לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA Israel - Institute of Internal Auditors

הכנס המקצועי השנתי של הביקורת הפנימית 2026

Internal Audit NextGen2.0

Fahn Kanne
Grant Thornton

תיקון 13 לחוק הגנת הפרטיות - עדכונים מהשטח

פברואר 2026

רו"ח חנן טויזר, CISA, CDPSE
שותף, פאהן קנה ניהול בקרה

Fahn Kanne
Grant Thornton

עיקרי התיקון

✓ צמצום בירוקרטיה

צמצום משמעותי בחובה הארכאית לרישום מאגרי מידע.

✓ שקיפות

חובת דיווח על מאגרי מידע המכילים מידע רגיש במיוחד.

✓ בעל תפקיד חדש

חובת מינוי ממונה הגנת פרטיות (DPO) בארגונים רלוונטיים.

✓ שיניים לרגולטור

הרחבה דרמטית של סמכויות הרשות להגנת הפרטיות (כולל סמכויות חקירה).

✓ הרתעה כלכלית

הגדלה משמעותית של הקנסות והעיצומים הכספיים על הפרת החוק.

Fahn Kanne
Grant Thornton

סמכויות אכיפה נרחבות

עיצומים כספיים

קנסות מנהליים היכולים להגיע למיליוני שקלים בגין הפרות הוראות החוק.

פיצוי ללא הוכחת נזק

בית המשפט רשאי לפסוק פיצויים לאזרחים שנפגעה פרטיותם גם ללא הוכחת נזק כלכלי.

אחריות אישית

מנהלים ודירקטורים חשופים לתביעות ואחריות אישית אם לא נקטו באמצעי פיקוח.

נזק תדמיתי

פרסום דבר הטלת העיצום הכספי עלול לגרום לגחם לפגיעה קשה במוניטין הארגון.

Fahn Kanne Grant Thornton

משמעויות כלכליות: מדרג העיצומים הכספיים

נושא	עיצום כספי בש"ח		
	מאגר שחלה עליו רמת אבטחה בסיסית	מאגר שחלה עליו רמת אבטחה בנונית	מאגר שחלה עליו רמת אבטחה גבוהה
הכנה / עדכון מסמך הגדרת מאגר	2000	40,000	160,000
בדיקת מידע עודף	2000	40,000	160,000
הכנה, שמירה ותיקוף נוהל אבטחת מידע	2000	40,000	160,000
סקר סיכונים ומבדק חדירה	-	-	320,000
הדרכת כוח אדם	1000	20,000	80,000
הרשאות גישה	2000	40,000	160,000
דיווח על אירוע אבטחת מידע	-	80,000	320,000
דיון תקופתי באירועי אבטחת מידע	-	40,000	160,000
עדכון מערכות מאגר	2000	40,000	160,000
בקרה ופיקוח על גורמים צד ג'	4000	80,000	320,000
ביקורות תקופתיות	-	40,000	160,000

Fahn Kanne
Grant Thornton

ממצאים מרכזים מתהליך פיקוח רוחב של הרשות להגנת פרטיות

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

תמונת מצב הגנת הפרטיות במשק: ניתוח ממצאי רוחב

ממצאים מרכזיים, מגמות ציות וסיכונים
רוחביים ב-11 מגזרי שוק עיקריים

מבוסס על דוחות פיקוח רוחב של הרשות להגנת הפרטיות (2020-2024)

הכנס המקצועי השנתי של הביקורת הפנימית 2026

לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA Israel - Institute of Internal Auditors

Fahn Kanne
Grant Thornton

המתודולוגיה: כיצד נמדדת בשלות ארגונית

הליך 'פיקוח הרוחב' אינו בדיקה נקודתית, אלא סקירה מערכתית שנועדה לאתר כשלים ענפיים ולהעלות את רמת הציות במשק. כל גוף נבחן תחת ארבעה קריטריונים מרכזיים:

בקרה ארגונית

קיום נהלים, מינוי ממונים, ומבנה ארגוני התומך בפרטיות.

ניהול מאגרי מידע

רישום מאגרים, הגדרת מטרות איסוף, וצמצום מידע עודף.

אבטחת מידע

עמידה בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

מיקור חוץ

פיקוח על ספקים חיצוניים והסכמי עיבוד מידע (תקנה 15).

Fahn Kanne
Grant Thornton

מפת החום המגזרית: רמת בשלות לפי מגזרים טרום תיקון 13

מבוסס על דוחות פיקוח רוחב של הרשות להגנת הפרטיות (2020-2024)

Fahn Kanne
Grant Thornton

הליקויים הנפוצים ביותר

הסכמים חסרים – מיקור חוץ
התקשרות עם ספקים ללא הסכם עיבוד נתונים (DPA) ואבטחת מידע.

אי-ביצוע הדרכות עובדים
הדרכות בנושאי הגנת פרטיות ואבטחת מידע, או היעדר תיעוד להדרכות.

שמירת מידע עודף
אגירת נתונים היסטוריים ללא צורך.

