ציות אפקטיבי

ACC - פורום פרטיות וסייבר

Israel

Association of Corporate Counsel
ISRAEL

ליטל נוף סבג, יועמ"ש

Director of Legal, Head of IP & Product

Monday.com

אסף גלעד, יועמ"ש ו - DPO

Deputy GC, Director of Privacy & Compliance

Lusha.com

להצטרפות

מנהלים במשותף של פורום הסייבר והפרטיות

מהי תוכנית אכיפה?

1. מבוא - מהי תכנית אכיפה פנימית?

תכנית אכיפה פנימית הינה מנגנון וולונטרי אותו מאמץ ומיישם תאגיד באופן שוטף כדי לאתר ולמנוע הפרות ועבירות וכדי לוודא ציות של התאגיד ושל היחידים בו להוראות חוק ניירות ערך, התשכ"ח-1968 (להלן: "**חוק ניירות ערך**"), חוק השקעות משותפות בנאמנות, התשנ"ד-1994 (להלן: "**חוק השקעות משותפות בנאמנות**"), וחוק הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, התשנ"ה-1995 (להלן: "**חוק הייעוץ**") (לעיל ולהלן ביחד: "**דיני ניירות ערך**").

קריטריונים להכרה בתכנית אכיפה פנימית בתחום ניירות הערך וניהול ההשקעות

אוגוסט 2011

למה צריך תוכנית ציות

1. הגנה על הדירקטוריון ונושאי משרה (הנחיה 1/2024)
2. "תעודת מעבר" לעסקים בינלאומיים(GDPR & Adequacy)
3. מעבר מ"כיבוי שריפות" לניהול סיכונים
4. הוכחת הציות(Accountability)

'חלק א

תנאי הסף :המינימום המחייב

דרישות ה"מינימום "לפי תיקון 13 והרגולציה הבינלאומית

תחום	מקור חוקי: ישראלGDPR /	מה צריך לעשות בפועל
מינוי פונקציות וממשל	מינוי DPO סטטוטורי) סע' 17ט לחוק; סע' 37 ל-GDPR)	הגדרת כפיפות ישירה למנכ"ל, תקציב עצמאי, ואישור מדיניות בדרג דירקטוריון (לפי הנחיה 1/2024).
מיפוי נתונים (Data Inventory)	ניהול RoPA ופנקס מאגרי מידע מעודכן (כולל מטרות המאגר החדשות בתיקון 13).	מיפוי זרימת מידע ,(Data Flow) זיהוי ספקי משנה (Sub-processors)וסיווג מידע לפי רמות רגישות.
שקיפות + בסיס חוקי	חובת יידוע, פירוט בסיס משפטי (Legal Basis) ומטרות העיבוד.	עדכון מדיניות פרטיות (חיצונית ופנימית), הטמעת הודעות במועד איסוף המידע האישי, וניהול "הסכמות.(Consent Management) "
זכויות נושאי המידע	מימוש זכויות: עיון, תיקון, מחיקה (הזכות לְהִישָׁכֵחַ) וניידות המידע.	נהלים והליכים למימוש זכויות נושאי המידע
ייעוץ והדרכה	17ט מתן יעוץ והדרכה, ב Art.39 גם העלאת המודעות	קיום הדרכות ופעילויות להעלאת המודעות , זמינות ו SLAלייעוץ
ניהול סיכונים	חובת ביצוע תסקיר השפעה על הפרטיות) סע' 35 ל GDPR-ובקרות אבטחה בישראל.(	מיפוי סיכונים וניהול סיכונים
אבטחת המידע האישי	אבטחה "לפי רמת הסיכון) "סע' 32 ל (GDPR-ותקנות אבטחת מידע הישראליות.	ניהול הרשאות ,(RBAC) הצפנה במנוחה ובמעבר, ניטור לוגים (Logging)וביצוע מבדקי חדירות.(PT)
ניהול שרשרת אספקה	אחריות על מעבדי מידע (Processors) וחתימה על) DPA סע' 28 ל.(GDPR-	נספח פרטיות סטנדרטי לחוזים, שאלון אבטחה לספקים (Vendor Assessment)וביקורות מדגמיות על ספקים קריטיים.
Data Retention & Disposal	הגבלת תקופת השמירה למינימום הנדרש (Storage Limitation).	מדיניות מחיקה אוטומטית (Automated Deletion) או אנונימיזציה של מידע בתום תקופת ההתקשרות/התיישנות.

