

תיקון 13 לחוק הגנת הפרטיות - מתי חייבים למנות ממונה פרטיות ומה המשמעות לעסקים?

הכותב: רועי בסר, מנהל הגנת סייבר וממונה הגנת הפרטיות *

האם המידע של לקוחותיכם בטוח? זו כבר לא רק שאלה טכנולוגית אלא שאלה משפטית, עסקית ואתית מהמעלה הראשונה.

בעולם שבו מידע אישי ורגיש זורם בכל אינטראקציה עסקית, משרדי רו"ח, עורכי דין, חברות פיננסיות וארגונים מכל תחום הופכים לשומרי סף של פרטיות הלקוחות. כל אירוע אבטחת מידע אינו רק תקלה טכנית אלא פגיעה באמון, בחוסן העסקי ובמוניטין.

תיקון 13 לחוק הגנת הפרטיות, שנכנס לתוקף ב-2024, מגדיר מחדש את אחריות בעלי מאגרי המידע. הוא מטיל חובות חדשות וברורות - ובראשן **החובה למנות ממונה על הגנת הפרטיות (Data Protection Officer DPO)** במקרים מוגדרים.

מה השתנה?

- **חיזוק האחריות האישית של בעלי מאגרי מידע ונושאי משרה בכירה.**
- **חובת דיווח על אירועי אבטחת מידע** לרשות להגנת הפרטיות ולעיתים גם לנושאי המידע עצמם.
- **הטלת חובת מינוי DPO** בארגונים שמנהלים מידע רגיש או בהיקפים רחבים.

מתי החוק מחייב למנות DPO?

לפי תיקון 13 וטיוטת גילוי דעת שפרסמה הרשות להגנת הפרטיות (2025), קיימת חובה למנות ממונה במקרים הבאים:

1. **גופים ציבוריים** - משרדי ממשלה, רשויות מקומיות, מוסדות בריאות, קופות חולים, אוניברסיטאות ועוד.
2. **גופים העוסקים בסחר במידע** - כאשר מאגר המידע נועד למסירת מידע לצדדים שלישיים (בתמורה או כחלק מהפעילות העסקית), במיוחד אם כולל למעלה מ-10,000 נושאי מידע.
3. **גופים המבצעים ניטור שוטף ושיטתי של בני אדם** - למשל ספקי אינטרנט ותקשורת, מנועי חיפוש, אפליקציות למעקב מיקום, מערכות דירוג אשראי, חיתום ביטוחי או פרסום ממוקד.
4. **גופים המעבדים מידע בעל רגישות מיוחדת בהיקף ניכר** - בנקים, חברות ביטוח, מוסדות רפואיים או כל עסק שעיסוקו המרכזי כולל עיבוד נתונים בריאותיים, פיננסיים או אישיים רגישים אחרים בקנה מידה רחב. חשוב לדעת כי המונח "עיבוד בהיקף ניכר" נקבע לפי מכלול נסיבות כדוגמת מספר נושאי מידע, רגישות הנתונים, היקף ותדירות השימוש, ומשך שמירת המידע.

ומה אם לא ברור?

במקרים גבוליים, הרשות ממליצה על **מינוי וולונטרי**. גם כשאין חובה פורמלית מינוי DPO נחשב Best Practice והוא מחזק את עמידת הארגון בדרישות החוק, מצמצם סיכונים משפטיים ותפעוליים, ומקדם אמון מול לקוחות ורגולטורים.

מה תפקידו של ה-DPO?

- ייעוץ והכוונה להנהלה ולעובדים.
- פיקוח על סקרי סיכונים, בקורות גישה ונהלי אבטחת מידע.
- מתן מענה לפניית נושאי מידע (בקשות למחיקה, תיקון, הגבלת שימוש).
- נקודת קשר מול הרשות להגנת הפרטיות.
- הטמעת עקרונות **Privacy by Design** ותרבות פרטיות בארגון.

החיבור בין האתיקה המקצועית לחובת המינוי

כללי האתיקה של לשכת רואי החשבון בישראל קובעים כבר שנים כי רואה חשבון חייב לשמור על **סודיות המידע** המגיע אליו במסגרת עבודתו, ולנקוט צעדים סבירים כדי להבטיח שגם עובדיו ישמרו על חובה זו. עקרון זה מבוסס על ערכים של אמון, יושר ושקיפות מול הלקוח – ערכים שהם ליבת המקצוע.

תיקון 13 לחוק הגנת הפרטיות מחזק עקרון זה ומתרגם אותו לדרישה רגולטורית ברורה: במקרים בהם הארגון מחויב, עליו למנות **ממונה על הגנת הפרטיות**. הממונה הוא הגורם שמוודא כי חובת הסודיות וההגנה על מידע אישי מתורגמות למדיניות, נהלים ובקרה יומיומית.

בכך מתלכדים שני עולמות – **החובה האתית** מצד המקצוע והלשכה, ו**החובה המשפטית** מצד החוק. עבור משרדי רו"ח, המשמעות ברורה: מינוי DPO איננו רק עמידה בדרישה חוקית, אלא גם מימוש הערכים המקצועיים המחייבים את המשרד אל מול לקוחותיו.

המשמעות למשרדי רו"ח ולקוחותיהם

משרדי רו"ח מנהלים מדי יום **מידע פיננסי רגיש במיוחד** כדוגמת דוחות מס, נתוני שכר, הצהרות הון ופרטים אישיים.

- **למשרדים עצמם** - חובה לבחון האם היקף המידע מחייב מינוי DPO.
- **ללקוחותיהם** - חברות פיננסיות, טכנולוגיות או בריאות במקרים רבים אין מדובר בבחירה אלא בחובה חוקית. גם אם לא נדרשת חובה, מינוי כזה מהווה הצהרת אמון, שקיפות והגנה על הלקוחות.

חמש פעולות שכדאי לבצע כבר עכשיו

1. **מיפוי מאגרי מידע** - להבין איזה מידע מוחזק ומה היקפו.
2. **בחינת החובה למנות DPO** - לפי ארבעת הקטגוריות שבחוק.
3. **שקילת מינוי וולונטרי** - כהצהרת אמון כלפי הלקוחות.
4. **עדכון נהלי אבטחת מידע** - בהתאם לתיקון 13 ותקנות אבטחת המידע.
5. **תיעוד ובקרה שוטפת** - כל החלטה, מינוי או תהליך חייבים להיות מתועדים.

לסיכום

תיקון 13 לחוק הגנת הפרטיות הופך את ניהול המידע האישי מנושא "נלווה" - לאחד מעמודי התווך של פעילות עסקית אחראית.

החוק לא רק מחייב, אלא גם מסמן ללקוחות: מי שממנה DPO משדר שהוא מתייחס לפרטיותם ברצינות.

עבור משרדי רו"ח ולקוחותיהם, המשמעות כפולה:

- **הגנה משפטית** - עמידה בדרישות החוק והפחתת חשיפה לעיצומים כספיים.
 - **ערך עסקי** - שימור אמון הלקוחות, מוניטין חיובי והבלטת אחריות מקצועית.
- בסופו של דבר, מינוי ממונה פרטיות (DPO) הוא לא רק סעיף חוק – הוא **השקעה בהון האמיתי של העסק: אמון הלקוחות**.

*רועי בסר, בעל 30 שנות ניסיון באבטחת מידע, יועץ ניהול סיכונים סייבר לרשות שוק ההון, ביטוח וחסכון.