



אחריות הדירקטוריון בהיבטי פרטיות ואבטחת מידע

מועדון הדח"צים בשיתוף אונ' בר-אילן

עו"ד רבקה גניס שפטובסקי, שותפה



01 עיקרי דרישות הגנת הפרטיות בישראל

02 הנחיית הרשות – תפקיד הדירקטוריון

03 תיקון 13 לחוק הגנת הפרטיות

04 משמעויות

- "מידע אישי" ו-"מידע בעל רגישות מיוחדת"
- הודעה בעת איסוף המידע
- צמידות מטרה וצמצום מידע
- זכויות נושאי מידע
- מגבלות על מיקור חוץ והעברת מידע לחו"ל
- מינוי ממונה הגנת פרטיות וממונה אבטחת מידע



■ אבטחת מידע



■ מסמכים, אמצעים ורוטינות

■ חלוקה לרמות אבטחת

■ גיבוש מסמך הגדרות מאגר

■ אימוץ נוהל אבטחה

■ דיווח על אירועי אבטחה לרשות להגנת הפרטיות (בינונית/גבוהה)

■ ביקורת תקופתית – אחת ל-24 חודשים (בינונית/גבוהה)

■ עריכת סקרי סיכונים ומבדקי חדירות - אחת ל-18 חודשים (גבוהה)

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية



משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل



הנחיית הרשות להגנת הפרטיות מס' 1/2024:
תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות
(אבטחת מידע)



- חברות שעיבוד מידע אישי מצוי בליבת פעילותן
- חברות שפעילותן יוצרת קיים סיכון מוגבר לפגיעה בפרטיות
- סוג המידע
- היקף המידע
- מספר מורשי הגישה למידע
- דוגמאות: בנקים, חברות ביטוח, גופים מוסדיים, חברות
- תקשורת, חברות המעבדות מידע רפואי, מועדוני לקוחות עם
- מידע רגיש

■ פיקוח שוטף וקבלת דיווחים על ציות החברה לחוק הגנת הפרטיות והתקנות מכוחו

■ לוודא גיבוש, אימוץ ויישום של מדיניות ונהלים:

■ אופן השימוש במידע האישי בחברה וניהולו

■ הגדרת הליכי פיקוח, בקרה וציות אפקטיביים

■ חובת הדיווח המיידית לרשות להגנת הפרטיות על אירועי

אבטחת מידע

■ הגדרת בעלי תפקידים האחראים על ביצוע המדיניות



- מסמך הגדרות המאגר בטרם אישורו
- עקרונות נוהל אבטחת המידע בטרם אישורו
- תוצאות סקרי סיכוני אבטחת מידע ומבדקי חדירות, וכן הפעולות הנדרשות לתיקון הליקויים
- אירועי אבטחת המידע שהתרחשו בחברה
- תוצאות ביקורת התקופתית לעמידה בתקנות, אחת לשנתיים





- "במקרים המתאימים" ניתן לקבוע גורם אחראי בחברה שיהיה אחראי על ביצוע הפעולות, תוך פיקוח על קיומן בפועל
- פרמטרים:
 - מידת הסיכון לפרטיות מפעילות החברה
 - גודל החברה
 - הרכב הדירקטוריון
- יש **לתעד** את הנימוקים להחלטה הנ"ל ואת אופן ביצוע הפעולות הנדרשות על-פי התקנות



- מינוי ממונה הגנת פרטיות
- הרחבת חובת השקיפות באיסוף מידע אישי
- התאמת הגדרות ל-GDPR
- עיצומים כספיים משמעותיים
- הרחבת העילות לפיצוי בלא הוכחת נזק
- צמצום החובה לרישום מאגרי מידע

- עדכון מסמך הגדרות מאגר אחת לשנה – ₪ 160,000
- אי עריכת סקר סיכונים / מבדק חדירות או אי דיון בתוצאותיו – ₪ 320,000
- אי עריכת נוהל אבטחה בהתאם לנדרש בתקנות – ₪ 160,000
- היעדר דיון באירועי אבטחת מידע – ₪ 160,000
- אי דיווח על אירועי אבטחת מידע לרשות להגנת הפרטיות – ₪ 320,000
- אי ביצוע ביקורת תקופתית – ₪ 160,000

- ☑ אימוץ תכנית אכיפה לעמידה מתמשכת בהוראות החוק והתקנות מכוחו
- ☑ מינוי גורם אחראי במקרים המתאימים
- ☑ פיקוח שוטף של הדירקטוריון
- ☑ מעורבות פעילה וקיום דיונים עיתיים



תודה!



עו"ד רבקה גניס
שפטובסקי
שותפה
גורניצקי GNY

rebeccage@gornitzky.com