דוגמא של רשות מקומית Risk Matrix

	Negligible	Minor	Moderate	Significant	Severe
Very likely					
Likely			גישת ספקי צד ג'		חשיפת פרוטוקולים של ועדות השמה בגנים ובחינוך מיוחד
Possible		שמירת מידע גבייה	שימוש לרעה במצלמות	פריצה לפורטל תושבים (הנחות באנרונה מבוססות תלושי שכר, נכויות ומידע רגיש)	חשיפת תיקי רווחה
Unlikely				חשיפת פרטי שכר עובדים	דליפת אבחוני תלמידים
Very unlikely					

חלק ב'

מעבר מ"שוטר" ל"ארכיטקט"

למה מדיניות טובה לא תמיד עובדת?

כוונות טובות פוגשות כשלים תפעוליים

- קיימים נהלים, תבניות ומיפויים על הנייר
- בשטח: החלטות מתקבלות בזמן אחר ועל ידי אנשים אחרים
- נוצר פער בין "הצהרת כוונות" לבין "שליטה בפועל"

פערים נפוצים

- פרטיות נכנסת לאירוע בזמן הלא נכון
- התיישנות וחוסר במנגנון זיהוי שינויים
- מדיניות ללא גורם אחראי על ביצוע
- Silos

פרטיות כערך עסקי

- **מאיץ עסקי:** מאפשר שימוש בדאטה בביטחון ובמהירות.
- **שפה משותפת:** מחבר בין משפטי, מוצר, דאטה, אבטחה ורכש.
- **מקור אמת אחד:** בסיס להחלטות עקביות במערכות מורכבות.
- בניית אמון פנימי וחיצוני כחלק מההצעה העסקית.

כדי להביא להשפעה ארוכת טווח וחוצה פני ארגון, יש ליצור שפה משותפת בין אנשי הפרטיות ליחידות העסקיות בארגון

DPOכאדריכל תשתית

הגדרת התפקיד

- סמכות מקצועית, מוקד ידע וייעוץ להנהלה
- הכנה ופיקוח על תוכניות הדרכה לעובדים
- וידוא קיום נוהל אבטחה ומסמך הגדרות מאגר
- טיפול בפניות ומימוש זכויות בצורה נגישה
- שימוש כאיש קשר ישיר מול הרשות

אלו לא תיאורים של 'מאשר' - אלא של מי שמתכנן ומתחזק מערכת

בקרות נקודתיות מול ניהול כתשתית

בקרות נקודתיות

- החלטה לפי בקשה/צורך
- עבודה תחת זמן לחץ
- **תלות גבוהה באדם**
- תוצאה: חוסר עקביות, פספוסים

ניהול כתשתית

- קביעת "כללי משחק" קבועים
- מנגנונים מובנים מראש
- **תלות במערכת**
- תוצאה: החלטות צפויות, מעורבות בתהליכים ארגוניים

קל להגיד, קשה להטמיע: מה צריך כדי שתשתית פרטיות תעבוד

הבנה טכנולוגית

לדעת לשאול נכון: איפה נאסף/נשמר/נגיש/מועבר מידע?

מימוש פונקציונלי של הרשאות, לוגים, ריטנשן ומחיקה.

