17 ביוני, 2026

הצעת חוק הגנת הסייבר הלאומית

עדכוני לקוחות

ב-8 ביוני 2026 עברה בכנסת בקריאה ראשונה הצעת חוק הגנת הסייבר הלאומית, התשפ"ו-2026 ("**הצעת החוק**"). מדובר בצעד משמעותי לקראת הסדרה רוחבית ומקיפה של תחום הגנת הסייבר בישראל, לראשונה בחקיקה ייעודית. הצעת החוק נועדה להבטיח את תפקודו הרציף והבטוח של מרחב הסייבר הלאומי כחלק מחוסנה וביטחונה של מדינת ישראל, תוך קביעת הסדרים ייעודיים ביחס לארגונים חיוניים וביחס לספקי שירותים דיגיטליים ושירותי אחסון. ההסדר המוצע מבוסס על גישה דיפרנציאלית, המתאימה את היקף החובות ואופן הפעלתן למאפייני הארגון, למגזר שבו הוא פועל ולרמת הסיכון הנשקפת מפעילותו.

בעדכון זה ריכזנו את עיקרי הצעת החוק, את ההשלכות המרכזיות שלה על ארגונים עסקיים ואת הצעדים שנכון לנקוט כבר כעת כדי להיערך.

מי עשוי להיות מושפע מהצעת החוק?

ליבת ההסדר שבהצעת החוק מתמקדת ב"**ארגונים חיוניים**", אך נדגיש כבר עתה כי גם ארגון שלא מהווה "ארגון חיוני" עשוי להיות מושפע מהצעת החוק, כפי שיפורט בהמשך.

ארגון ייחשב חיוני אם הוא גוף ממשלתי או אם הוא פועל באחד המגזרים המנויים בתוספת השלישית ועומד בתבחינים שנקבעו לאותו מגזר, אשר מבוססים לרוב על מאפייני פעילות, היקף פעילות או חשיבות השירות. המגזרים שעליהם יחול החוק המוצע כוללים, בין היתר, תקשורת, אנרגיה, בריאות, תחבורה, מזון ואספקת מוצרים ושירותים חיוניים, ושירותים דיגיטליים ושירותי אחסון.

למשל, הארגונים הבאים עשויים להיחשב חיוניים: ספק תקשורת מורשה בעל 200,000 מנויים לפחות; ארגון בעל מתקנים לייצור חשמל בהספק העולה על 100 מגה-ואט; מפעיל תחבורה ציבורית המסיע יותר מ-14 מיליון נוסעים בשנה או שבבעלותו 1,000 כלי רכב ציבוריים או יותר; ארגון המפעיל מחסן חירום ייעודי למוצרי מזון חיוניים; ספק/קמעונאי מזון גדול (מעל נתח שוק מסוים), וכן ספקים מסוימים של תשתיות, שירותי אחסון מידע, שירותי תוכנה, עיבוד נתונים או IT העונים על התנאים המנויים בחוק. בנוסף, הצעת החוק מאפשרת לגורם המאסדר הרלוונטי, בנסיבות חריגות ולאחר מתן זכות טיעון, לקבוע באופן פרטני כי ארגון ייחשב חיוני אף שאינו עומד בתבחינים, או שלא ייחשב חיוני אף שהוא עומד בהם.

הצעת החוק מגדירה **ספקי שירותים דיגיטליים ושירותי אחסון** באופן רחב, כך שהם עשויים לכלול ספקי תוכנה ושירותים טכנולוגיים מסוימים, שירותי ניהול והפעלה של מערכות מחשבים, שירותי עיבוד נתונים, שירותי הגנת סייבר, שירותי אחסון ותשתיות עיבוד – אשר במקרים מסוימים עשויים להיחשב "ארגונים חיוניים". בהקשר זה, הצעת החוק מבחינה בין ספקים בעלי תפקיד תשתיתי בפעילות האינטרנט (שנחשבים ארגונים חיוניים), לבין ספקים אחרים דוגמת ספקי ענן, מרכזי נתונים ואירוח או אבטחת סייבר מנוהל (MSSP), אשר ייחשבו ארגונים חיוניים רק אם מתקיים לגביהם

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין

תנאי נוסף - מחזור עסקאות שנתי ממכירות בישראל העולה על 40 מיליון ש"ח, או אספקת שירותים לגורמים ממשלתיים או לגוף מונחה תוך החזקת הרשאות גישה מועדפות לנכסי הסייבר של מקבל השירות. ספקים הנמנים עם מגזר השירותים הדיגיטליים ושירותי האחסון כפופים כבר כיום לחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה), התשפ"ד-2023, שנחקק בעקבות מלחמת "חרבות ברזל".

