הנחיית הרשות להגנת הפרטיות מס' 1/2024:

תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)

רקע

1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן - "**התקנות**") קובעות שורה של חובות ופעולות אשר בעל מאגר מידע, מחזיק במאגר ומנהלו נדרשים לבצע בכדי לקיים את האחריות המוטלת עליהם לפי סעיף 17 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן - "**החוק**") בעניין אבטחת המידע במאגר.

2. **בחברה אשר עיבוד מידע אישי מצוי בליבת הפעילות שלה, או שקיימת סבירות כי פעילותה תיצור סיכון מוגבר לפרטיות, עמדת הרשות היא שעל דירקטוריון החברה מוטלת חובה לפקח על ציות החברה לחוק ולתקנות בהתאם לעקרונות שלהלן. באחריות הדירקטוריון לוודא גיבוש, אימוץ ויישום של מדיניות בדבר אופן ביצוע דרישות החוק והתקנות בחברה**, לרבות חובת הדיווח המיידי לרשות להגנת הפרטיות על קרות אירועי אבטחת מידע. המדיניות תתייחס בין היתר לאופן השימוש במידע אישי בחברה וניהולו בנושאים מהותיים, וכן תגדיר תהליכי פיקוח, בקרה, וציות אפקטיביים. עוד על הדירקטוריון לוודא כי המדיניות מוטמעת בנהלי העבודה בארגון ולקבוע מי הם בעלי התפקידים האחראים על ביצועה. הדירקטוריון יהיה אמון על פיקוח שוטף וקבלת עדכונים ודיווחים על ביצוע החובות על פי התקנות בידי האחראים לכך בחברה.

3. בנוסף, הגם שהתקנות אינן קובעות במפורש את זהות האורגן האמור לבצע בפועל את המשימה המוטלת על התאגיד,[1] עמדת הרשות היא כי בחברות שעיבוד מידע אישי מצוי בליבת הפעילות שלהן או שפעילותן יוצרת סיכון מוגבר לפרטיות, ביצוען של דרישות מסוימות, פיקוחיות באופיין, המוטלות בתקנות על בעל המאגר או על מחזיק במאגר שהוא תאגיד, המפורטות בסעיף 11 להלן – הוא באחריות דירקטוריון החברה, והכל בשים לב למאפיינים הפרטניים של התאגיד, כפי שיפורט בהמשך.

4. עמדה זו מבוססת על פרשנות תכליתית של חוק הגנת הפרטיות והתקנות, בשים לב לעקרונות הממשל התאגידי וחלוקת התפקידים המקובלת בין האורגנים של התאגיד לפי דיני התאגידים בישראל. כך למשל, סעיף 92 לחוק החברות, תשנ"ט-1999 קובע כי "הדירקטוריון יתווה את מדיניות החברה ויפקח על ביצוע תפקידי המנהל הכללי ופעולותיו", וכך גם בפסיקת דיני התאגידים בארה"ב, אשר החלה לקנות אחיזה גם בפסיקת בתי המשפט בישראל.

[1] מלבד מספר מצומצם של משימות אשר תקנה 3 קובעת במפורש כי הן מתפקידו של ממונה אבטחת המידע הארגוני.

5. בפרשת **Caremark**[2] קבע בית המשפט בדלאוור כי על הדירקטוריון מוטלת חובה ליצור מנגנוני בקרה ופיקוח פנימיים בחברה, במטרה לנטר את אופן עמידת החברה בכלל הוראות הדין החלות עליה. בתוך כך, קבע בית המשפט כי על דירקטוריון חברה לוודא קיומם של מערכי ציות ודיווח פנימיים **סבירים** שיספקו לדירקטוריון מידע מספק, מדויק ועדכני, על מנת שיוכל לקבל החלטות מיודעות לגבי ציות החברה לחוק. חובה זו אינה נכנסת לתוקף רק כאשר בפני הדירקטוריון קיים מידע המעורר חשד להפרה של החוק. מדובר בחובה כללית, אשר לפיה על הדירקטוריון לפעול בשגרה, ומראש, להטמעת מנגנוני בקרה ודיווח פנימיים.

