מחלקת סייבר וטכנולוגיות מידע **ספטמבר 2023**

אחריות הדירקטוריון וההנהלה להיבטי פרטיות ואבטחת מידע בארגון

לקוחות יקרים,

ביום 7 בספטמבר 2023 פרסמה הרשות להגנת הפרטיות טיוטת הנחיה בדבר תפקיד הדירקטוריון בקיום חובות התאגיד בתחום הגנת הפרטיות.[1] לפי טיוטת ההנחיה, הרשות סבורה שבהתאם למקובל בדיני החברות בדבר אחריות הדירקטוריון ונושאי המשרה בחברה לניהול סיכוני החברה, אחריות זו חלה גם ביחס לסיכונים וחובות חוקיות ורגולטוריות בתחום הגנת הפרטיות ואבטחת המידע.

<u>טיוטת הנחיית הרשות</u>

הרשות סקרה את החקיקה והפסיקה בישראל ובארצות הברית בדבר אחריותם של הדירקטוריון ונושאי המשרה בחברה לעמידתה של החברה בהוראות החוק והרגולציה החלים עליה. לפי סקירה זו, הדין בארצות הברית מלמד שהדירקטוריון וההנהלה יכולים להיות אחראים לנזק שייגרם לחברה מעצם כך שלא עמדה בחובות הדין החל עליה, וזאת בשני מצבים עיקריים – האחד, כאשר הזניחו לחלוטין את הצורך בקיום תכנית ציות ובקרה לעמידה בהוראות אותם דינים, והשני, כאשר נמנעו במודע מלפקח על קיום הבקרות והתעלמו מדגלים אדומים בדבר הפרות.

בשים לב לסקירה זו, ובהיקש שערכה הרשות לדין הישראלי בשים לב להוראות חוק החברות והפסיקה, הרשות הגיעה למסקנה כי על דירקטוריון של חברה שמתקיימים בה תנאי מסוימים מוטלת האחריות להחליט מיהם האחראים בחברה על ביצוע דרישות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, לרבות חובת הדיווח המיידי לרשות להגנת הפרטיות על קרות אירועי אבטחת מידע; ליישם בחברה תהליכי פיקוח, בקרה, ציות, חובת עדכון ודיווח על ביצוע התקנות בידי אותם אחראים; ולקבוע החלטות מדיניות בדבר אופן השימוש במידע אישי בחברה וניהולו בנושאים מהותיים.

הרשות מבהירה כי תחולת חובה זו תהיה רק על חברות אשר עיבוד מידע אישי מצוי בליבת הפעילות שלהן, או על חברות אשר פעילותן יוצרת סיכון מוגבר לפגיעה בפרטיות. זאת, בין בשל מאפייני הארגון (כגון חברות ציבוריות או חברות העוסקות בסחר במידע); בין בשל סוג המידע המעובד על ידן ורגישותו; ובין

---

[1] https://www.gov.il/BlobFolder/reports/2023privacy_protection_regulations/he/Privacy%20protection%20regulations.pdf

בשל היקף המידע או מספר מורשי הגישה אליו.

באופן ספציפי, הרשות הבהירה כי הנושאים הבאים מצויים במסגרת חובת הפיקוח האמורה של הדירקטוריון:

- אישור מסמך הגדרות המאגרים של החברה;
- אישור העקרונות המרכזיים בנוהל אבטחת המידע הארגוני;
- קיום דיון בתוצאות סקר סיכונים ומבדקי חדירות, ואישור הפעולות הנדרשות לתיקון הליקויים שנמצאו בהם;
- קיום דיון רבעוני או שנתי, על פי רמת האבטחה של המאגר לפי התקנות, באירועי אבטחת המידע שהתרחשו בארגון;
- קיום דיון בתוצאות הביקורת התקופתית בנוגע לעמידה בתקנות;
- להבטיח כי מתקיים בחברה תיעוד סביר של ההחלטות המתקבלות בעניינים אלו.

בצד זאת, הרשות הבהירה כי במקרים המתאימים ובשים לב למידת הסיכון לפרטיות הכרוך בפעילותה של החברה, לגודלה ולהרכב הדירקטוריון, רשאי הדירקטוריון לקבוע גורם אחר בחברה שיהיה אחראי על ביצוע חובות אלה , תוך פיקוח על קיומן בפועל.

<u>סיכום</u>

אנו סבורים שטיוטת ההנחיה של הרשות מחדדת ומבהירה מצב משפטי קיים לפיו ניהול הסיכונים בתחום הפרטיות ואבטחת המידע בארגון מסור לדירקטוריון ולהנהלת החברה, ולהן החובה לקבוע את תהליך ניהול הסיכונים, הבקרות המתאימות לכן ולמנות ולהסמיך גורמים בארגון להוציא לפועל את תכנית הציות וניהול הסיכונים בתחומים אלו. הימנעות מניהול סיכון זה וקבלת החלטות מיודעת לגביו, עלולה להקים אחריות מסוגים שונים בהתאם לכללי הממשל התאגידי הנוהגים בישראל.

מחלקת הסייבר וטכנולוגיות המידע במשרדנו ליוותה לאורך השנים שורה ארוכה של ארגונים בתהליכי ציות וניהול סיכונים בתחום הגנת הפרטיות ואבטחת המידע, ומייעצת לדירקטוריון והנהלות בארגונים מובילים בישראל בתחומים אלו. נשמח לעמוד לרשותכם בכל שאלה בעניין זה.

למידע נוסף ניתן לפנות אל:

עו"ד עמית דת	adat@fbclawyers.com	03-6941320
עו"ד עמרי רחום-טוויג	orachum@fbclawyers.com	03-6941320

הכלול באגרת מידע זו הוא מידע כללי בלבד, הוא אינו חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו. כל הזכויות שמורות לפישר (FBC & Co.).
להירשם למייל זה או להסרה מרשימת התפוצה: news@fbclawyers.com