לצד זאת, החוק המוצע מאפשר לארגון חיוני שעומד בתקנים ובדרישות המנויים בתוספת השביעית (כגון יישום דרישות תקן NIST SP 800-53), ומגיש תצהיר מתאים ומסמכים כמתואר בתוספת, ליהנות מפטור מחלק מהחובות המוטלות על ארגון חיוני.

<u>החובות המרכזיות שיחולו על ארגונים</u>

- **חובת הגנת סייבר כללית**. הצעת החוק מעגנת **חובה כללית החלה על כל ארגון**, גם אם אינו מוגדר "חיוני", לנקוט **אמצעים סבירים להגנת סייבר** בפעילותו, באופן התואם את אופי פעילותו ואת רמת הסיכון הנובעת ממנה. בבחינת סבירות האמצעים יובאו בחשבון, בין היתר, סוג השימוש במחשב או בחומר מחשב והיקפו, אופי המידע המוחזק, סיכוני הסייבר והנזק שעלול להיגרם מהם לארגון, לציבור או לצדדים שלישיים, העלות הכלכלית של אמצעי ההגנה ביחס למשאבי הארגון ומאפייניו, ואמצעים מקובלים בארגונים דומים. גודל הארגון אף הוא שיקול רלוונטי, בפרט כשמדובר בעסקים זעירים.
- **חובת רמת הגנת סייבר בסיסית לארגונים חיוניים.** לצד החובה הכללית, ומבלי לגרוע ממנה, הצעת החוק מטילה על ארגונים חיוניים חובה ייעודית לקיים רמת הגנת סייבר בסיסית בהתאם לדרישות המפורטות בחלק א' לתוספת הרביעית, תוך יישום ההוראות הנוגעות לאותן דרישות בתקן אחד שיבחר הארגון מבין התקנים המנויים בחלק ב' לתוספת (ISO/IEC 27001 בצירוף ISO/IEC 27002, NIST Cybersecurity Framework 2.0, או NIST SP 800-53), בהתאמות המתחייבות.

הדרישות כוללות, בין היתר, ניהול סיכוני סייבר ומיפוי נכסי סייבר, היערכות לאירועי סייבר ורציפות תפקודית, קביעת מנגנוני דיווח על אירועי סייבר או אירועים חשודים, ניהול סיכוני שרשרת אספקה וממשל פנימי בתחום הגנת הסייבר. בכך, הצעת החוק מבקשת לעגן ביחס לארגונים חיוניים מסגרת סדורה לניהול הגנת הסייבר כחלק מפעילות הארגון. לצד זאת, ארגון חיוני רשאי לבקש מהרשות המוסמכת חוות דעת מקדמית לגבי אופן יישום דרישות מסוימות באמצעות התקן שבחר.

- **חובת דיווח על תקיפת סייבר משמעותית**. ארגון חיוני שנודע לו על תקיפת סייבר משמעותית נגדו נדרש לדווח על כך למערך הסייבר הלאומי ולרשות המוסמכת הרלוונטית. תקיפה תיחשב "משמעותית" אם היא פוגעת, או שקיים חשש ממשי כי תפגע, באופן משמעותי בזמינות, רציפות או מהימנות השירות שהארגון מספק; אם היא עלולה לפגוע בנכס מידע משמעותי או להביא לגישה בלתי מורשית אליו; או אם קיים חשש ממשי כי השפעתה אינה מוגבלת לארגון שהותקף בלבד.
- **הוראות דחופות למניעת סיכון סייבר משמעותי.** במקרים שבהם מתקיים סיכון סייבר העלול לאפשר תקיפת סייבר חמורה (כהגדרתה בהצעת החוק) נגד ארגונים חיוניים או באמצעותם, הצעת החוק מאפשרת לראש מערך הסייבר הלאומי, באישור ראש הממשלה, להורות בכתב לארגון חיוני לנקוט אמצעים דחופים להתמודדות עם הסיכון, תוך שלארגון ניתנת אפשרות להשיג על ההוראה. מדובר בסמכות חריגה ומניעתית, שנועדה לאפשר התערבות מהירה עוד לפני התממשות תקיפה חמורה.
- **תיעוד, שמירת מסמכים והגנה על מידע אישי.** הצעת החוק אינה מסתפקת בקביעת דרישות אופרטיביות,