ממשק קבוע עם Security

תמונת מצב של אירועים, עדיפויות ושגרת עדכון הדדית

יצירת ממשק לבקרות, תיקון וזיהוי של אירועים רלוונטיים לפרטיות

ניהול ספקים מתמשך

זיהוי שינויי Scope כטריגר (ולא רק חתימת חוזה חד-פעמית)

שליטה טכנית (מינימיזציה/הרשאות/לוגים) ובקרה תקופתית בשטח.

הבנה של מערכות יחסים מורכבות עם מגוון צדדים שלישיים

תיעוד מעברי מידע וגורמים רלוונטיים

היכולת לחזור להחלטה ולעדכן אותה כשהמציאות או הטכנולוגיה משתנים

רדאר ארגוני

תשתיות ומסמכי בסיס

הגדרת הגבולות המשפטיים: נוהל אבטחה, מדיניות ותשתית נורמטיבית

מיפוי וניהול נכסי דאטה

ה"רדאר" הארגוני: מרשם מאגרי מידע (ROPA), מיפוי זרימת מידע וקטגוריזציה של נתונים

תפעול שוטף ובקרה

מנגנון מתמשך: תוכנית בקרה שוטפת, הדרכות צוותים וניטור, ממצאים בזמן אמת

ניהול ממשקים

ניהול הקשר עם השטח: טיפול בזכויות, נקודת קשר נגישה ודיווח שוטף לקו הנהלה

מיפוי חי: לא מסתפקים בצ'ק ליסט תקופתי

אירוע עסקי כטריגר

כניסה לשוק חדש,
אינטגרציה חדשה או שינוי
מהותי אצל ספק קיים

מסלול עבודה אוטומטי

הטריגר מוביל ל Intake-
שמזין אוטומטית את הרדאר
הארגוני

שגרה עסקית

פרטיות הופכת לחלק
מתהליכים עסקיים כברירת
מחדל

פרטיות פוגשת AI Governance

תכנון פרטיות - Privacy by Design

- **לא "בדיקה חיצונית":** חלק אינטגרלי מקבלת ההחלטות והפעלת המערכות
- תחום דינמי המשתנה ומתהווה בין ארגונים
- מעבר מבקרות נקודתיות לממשל **מובנה**

האתגר: מהירות וסקייל

- המרחק בין POC ליכולת התקצר
- פעולות שנוגעות בהיקף רחב של אנשים במהירות
- הסתמכות על בדיקה נקודתית או אישור של כל פעולה לא עובדים

כשהסיכון מאיץ – הממשל חייב להיות בתוך הטריגרים והמיפוי

מה מרוויחים כשפרטיות הופכת לתשתית

מהירות החלטות(Velocity)

פחות הפתעות מאוחרות ← החלטות מוקדמות ועקביות. ירידה בזמן לקבלת החלטה

פחות Rework וחיכוך

פחות תיקונים אחרי השקה ← מניעת עצירות "חירום" וירידה משמעותית בחיכוך בין הצוותים השונים

יכולת סקיילScalability)

הוספת ספקים ויוזמות עסקיות ללא צורך להמציא מחדש את התהליך בכל פעם. התשתית מוכנה לצמיחה

אמון כיכולת ניהולית

עקיבות + (Traceability) בעלות + בקרה. קל יותר להסביר ולהגן על החלטות

ה DPO-כמעצב: ארכיטקטורה לפני בקרה

התפקיד לא עוצר במסמך המשפטי:

