

⚠ עידן האכיפה של תיקון 13 כבר כאן

מוכנים לתיקון 13? צ'קליסט 21 הבדיקות שכל מנכ"ל חייב לעבור

לפני שהרשות להגנת הפרטיות מגיעה אליכם: בדיקה עצמית בשלושה צירים — דיווח, ממונה ומסמכים, ואבטחת מאגרי מידע — עם ציון מוכנות בסוף.

₪10,000

תביעה ללא הוכחת נזק, לכל נפגע — לצד אחריות אישית לנושאי משרה

+100

תיקי אכיפה שמנהלת הרשות להגנת הפרטיות נגד גופים במשק

₪256,000

הקנס הראשון לפי תיקון 13 (יולי 2026) — על איחור בדיווח, לא על הפריצה

ציר ראשון: חובות דיווח ולוחות זמנים

הלקח מהקנס הראשון: איחור בדיווח לבדו — 256,000 ₪. הציר הזה קודם לכולם.

1

1. קיים נוהל כתוב לטיפול באירוע אבטחת מידע קריטי

מסמך מאושר על ידי ההנהלה — לא "ידע שבעל-פה" של איש המחשוב.



2. מוגדר מי מוסמך להכריז ש"זה אירוע" קריטי

שם ותפקיד. בלי בעל סמכות ברור — השעון הרגולטורי רץ בזמן שכולם מתלבטים.



3. נקבע לוח זמנים מחייב לדיווח לרשות

הרשות דורשת דיווח מיידי על אירוע חמור — לא אחרי סיום החקירה הפנימית.



4. ידוע מה מדווחים ובאיזה ערוץ

תבנית דיווח מוכנה מראש + הכרת מערכת הדיווח של הרשות להגנת הפרטיות.



5. מוגדר מתי ואיך מיידעים את נושאי המידע

באירועים מסוימים חובה ליידע גם את האנשים שמידע עליהם נפגע.



6. מוגדר דובר יחיד מול הרשות, הלקוחות והתקשורת

מסר לא מתואם באירוע = נזק תדמיתי ומשפטי כפול.



7. ההנהלה תרגלה אירוע לפחות פעם אחת (Tabletop)

נוהל שלא תורגל הוא נייר. תרגיל שולחני אחד חושף את רוב הפערים.



ציר שני: ממונה הגנת פרטיות ומסמכי חובה

2

תיקון 13 מחייב ארגונים רבים במינוי ממונה — וגם מי שפטור חייב להוכיח שבדק.

8. נבדק האם הארגון חייב במינוי ממונה הגנת פרטיות **קריטי**
בדיקה מתועדת בכתב — חוות דעת שמציגים בביקורת גם אם התשובה שלילית.

9. אם חלה חובה — מונה ממונה בפועל (פנימי או במיקור חוץ)
מיקור חוץ מותר במפורש; העיקר שהתפקיד מאויש ומתועד.

10. קיימת מדיניות פרטיות עדכנית — לאתר וללקוחות
משקפת את מה שקורה בפועל, לא תבנית שהועתקה מאתר אחר.

11. קיימים נהלים פנימיים: הרשאות, שימור ומחיקה, זכויות נושאי מידע
מי ניגש למה, כמה זמן שומרים, ואיך עונים לפניית "מחקו אותי".

12. העובדים עברו הדרכת פרטיות ואבטחה — ויש תיעוד
הדרכה מתועדת היא דרישה — ותיעוד ההדרכה הוא ההגנה שלכם בביקורת.

13. ההנהלה והדירקטוריון מקבלים דיווח תקופתי על ציות ופרטיות
תיקון 13 מטיל אחריות גם על נושאי משרה — דוח רבעוני מגן עליהם אישית.

14. נבחנו כלי ה-AI שבשימוש הארגון מזווית פרטיות
לאן נשלח המידע שמוזן ל-ChatGPT ודומיו? יש נוהל שימוש ב-AI לעובדים?

ציר שלישי: מאגרי המידע והאבטחה בפועל

3

אי אפשר להגן על מה שלא מיפית — והרשות בודקת קודם כל את התיעוד.

15. כל מאגרי המידע האישי ממופים ומתועדים קריטי

אילו מאגרים קיימים, מה יש בהם, איפה הם יושבים ולאן המידע זורם.

16. לכל מאגר יש מסמך הגדרות וסיווג רמת אבטחה

בסיסית / בינונית / גבוהה — לפי תקנות אבטחת מידע. הסיווג קובע את החובות.

17. הרשאות הגישה נסקרות תקופתית

עובד שעזב לפני שנה עדיין עם גישה? זה הממצא הראשון בכל ביקורת.

18. מוגדרת מדיניות שימור ומחיקת מידע — ומיושמת

מידע שלא צריך = סיכון שלא צריך. מחיקה מתועדת מקטינה חשיפה.

19. ספקים וצדדים שלישיים עם גישה למידע — ממופים ומחויבים חוזית

סעיפי אבטחה ופרטיות בחוזים + בקרה שוטפת על ספקים קריטיים.

20. נערך תסקיר השפעה על פרטיות (DPIA) לפני מערכת או תהליך חדש

מסמך שמוכיח שחשבתם על פרטיות מראש — הגנה מצוינת בדיעבד.

21. נערך סקר סיכונים אבטחת מידע בשנתיים האחרונות

סקר עדכני עם תוכנית טיפול מתועדת — הבסיס שהרשות והמבטחים מצפים לו.

הצ'קליסט מבוסס על חוק הגנת הפרטיות ותיקון 13, תקנות הגנת הפרטיות (אבטחת מידע), והנחיות הרשות להגנת הפרטיות — נכון לאוגוסט 2026. הוא כלי עזר ניהולי ואינו מהווה ייעוץ משפטי. לכל ארגון נסיבות משלו — מומלץ לבצע בדיקה פרטנית.

ציון המוכנות שלכם

ספרו כמה משבצות סימנתם ✓ מתוך 21 — והשוו:

מוכנות גבוהה — שמרו על זה

הבסיס איתן. השלב הבא: תרגול שנתי, בקרה רבעונית ועדכון שוטף מול הנחיות חדשות של הרשות.

21–18

מוכנות חלקית — הפערים ידועים לרשות

יש תשתית, אבל הפערים שסימנתם הם בדיוק מה שביקורת מוצאת. תעדפו את סעיפי ה"קריטי" — במיוחד בציר הדיווח.

17–12

חשיפה גבוהה — נדרשת פעולה מיידית

במצב הזה, אירוע אחד קטן יכול להפוך לקנס, לתביעות ולאחריות אישית של ההנהלה. אל תחכו לפנייה מהרשות.

11–0

 **שימו לב:** גם ציון גבוה עם פער אחד בסעיפי ה"קריטי" (1, 2, 8, 15) = חשיפה ממשית. הקנס הראשון בישראל ניתן לארגון גדול ומאובטח — על סעיף 3 בלבד.

סימנתם פחות מ-18? בואו נסגור את הפערים — לפני שהרשות תמצא אותם

שיחת הערכה עם יועץ בכיר, ללא עלות וללא התחייבות: נעבור יחד על התוצאות, נתעדף את הפערים לפי סיכון אמיתי, ותצאו עם תמונת מצב ברורה — גם אם תבחרו להמשיך לבד.

לתיאום שיחת הערכה: sec-it.co.il

LinkedIn: linkedin.com/in/idan-zabari · YouTube: @IdanZabari-sec-IT