LALUM

מוכנות רגולטורית: תיקון 13 ו-EU AI Act

מה נכנס לתוקף, מה נמדד, ומה עולה כשזה לא נעשה. מדריך היערכות לגוף ציבורי ולארגון.

ספטמבר 2026
lalumapp.com/ai-legal-advisory/tools#regulatory-readiness/
ד״ר עו״ד אברהם ללום

מה השתנה, ומתי

תיקון 13 לחוק הגנת הפרטיות אושר בכנסת ב-5 באוגוסט 2024 ונכנס לתוקף ב-14 באוגוסט 2025. זהו השינוי המקיף ביותר בדיני הפרטיות בישראל מאז חקיקת החוק ב-1981. הוא מרחיב את סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות, מחליף את מנגנון הקנסות המנהלי הישן במנגנון עיצומים כספיים, מחייב מינוי ממונה הגנת פרטיות בגופים ציבוריים ובארגונים נוספים, ומרחיב את תקופת ההתיישנות על תביעה אזרחית משנתיים לשבע שנים.

העיצום אינו מספר אחד

זו הנקודה שהכי מרבים לפספס. חלק מההפרות נושאות סכום קבוע, וחלקן מחושבות לכל נושא מידע במאגר, לעיתים עם רצפה. אי-מינוי ממונה, למשל, מחושב לפי 2 ש״ח לכל אדם שמידע עליו נמצא במאגר, או 4 ש״ח במידע בעל רגישות מיוחדת, עם רצפה של 20,000 או 40,000 ש״ח. לפי שיעורים אלה, מאגר של 100,000 איש עם מידע רגיש מגיע ל-400,000 ש״ח. אי-ביצוע סקר סיכונים אחת ל-18 חודשים ואי-ביצוע מבדקי חדירות נושאים 320,000 ש״ח כשחלה על המאגר רמת האבטחה הגבוהה. המשמעות המעשית: ככל שהמאגר גדול יותר, כך הפרה שנשמעת טכנית הופכת מהר לחשיפה של מאות אלפי שקלים.

זה כבר לא תיאורטי

ביולי 2026 הטילה הרשות להגנת הפרטיות עיצום של 256,000 ש״ח על קופת חולים בגין איחור בדיווח על אירוע אבטחה חמור, העיצום הראשון מאז כניסת התיקון לתוקף. במקביל, החל מאפריל 2026 קיים מסלול חריג של התראה מינהלית במקום עיצום, אך הוא נתון לשיקול דעת ראש הרשות ואינו ברירת מחדל ואינו זכות של המפר.

המינוי אינו סוף הסיפור

לפי עמדת הרשות להגנת הפרטיות, מינוי מנהל מערכות המידע או ממונה אבטחת המידע לתפקיד הממונה מייצר ניגוד עניינים מובנה, וכך גם כפיפות לגורם שקובע את מדיניות עיבוד המידע. מינוי בניגוד עניינים, כפיפות שאינה תואמת, או מינוי בלי הקצאת זמן ומשאבים בפועל, הם עצמם הפרות. מינוי על הנייר אינו סוגר את הפינה, והוא עלול ליצור חשיפה חדשה במקום לסגור אחת.

מוכנות רגולטורית: תיקון 13 ו-EU AI Act

חמש השאלות שבהמשך הן מבדק מוכנות קצר. כל תשובה שאינה ״כן״ מסמנת פער, ולכל פער מצורף מה נשאל ומה עושים. את אותו מבדק אפשר להריץ באתר, ולקבל בסופו מפת פערים מותאמת.

שאלה 1

האם מערכות הבינה המלאכותית בארגון עברו סיווג מסודר לפי רמת הסיכון שהן מייצרות?

למה זה נשאל

בלי סיווג, כל המערכות מקבלות את אותה רמת בקרה: או שכולן חנוקות, או שאף אחת אינה מבוקרת. מערכת שנוגעת בקבלה לעבודה, באשראי, בשירות חיוני או בזכויות של אדם אינה באותה קטגוריה ככלי לניסוח טיוטות פנימיות.

מה עושים

מדרג סיכון לכל שימוש, לפי ההשפעה על מי שההחלטה נוגעת בו, ורמת בקרה, תיעוד ואישור שנגזרת ממנו. שיטת הסיווג של ה-EU AI Act משמשת כאן ככלי עבודה מוכן, ולא כמקור חובה.