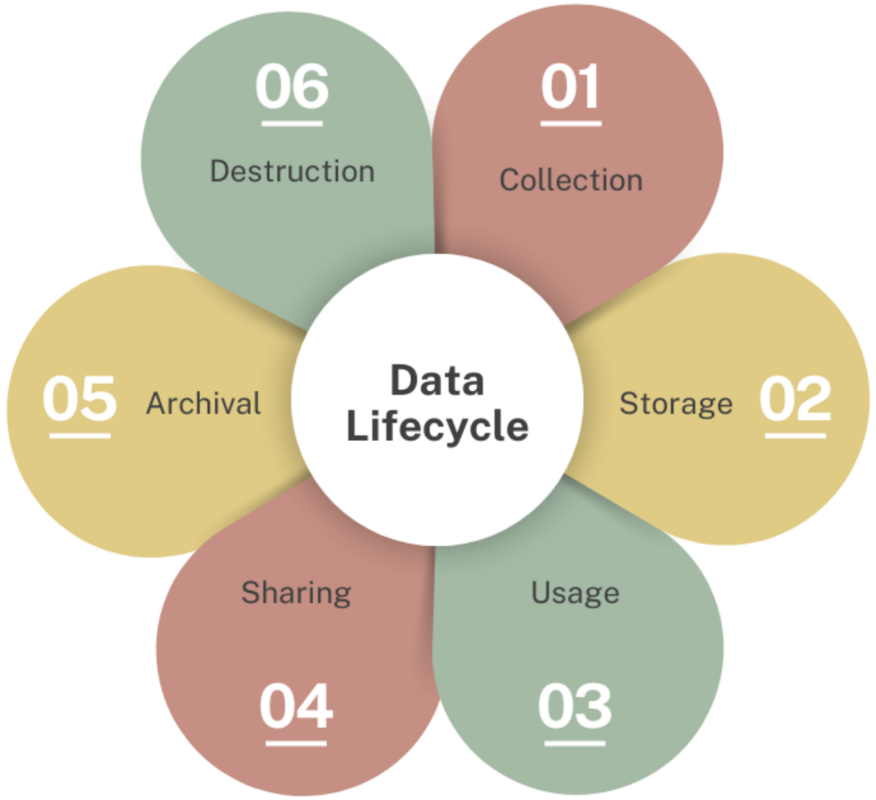
ניהול VS מסמכים: לא מספיק ליצור מדיניות; צריך לנהל אותה בתוך מערכות הארגון.

בנייה נכונה מהיסוד: ארכיטקטורה של הטמעת פרטיות (Privacy by Design) היא ליבת התפקיד.

מניעת כשלים מראש: כניסה לבקרה ללא תשתית ארכיטקטונית היא "כיבוי שריפות" כרוני.

ה DPO-כ Enabler: ה DPO-לא כאן כדי להגיד "לא", אלא כדי להגיד "איך כן, במינימום סיכון."

שלב האיפיון של המוצר) יחד עם ה (PM
כל מידע אישי שנאסף במהלך הפעילות העסקית צריך לקבל פירוט:



Data Protection

Impact Assessment

שלב האיפיון של המוצר) יחד עם ה(PM

שילוב ה DPO-במחזור חיי הפיתוח (**SDLC - Software Development Life Cycle**) הוא הדרך היחידה להפוך את ה **Privacy by Design**-מסיסמה למציאות הנדסית. ככל שהמעורבות מוקדמת יותר, כך עלות התיקון נמוכה יותר והחסינות המשפטית של הארגון גבוהה יותר.

