

שאלון הערכה עצמית: האם העסק שלך מחויב במינוי DPO?

בחינת חובת מינוי ממונה על הגנת הפרטיות בהתאם לתיקון 13 לחוק הגנת הפרטיות

מנהלת יקרה,

תיקון 13 לחוק הגנת הפרטיות מביא עמו את הרפורמה המקיפה ביותר מזה עשורים בדיני המידע בישראל. אחד השינויים הדרמטיים ביותר הוא החובה החוקית למנות **ממונה על הגנת הפרטיות (DPO - Data Protection Officer)** בארגונים רבים במשק.

שאלון מקצועי זה נועד לסייע לך להעריך האם הארגון שלך נכנס תחת הגדרות החובה, או האם מומלץ למנות כפרקטיקה של ממשל תאגידי וניהול סיכונים. אנא סמן וי [✓] ליד כל היגד הרלוונטי לארגון שלך DPO

חלק א': סיווג הארגון ומהות משפטית

סמן הקריטריון החוקי

הארגון הוא **גוף ציבורי** (משרד ממשלתי, רשות מקומית, תאגיד סטטוטורי, גוף ביטחוני או גוף מבוקר כהגדרתו בחוק מבקר המדינה).

הארגון משמש כ**מחזיק או קבלן משנה** המעבד מידע בהיקף משמעותי עבור גוף ציבורי.

חלק ב': עיסוק עיקרי וסוג המידע המעובד בארגון

סמן	הקריטריון החוקי
<input type="checkbox"/>	העיסוק המרכזי של הארגון (Core Business) כולל עיבוד, איסוף או ניתוח של מידע אישי (המידע אינו רק לצרכים מנהלתיים פנימיים כמו שכר עובדים, אלא מהווה חלק ממוצר/שירות החברה).
<input type="checkbox"/>	הארגון מעבד " מידע בעל רגישות מיוחדת " כגון: מידע רפואי/בריאותי, מידע גנטי, נתונים ביומטריים, דעות פוליטיות, אמונות דתיות, או מידע על עבר פלילי.
<input type="checkbox"/>	הארגון מעבד נתונים פיננסיים רגישים , נתוני שכר, או חוות דעת מקצועיות להערכת אישיות (כגון חברות השמה, פלטפורמות אשראי או חברות פינטק).
<input type="checkbox"/>	הארגון אוסף או מעבד נתוני מיקום (Location Data) או נתוני תעבורה דיגיטליים של משתמשים כחלק קבוע מפעילותו.

חלק ג': היקף העיבוד, מעקב וטכנולוגיה

סמן	הקריטריון החוקי
<input type="checkbox"/>	פעילות הארגון כרוכה במעקב, ניטור או התחקות שיטתית אחר אנשים (לדוגמה: מערכות ניווט, אפליקציות בריאות, פרופילינג שיווקי מתקדם, עוגיות מעקב קבועות או מערכות הגנת סייבר המנטרות משתמשים).
<input type="checkbox"/>	העיבוד מתבצע ב" היקף ניכר " (מאגרי המידע של החברה כוללים נתונים של עשרות אלפי או מאה אלף נושאי מידע ומעלה, או שהעיבוד מכסה פלח אוכלוסייה רחב מאוד ברמה הלאומית/האזורית).
<input type="checkbox"/>	הארגון עוסק בסחר במידע או דיוור ישיר כדרך עיסוק מרכזית (Data Brokers / חברות שיווק מבוססות דאטה).

מטריצת פענוח תוצאות והנחיות פעולה

מצב 1: חובת מינוי חלוטה (מנדטורי על פי חוק)

אם סימנת לפחות קריטריון אחד בחלק א', או שסימנת שילוב של עיסוק עיקרי (חלק ב') יחד עם היקף ניכר/ניטור שיטתי (חלק ג') - הארגון שלך מחויב למנות ממונה הגנת פרטיות (DPO) באופן רשמי. אי מינוי מהווה הפרה ישירה של החוק וחשוף לעיצומים כספיים כבדים.

מצב 2: אזור סיכון רגולטורי גבוה (מומלץ מאוד)

אם סימנת היגדים בחלק ב' בלבד (עיבוד מידע רגיש) אך ההיקף אינו מוגדר כ"ניכר" באופן מובהק – החוק נתון לפרשנות מהותית של הרשות להגנת הפרטיות. מומלץ לקבל חוות דעת משפטית או למנות DPO מרצון כדי להגן על הדירקטוריון והנהלת החברה מאחריות אישית במקרה של דלף מידע.

מצב 3: פטור חוקי (ניהול סיכונים בסיסי)

אם לא סימנת אף היגד בשאלון, הארגון שלך ככל הנראה פטור מחובת מינוי DPO. עם זאת, עליך להמשיך ולעמוד בתקנות הגנת הפרטיות (אבטחת מידע) הרגילות החלות על כל מאגר מידע בישראל.

מסמך זה מהווה כלי עזר מתודי והערכה ראשונית בלבד בהתאם לנוסח תיקון 13 לחוק הגנת הפרטיות וטיוטות ההנחיה של הרשות להגנת הפרטיות. אין לראות במסמך זה או בתוצאותיו משום ייעוץ משפטי מחייב. מומלץ לבצע בדיקת התאמה מלאה (Gap Analysis) בליווי יועץ משפטי מומחה בתחום הפרטיות והסייבר.