היעדר תיעוד אירועים אוטומטי (לוגים)
המאפשר ביקורת על הגישה למערכות.

סקרי סיכונים
אי ביצוע סקרי סיכונים למערכות המאגר בפרקי הזמן הנדרשים.

אי-ביצוע מבדקי חדירה
בתדירות הנדרשת (עבור מאגרים ברמת אבטחה גבוהה).

היעדר נהלי אבטחת מידע
קיומם של נהלים חסרים שאינם מכסים את דרישות התקנות.

הפרת חובת היידוע
אי-מתן הודעה כנדרש בעת איסוף מידע על מטרתו והזכויות לגביו.

פגיעה בזכות העיון
אי-מתן אפשרות נאותה לנושא המידע לעיין במידע המוחזק עליו

מנגנון הרשאות לקוי
מאפשר גישה רחבה מדי למידע שאינה לפי עיקרון "הצורך לדעת".

Fahn Kanne
Grant Thornton

כשל בשרשרת אספקה ומיקור חוץ

<u>כ-40% מהגופים שנבדקו אינם מבצעים פעולות פיקוח לווידוא עמידת הספק החיצוני בהוראות החוק וההסכם</u>

הכשל המרכזי
היעדר עיגון חוזי של חובות אבטחת מידע וחוסר פיקוח שוטף.

שכיחות הממצא
ליקוי רוחבי בולט במוקדים טלפוניים, תחבורה חכמה, ועמותות.

התוצאה
אובדן שליטה על המידע ברגע שהוא יוצא מהארגון.

"יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של ספק במיקור חוץ."

תקנה 15: ניהול ספקי מיקור חוץ – דגשים לטיפול

הבטחת שמירת המידע והפרטיות בעבודה עם ספקים חיצונים המקבלים גישה למאגר

מבדקי חדירה

במאגרים בעלי רמת אבטחה גבוהה קיימת חובה לביצוע מבדקי חדירה אחת ל-18 חודשים או לאחר שינוי טכנולוגי, אך נמצא גופים רבים אינם עומדים בכך.

320,000 ₪
קנס

<u>ממצא: יותר ממחצית מהגופים שנבדקו לא עמדו בהוראה זו באופן הנדרש</u>

תקנה 5(ד): מבדקי חדירה (PT) – דגשים לטיפול

סימולציה מבוקרת של התקפת סייבר על תשתיות ומערכות המחשוב של הארגון.

- **היקף:** המבדק יכלול את תשתית המאגר ואת המערכות התומכות.

- **תוצרים:** דוח מבדק חדירה מלא, תוכנית עבודה לטיפול בממצאים, ותיעוד הטיפול בפועל.

- **דיווח:** חובה לתעד את הצגת הממצאים להנהלה.

במאגרי מידע ברמת אבטחה גבוהה: חובה לבצע מבדק חדירה אחת ל-18 חודשים לפחות.

סקר סיכונים

במאגרים בעלי רמת אבטחה גבוהה קיימת חובה לביצוע סקרי סיכונים אחת ל- 18 חודשים, או לאחר שינוי טכנולוגי, אך גופים רבים אינם עומדים בכך.

320,000 ₪
קנס

<u>כ-35% מהגופים שנבדקו אינם מקפידים על עריכת סקרי סיכונים בפרקי הזמנים הקבועים בחוק</u>

תקנה 5(ג): סקר סיכונים (Risk Assessment) – דגשים לטיפול

זיהוי וניתוח סיכונים פוטנציאליים לפרטיות ואבטחת מידע במערכות המאגר.

- **היקף:** המבדק יכלול את תשתית המאגר ואת המערכות התומכות.

- **תוצרים:** דוח מבדק חדירה מלא, תוכנית עבודה לטיפול בממצאים, ותיעוד הטיפול בפועל.

- **דיווח:** חובה לתעד את הצגת הממצאים להנהלה.

בקרה ותיעוד גישה

80,000 ₪
קנס

תקנה 10 מחייבת ניהול מנגנון תיעוד אוטומטי (לוגים) שיכלול את זהות המשתמש, התאריך, השעה וסוג. נתונים אלו חייבים להישמר למשך 24 חודשים לפחות

<u>כ-65% מהגופים שנבדקו לא עמדו בהוראה זו</u>

תקנה 10: מנגנון תיעוד אוטומטי – דגשים לטיפול

מנגנון תיעוד אוטומטי של זהות המשתמש, זמן וסוג הגישה.

- המנגנון צריך להיות עצמאי ככל הניתן.
- חובה לקבוע נוהל בדיקה שגרתי.
- שמירת נתונים ל-24 חודשים.

Fahn Kanne
Grant Thornton

הדרך הנכונה ליישום התקנות

Fahn Kanne
Grant Thornton

תודה על ההקשבה!

חנן טויזר
שותף, מנהל מחלקת מערכות מידע וסייבר
Fahn Kanne Grant Thornton
050-8230209
Hanan.Twizer@il.gt.com