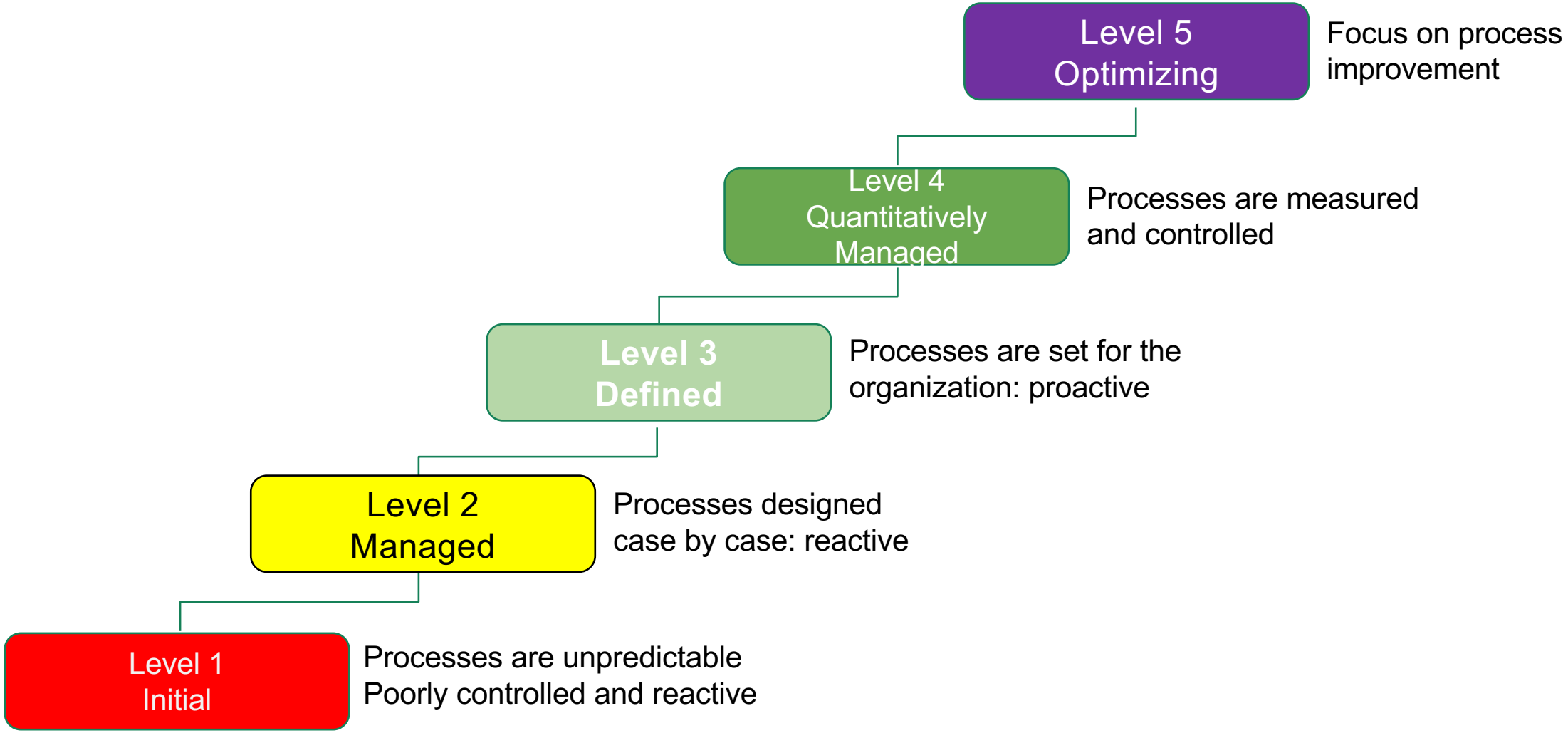
להלן פירוט של צמתי ההשפעה הקריטיים שבהם ה DPO-חייב להטביע חותם:

שלב בSDLC-	**פעולת הDPO-**	**התוצר המצופה**
שלב הייזום והדרישות (Requirements Phase)	הגדרת שדות מידע הכרחיים	מסמך דרישות פרטיות (Privacy Requirements)
שלב העיצוב והארכיטקטורה (Design Phase)	בחירת שיטת הצפנה והפרדה	אישור ארכיטקטורה מאובטחת
שלב הפיתוח והמימוש (Development Phase)	הדרכת מפתחים על ניקוי לוגים	קוד נקי מ PII-גלוי
שלב הבדיקות(Testing / QA)	הרצת תרחישי "תקיפת פרטיות"	דו"ח בדיקות פרטיות תקין
שלב ההשקה ותחזוקה (Deployment & Maintenance)	וידוא הודעת פרטיות מעודכנת	Privacy Noticeתואם מוצר

חלק ג'

סיכום

The Privacy & Security Maturity Plan (AICPA/CICA)



שאלות?

תודה רבה על השתתפותכם!

ACC Israel - פורום פרטיות וסייבר