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין

אלא גם מחייבת שמירת מסמכים המעידים על יישום הדרישות. בהתאם, ארגונים חיוניים נדרשים לשמור מסמכים המעידים על עמידתם בדרישות החוק, לרבות ביחס לרמת הגנת הסייבר הבסיסית וליישום הוראות דחופות שניתנו להם למניעת סיכון סייבר משמעותי. לחובה זו חשיבות מעשית וראייתית, שכן במסגרת סמכויות הפיקוח (כמתואר להלן) ניתן לדרוש מכל גורם רלוונטי למסור ידיעות ומסמכים, לרבות עותקים מחומר מחשב. מידע אישי שהתקבל מארגון יהיה כפוף לחובת סודיות, ועיבוד מידע אישי במסגרת פעולות לפי החוק ייעשה רק במידה הנדרשת לשם הגנת סייבר. המידע יישמר בהיקף המזערי הנדרש ויימחק בתוך שנתיים לכל היותר, אלא אם מתקיים צורך ייעודי בהמשך שמירתו.

<u>סמכויות פיקוח והתערבות</u>

הצעת החוק מקנה לרשות המוסמכת כלי פיקוח ואכיפה לצורך בחינת העמידה בהוראותיה. בכלל זה, עובד מוסמך יהיה רשאי לדרוש מכל גורם רלוונטי (גם אם לא מדובר בארגון חיוני) למסור ידיעות ומסמכים, לרבות עותקים מחומר מחשב, שיש בהם כדי להבטיח את ביצוען של הוראות החוק המוצע. כמו כן, עובד מוסמך יהיה רשאי להיכנס למקום הארגון לצורכי פיקוח על עמידת ארגון חיוני בחובות רמת ההגנה הבסיסית ובחובת הדיווח על תקיפת סייבר משמעותית. בנוסף, במקרה של תקיפת סייבר חמורה, הצעת החוק מאפשרת לרשות המוסמכת לתת הוראות לארגון לשם איתור התקיפה, מניעתה או בלימתה, לרבות הוראות למסירת מידע או מסמכים ובנסיבות מסוימות גם לביצוע פעולות הגנת סייבר בחומר מחשב. סמכויות אלה רלוונטיות בעיקר ביחס לארגונים חיוניים, אך במקרים של תקיפת סייבר חמורה כאמור הן עשויות לחול גם ביחס לספקי שירותים דיגיטליים או שירותי אחסון, אף אם אינם מוגדרים כארגונים חיוניים.

<u>עיצומים כספיים, פרסום ואחריות פלילית</u>

הצעת החוק כוללת מנגנון אכיפה מנהלי שבמרכזו עיצומים כספיים משמעותיים בגין הפרות של חובות שונות, כאשר העיצומים בגין רוב ההפרות הם בהיקף של 640,000 ש"ח. ארגון עלול להיות מחויב בכמה עיצומים בגין מספר הפרות, ובכפל עיצומים בגין הפרות חוזרות. עיקר מנגנון העיצומים חל ביחס לארגונים חיוניים, בין היתר בגין אי-עמידה בחובות החלות עליהם, אי-דיווח על תקיפת סייבר משמעותית או דיווח שלא בהתאם למועדים ולמתכונת שנקבעו, וכן אי-מסירת מידע או מסמכים שנדרש למסור. לצד זאת, גם ספק שירותים דיגיטליים או שירותי אחסון שאינו ארגון חיוני עלול להיות חשוף לעיצום כספי, אם לא קיים הוראה שניתנה לו בכתב במסגרת סמכויות ההתערבות בעת תקיפת סייבר חמורה, לרבות הוראה לביצוע פעולות הגנת סייבר בחומר מחשב או למסירת ידיעה או מסמך.

החלטה על הטלת עיצום כספי תפורסם באתר הרשות המוסמכת, באופן שנועד להבטיח שקיפות לגבי הפעלת שיקול הדעת של הרשות המוסמכת. המשמעות המעשית היא שהחשיפה אינה רק כספית, אלא עלולה להביא לפגיעה במוניטין ואף לחשוף את הארגון לתביעות. לבסוף, ההצעה כוללת גם הוראות עונשיות במקרים מסוימים, לרבות ביחס לאי-קיום הוראות דחופות שניתנו להתמודדות עם סיכון סייבר משמעותי.