6. על פי פסיקה זו, עשויה לקום לדירקטוריון אחריות בשני סוגי מצבים: האחד, אם הדירקטוריון "כשל בצורה מוחלטת" (utter failure) להטמיע מערכת של בקרה, שליטה או קבלת מידע לגבי ציות לרגולציה; השני - אם הדירקטוריון הטמיע מערכת כזו, אולם כשל במודע לפקח על יישומה בפועל, ובכך מנע מהדירקטורים לדעת על סיכונים או בעיות, לרבות "דגלים אדומים", שדרשו את התייחסותם.[3] פסיקה עדכנית של בית המשפט בדלאוור קבעה כי לעניין זה תחום אבטחת המידע בקרב ספקי שירות מקוון הוא קריטי לחברה (mission critical).[4]

ראוי להזכיר גם את פסק הדין של בית המשפט בדלאוור בעניין רשת המלונות **Marriot** משנת 2021.[5] התביעה הוגשה בעקבות מתקפת סייבר שנבעה מכשל אבטחת מידע במערכות החברה, אשר כתוצאה ממנו נוצר איום בחשיפת מידע אודות מאות מיליוני לקוחותיה של החברה. לגבי חלק מהלקוחות הללו, כלל האיום חשיפה של מידע רגיש כגון מספרי דרכונים. המתקפה הביאה לדליפת מידע בהיקף נרחב, ובעקבותיה נוהלו נגד החברה הליכים שונים, פליליים ואזרחיים. לגבי אחריות הדירקטורים לנזק, קבע בית המשפט בדלאוור לפי הלכת **Caremark**, כי סיכוני סייבר ואבטחת מידע הם חלק מהנושאים שלגביהם חלה חובת ההשגחה:[6]

> "Delaware courts have not broadened a board's Caremark duties to include monitoring risk in the context of business decisions. Oversight violations are typically found where companies—particularly those operating within a highly regulated industry—violate the law or run afoul of regulatory mandates. **But as the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them. The corporate harms presented**

---

[2] *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996); ראו גם: *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).
[3] *Stone v. Ritter*, 911 A.2d 362 (Del. 2006)
[4] *Constr. Indus. Laborers Pension Fund v. Bingle*, (Del. Ch. Sept. 6, 2022)
[5] *Retirement System for Firefighters from St. Louis v. Sorenson et al.* (Del.Ch. Oct. 5, 2021)
[6] יצוין, כי באותו מקרה בית המשפט מצא כי הדירקטוריון נקט אמצעים מתאימים, ובשל כך פטר את הדירקטורים מאחריות לפי חובת ההשגחה. הנחיה זו נועדה להתוות את אמות המידה לקיום אמצעים כאלו ביחס לחובות המוטלות בישראל לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."

7. הפרת דין בידי תאגיד עומדת בשנים האחרונות במוקד של תביעות נגזרות רבות שהוגשו לבתי המשפט בישראל נגד דירקטורים, בטענה שהתרשלו בפיקוח על עסקי החברה לאחר שהוטלו על החברה קנס או סנקציה אחרת בשל הפרת דין בישראל או בחו"ל. רבים מההליכים הללו הסתיימו בפשרה.[7] אמנם אופן יישומה של פסיקת **Caremark** בישראל טרם הוכרע בפסיקה. אולם, בעקבות התייצבות היועץ המשפטי לממשלה בעניין **אהרוני**, שנדון בבית המשפט המחוזי בתל אביב, ובמסגרתו עלו שאלות דומות בדבר חובת ההשגחה של הדירקטוריון ואחריות הדירקטורים לנזק שנגרם לחברה באותו עניין, גילה בית המשפט המחוזי דעתו כי "**דומה שקביעה זו בעניין Caremark שהייתה נכונה וראויה כבר בשנת 1996 ראוי שתאומץ כאמת מידה ראויה ונכונה גם בישראל שנת 2021**".[8]

ההנחיה

8. כאמור, הנחיה זו חלה על חברות אשר עיבוד מידע אישי מצוי בליבת הפעילות שלהן,[9] או על חברות אשר פעילותן יוצרת סיכון מוגבר לפגיעה בפרטיות. זאת, בין בשל **מאפייני הארגון** (כגון חברות העוסקות בסחר במידע) ; בין בשל **סוג המידע המעובד על ידן ורגישותו**, כגון סוגי המידע המפורטים בפרט 1 לתוספת הראשונה לתקנות או בהגדרת "מידע בעל רגישות מיוחדת" בתיקון מס' 13 לחוק הגנת הפרטיות שאושר לאחרונה בכנסת[10] או מידע על אוכלוסיות מיוחדות כדוגמת קטינים ; ובין בשל **היקף המידע או מספר מורשי הגישה** אליו (ראו למשל כמות נושאי המידע ומורשי הגישה שנקבעו כמבססים רמת אבטחת גבוהה בתוספת השנייה לתקנות).

9. דירקטוריון חברה שמתקיים לגביה האמור בסעיף 8 לעיל, נדרש לוודא את קיומה של מדיניות בדבר אופן ביצוע דרישות החוק והתקנות בחברה, לרבות חובת הדיווח המיידי לרשות להגנת הפרטיות על קרות אירועי אבטחת מידע. המדיניות תתייחס בין היתר לאופן השימוש במידע אישי בחברה וניהולו בנושאים מהותיים[11], וכן תגדיר תהליכי פיקוח, בקרה, וציות אפקטיביים.

