לפרט פרטים מסווגים בתיעוד האמור).

3.2. הפעלת סמכויות כלפי ספק לעניין תקיפה מסוימת יינתנו בידי עובד מוסמך מקרב גוף  
אחד בלבד.

<sup>4</sup> עובדים שהוסמכו בגופים המנויים בה"ש 1, לפי הוראות המנויות בטיוטה.

- 3.3. ישנה חובת סודיות על מידע המתקבל מספק וחובה לעשות בו שימוש רק לצורך התמודדות עם התקפה.
- 3.4. בתי המשפט לעניינים מנהליים קונים סמכות לדון בהחלטות לפי הטייטה.
- 3.5. ככל שתתקבל הטייטה, החוק יעמוד בתוקף בתקופה שממועד תחילתו ועד חודש לאחר מועד פקיעתה של הכרזה על מצב מיוחד בעורף שתחילה ביום 7 באוקטובר 2023 והוא יחליף את התקנות.

נשמח לסייע ולוודא כי ארגונכם עומד בהוראות הגנת הפרטיות ואבטחת המידע החלות עליו לאור פרסום זה.

המידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו.

בעדכון לקוחות זה נבקש לעדכן בפרסום הידיעה (לקריאת הידיעה אפשר ללחוץ [כאן](#)).



הלל וייס, עו"ד

מחלקת הייטק וטכנולוגיה

[hillel@agmon-law.co.il](mailto:hillel@agmon-law.co.il)



סער רוסמן, עו"ד

שותף מחלקת הייטק וטכנולוגיה  
וראש תחום פרטיות וסייבר

[saar@agmon-law.co.il](mailto:saar@agmon-law.co.il)