שאלה 2

האם מונה ממונה הגנת פרטיות עצמאי, שאינו מנהל מערכות המידע ואינו ממונה אבטחת המידע?

למה זה נשאל

תיקון 13 לחוק הגנת הפרטיות, שנכנס לתוקף באוגוסט 2025, מחייב מינוי בגופים ציבוריים ובארגונים נוספים. לפי עמדת הרשות להגנת הפרטיות, מינוי מנהל מערכות המידע או ממונה אבטחת המידע לתפקיד מייצר ניגוד עניינים מובנה, וכך גם כפיפות לגורם שקובע את מדיניות עיבוד המידע. העיצום על אי-מינוי מחושב לפי מספר נושאי המידע במאגר, ולכן בארגון גדול הוא מגיע למאות אלפי שקלים.

מה עושים

מינוי בעל הכשרה מתאימה, במיקום ארגוני שמאפשר לו להתריע גם כלפי מעלה, עם זמן ומשאבים בפועל ולא רק בכתב המינוי. מינוי פורמלי שאינו עומד בכך פותר בעיה אחת ויוצר אחרת.

שאלה 3

האם נבחנים סיכוני הפרטיות של מערכת חדשה לפני הרכישה, ולא אחרי ההטמעה?

למה זה נשאל

בחינה שנעשית אחרי שהמערכת כבר עובדת אינה בחינה, היא הצדקה. זה נכון במיוחד למערכות שמעבדות מידע מזהה, מזהים ביומטריים או פרופיל התנהגותי.

מה עושים

בחינת סיכוני פרטיות כתנאי לרכישה, ולא כשלב אחריה. הממצאים שלה הם גם החומר שממנו נכתבים תנאי הסף במכרז וסעיפי החוזה מול הספק.

שאלה 4

האם מי שמדבר מול מערכת אוטומטית של הארגון יודע שהוא מדבר מול מערכת?

למה זה נשאל

חובת גילוי כזו טרם נקבעה בדין הישראלי, ובית המשפט העליון ציין שעשוי להיות היגיון בקביעתה בהקשרים שבהם ההשפעה על האדם גדולה. ארגון שמגלה מצמצם את פער הכוחות שעליו עמד בית המשפט, ומחזק את מעמדו אם ההתנהלות תיבחן.

מה עושים

החלטת הנהלה מתועדת על גילוי, ונוסח אחיד לכל הערוצים, ולא יוזמה של מחלקה בודדת. זו עלות נמוכה מול תועלת ברורה בביקורת.

שאלה 5

האם בוצעו בשנה האחרונה סקר סיכונים ומבדק חוסן למאגרי המידע שמזינים את המערכות?

למה זה נשאל

מידע שעובר למערכת חיצונית, ולעיתים לשרת מחוץ לישראל, מחייב בדיקה של אבטחת המידע, של מיקום השמירה ושל גישת ספקי משנה. זו גם החובה שנבדקת ראשונה אחרי אירוע.

מה עושים

סקר סיכונים ומבדק חוסן תקופתיים, ונספח אבטחת מידע מחייב בכל התקשרות עם ספק שמעבד מידע עבור הארגון.

איך לקרוא את התוצאה

בסיס מוסדר

הבסיס קיים. מכאן זו תחזוקה: בדיקה חוזרת אחת לתקופה, כי גם המערכות וגם הדין ממשיכים לזוז, ווידוא שמה שכתוב בנוהל מתקיים בפועל.

פערים שניתן לסגור

הפערים שסומנו הם ברובם עבודת נהלים, מיפוי ותיעוד, ולא החלפת מערכות. ארגון שמתחיל מהם סוגר את החשיפה המשמעותית בתוך רבעון.

חשיפה גבוהה

במצב הזה החלטות ותהליכים עלולים שלא לעמוד בבדיקה חיצונית, בין אם של רגולטור, של מבקר או של בית משפט. ההתחלה היא במיפוי, לא בהחלפת מערכות.

הכלים בעמוד זה מספקים מידע מקצועי כללי ואינם ייעוץ משפטי, אינם תחליף לבחינה פרטנית ואינם יוצרים יחסי עורך דין לקוח. תוצאת אבחון עצמי אינה חוות דעת.