<u>אחריות אישית של נושאי משרה</u>

הצעת החוק קובעת אחריות פיקוח אישית לנושאי משרה בתאגיד. על נושא משרה לפקח ולעשות ככל שניתן למניעת עבירות שנוגעות לאי-נקיטת אמצעים מספקים ואי-מילוי הוראות, ואי-עמידה בחובה זו עלולה לגרור קנס אישי. כמו כן, הצעת החוק קובעת כי אם בוצעה עבירה בידי התאגיד או עובד מעובדיו - חזקה היא שנושא המשרה הפר את חובת

הפיקוח, אלא אם הוכיח שעשה כל שניתן כדי למלאה. חזקה זו מחדדת את הצורך של ההנהלה הבכירה לגלות מעורבות פעילה ומתועדת בניהול סיכוני הסייבר.

<u>מה עליכם לעשות כדי להיערך לכניסתו של החוק לתוקף?</u>

הצעת החוק טרם אושרה בקריאה שנייה ושלישית בכנסת, ועשויה להשתנות במסגרת הליך החקיקה. ככל שתאושר בנוסחה הנוכחי, החוק ייכנס לתוקף שלושה חודשים ממועד פרסומו, כאשר חובות מרכזיות מסוימות יחולו רק בחלוף 12 חודשים ממועד הפרסום.

על רקע זה חשוב שחברות יפעלו כבר כעת ליישום הצעדים הבאים:

- **בחינה האם החברה מהווה "ארגון חיוני":** כאמור, הגדרה זו עומדת בליבת תחולתן של הוראות רבות תחת הצעת החוק. יש לבדוק האם החברה עונה על התנאים הקבועים בתוספת השלישית לפי המגזר הרלוונטי לפעילותה.
- **בחינה האם החברה נתונה לדרישות תחת הצעת החוק כספק שירותים דיגיטליים או שירותי אחסון:** יש לבחון האם פעילות החברה נכנסת לגדרי "שירותים דיגיטליים" או "שירותי אחסון" - וזאת בין אם מדובר בארגון חיוני ובין אם לאו, שכן חלק מהחובות חלות גם על ספקים שאינם מהווים ארגון חיוני.
- **מנגנוני זיהוי ודיווח:** יש לוודא שקיימים מנגנוני דיווח פנימיים שיאפשרו זיהוי מהיר של אירוע בר-דיווח ועמידה בלוחות הזמנים הקצרים הקבועים בהצעת החוק.
- **תקנים ואישורים:** יש לבחון האם החברה מחזיקה תקנים מוכרים שעשויים לסייע בעמידה בדרישות - ולחלופין, האם היא תוכל ליהנות מסייג לתחולת חלק מהחובות באמצעות הגשת תצהיר על עמידה בתקנים מתקדמים, כמפורט בתוספת השביעית.
- **שמירת מסמכים:** יש לוודא שקיים מנגנון מסודר לשמירת מסמכים המעידים על יישום דרישות הגנת הסייבר על-ידי החברה, ובכלל זה נהלים, הערכות סיכונים, החלטות, פעולות תיקון ותיעוד אירועים.
- **ממשל תאגידי והגנת סייבר:** מתקפות סייבר חושפות חברות לסיכונים תפעוליים ומשפטיים וכן לסיכוני מוניטין. הצעת החוק, אם תתקבל, צפויה להגביר את הסיכונים האלה ואף ליצור חשיפה אישית לנושאי משרה בחברות בגין אי-עמידה בחובות הפיקוח על יישום דרישות החוק המוצע. על נושאי המשרה בחברה (ובכלל זה ההנהלה הבכירה והדירקטוריון) לגלות מעורבות אקטיבית בניהול סיכוני הסייבר של החברה, ולוודא שקיים ממשל תאגידי ראוי בתחום. זאת במיוחד בארגונים חיוניים ובספקים של שירותי אחסון או שירותים דיגיטליים.
- **פערי ציות:** ארגונים חיוניים צריכים לבחון את הפערים בין דרישות החוק לבין הפרקטיקות והנהלים הקיימים אצלם, ולפעול לטיפול בהם בהקדם האפשרי.

קבוצת הסייבר והפרטיות במשרדנו מייעצת למגוון חברות וארגונים בהיבטים הנוגעים לצמצום החשיפה המשפטית כתוצאה מסיכוני סייבר וביישום הדרישות הרגולטוריות הרלוונטיות.

אנו מזמינים אתכם לפנות אלינו בכל שאלה או התייעצות בנושא.

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי, ואין להסתמך עליו.

אנשי קשר

אסף הראל
שותף

רבקה גניס שפטובסקי
שותפה

רונה טל
מתמחה

כל הזכויות שמורות, גורניצקי ושות' © משרד עורכי דין