---

[7] ראו מעין ויסמן, אסף חמדני וקובי קסטיאל "התביעה הנגזרת בישראל – סיכום ביניים ומבט לעתיד" **משפט ועסקים** כד 769 (2021).

[8] פסק הדין בתנ"ג (ת"א) 17044-12-14 **אהרוני נ' בנק מזרחי טפחות** (11.5.2021). ראו גם את עמדת היועץ המשפטי לממשלה אשר הוגשה בינואר 2021 במסגרת אותו הליך.

[9] להבדיל מעיבוד מידע שרק **נלווה** לפעילות הליבה.

[10] חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, שאושר לאחרונה בכנסת ועתיד להיכנס לתוקפו ביום 14.8.2025, קובע קטגוריה חדשה של סוגי מידע המוגדרים "מידע בעל רגישות מיוחדת", ומשליכים בין היתר על גובה העיצום הכספי שיוטל בגין הפרת החוק או התקנות, על חובת מינוי ממונה הגנת הפרטיות בארגון, ועל חובת ההודעה לרשות בדבר מאגרי מידע גדולים ורגישים.

[11] להשוואה ראו גילוי דעת שפרסם איגוד הדירקטורים בישראל בשנת 2022 בנושא "**אחריות הדירקטוריון בנושא הסייבר**". ראו במיוחד נספח א' לגילוי הדעת, ובו נושאים נבחרים בהם ראוי כי יתקיים דיון בדירקטוריון, ונספח ג' שעניינו דוגמה לעקרונות מכוונים לתכנית אכיפה פנימית.

עוד על הדירקטוריון לוודא כי המדיניות מוטמעת בנהלי העבודה בארגון ולקבוע מיהם בעלי התפקידים האחראים על ביצועה. הדירקטוריון יהיה אמון על פיקוח שוטף וקבלת עדכונים ודיווחים על ביצוע החובות על פי התקנות בידי האחראים לכך בחברה. אימוץ תכנית אכיפה פנימית אפקטיבית הינו אחת הדרכים באמצעותן מתמלאת חובת הפיקוח המוטלת על הדירקטוריון, כמפורט לעיל.[12]

10. מבלי לגרוע מכלליות האמור, עמדת הרשות היא כי בחברה שמתקיים בה האמור בסעיף 8 לעיל הדירקטוריון הוא ככלל האורגן המתאים לביצוע החובות שלהלן, שהן פיקוחיות באופיין, ומוטלות לפי התקנות על החברה בהיותה בעלת מאגר מידע או מחזיקה במאגר, לפי העניין:

10.1. דיון במסמך הגדרות המאגר – בטרם הגדרתו הסופית בהתאם לאמור בתקנה 2(א);
10.2. דיון בעקרונות המרכזיים בנוהל אבטחת המידע הארגוני – בטרם אישורו וקביעתו הסופית בהתאם לאמור בתקנות 3(2) ו-4(א);
10.3. קיום דיון בתוצאות סקר סיכונים ומבדקי חדירות, לרבות בפעולות הנדרשות לתיקון הליקויים שהתגלו – כאמור בתקנות 5(ג) ו-5(ד);
10.4. קיום דיון רבעוני או שנתי, על פי רמת האבטחה של המאגר לפי התקנות, באירועי אבטחת המידע שהתרחשו בארגון – בהתאם לאמור בתקנה 11(ג);
10.5. קיום דיון בתוצאות הביקורת התקופתית בנוגע לעמידה בתקנות, שיש לקיימה אחת לשנתיים – בהתאם לאמור בתקנה 16(ג).

11. יחד עם זאת, במקרים המתאימים ובשים לב בין השאר למידת הסיכון לפרטיות הכרוך בפעילותה של החברה, לגודלה ולהרכב הדירקטוריון, ניתן בהחלטת דירקטוריון לקבוע גורם אחר בחברה שיהיה אחראי על ביצוע פעולות אלה, תוך פיקוח על קיומן בפועל. בהתאם לתקנה 19, על הדירקטוריון להבטיח כי מתקיים בחברה תיעוד סביר של הנימוקים להחלטתו זו, ושל אופן ביצוע יתר הפעולות הנדרשות על פי התקנות.

12. אין בהנחיה זו כדי לפטור או להפחית מהאחריות המוטלת על מנכ"ל החברה, הנהלת החברה, או כל גורם אחר שהוסמך לביצוע החובות על פי התקנות, מכוח תקנון החברה או על פי כל דין.

[12] ראו איתי משיח וצבי גבאי "תכניות אכיפה פנימית: על האתגרים העומדים לפתחו של הרגולטור הישראלי", **תאגידים** טז (2012), בעמ' 9. השוו גם: "קריטריונים להכרה בתכנית אכיפה בתחום ניירות הערך וניהול ההשקעות", אשר פורסמו על ידי רשות ניירות ערך (2011). הקריטריונים זמינים כאן.