תפקיד היועמ"ש ביישום תיקון 13 לחוק הגנת הפרטיות

עו"ד איתמר כהן

שותף וראש תחום רגולציה, פרטיות וסייבר, עמית, פולק מטלון ושות'

בשיתוף פורום סייבר ופרטיות של ה-ACC
בניהולם של ליטל נוף סבג, יועמ"ש Monday
ואסף גלעד, יועמ"ש Lusha

GET STARTED

על מה נדבר היום?

תיקון 13 - הרקע ועיקרי הדברים

האתגר - "ייעוץ משפטי" למול "ניהול הציות"

התהליך - אז איך ניגשים לנושא?

תחנות בדרך - נושאים שחייבים לכסות

סיכום - הצ'קליסט


13

תיקון 13 - הרקע ועיקרי הדברים

תיקון מס' 13 לחוק הגנת הפרטיות, התשמ"א-1981, ייכנס לתוקף ב־14 באוגוסט 2025 והוא צפוי להביא עמו את הרפורמה המשמעותית ביותר שנעשתה בחוק מאז חקיקתו לפני 44 שנים.

התיקון כולל:

- עדכון של הגדרות מיושנות וביטול חובות שאינן רלוונטיות עוד.
- חידוד והרחבה של חובות שתכליתן חיזוק הציות הארגוני.
- הרחבה ניכרת של סמכויות האכיפה של הרשות להגנת הפרטיות.

באופן כללי, ניתן לחלק את עיקרי השינויים להתאמת החוק הישראלי לסטנדרטים מודרניים ומקובלים בעולם וחיזוק משמעותי של כוחה של הרשות.

APM
& CO
AMIT, POLLAK, MATALON

צמצום חובת הרישום הארכאית

ביטול דה פקטו של חובת הרישום עבור רוב הגופים הפרטיים להוציא:

- מאגר המיועד למכירת מידע אישי - דאטה ברוקרס (מעל 10K).
- מאגר של גוף ציבורי (להוציא מאגר עובדים).

חידוש של חובת "הודעה לרשות" על מאגר לא רשום הכולל:

מידע רגיש על יותר מ־100,000 נושאי מידע - אמצעי המאפשר לרשות לדעת היכן למקד את הליכי הפיקוח והאכיפה.

אחידות רגולטורית - שינוי בהגדרות

"מידע אישי"

"עיבוד" /"שימוש"

"מידע בעל רגישות מיוחדת"

גישה למידע = עיבוד המידע

"בעל שליטה" /"מחזיק"

- קוקיז?
- פרטי קשר
- מידע עובדים

בתקנה 15 - גורם חיצוני

הרחבת חובת היידוע

הרחבת סעיף 11:

- זהות בעל השליטה ופרטי הקשר עימו.
- תוצאות אי הסכמה לאיסוף המידע .
- יידוע לגבי זכויות נושאי המידע (עיון ותיקון).

הגברת השקיפות כבסיס לאכיפה - קל יותר לרגולטור וכן לנושאי המידע.

חובת מינוי ממונה על הגנת הפרטיות

חובת מינוי ממונה על הגנת הפרטיות

<u>מי חייב:</u>

- גופים ציבוריים.
- דאטה ברוקרס (מעל 10K).
- מי "שעיסוקיו העיקריים כוללים...ניטור שוטף ושיטתי של בני אדם".
- מידע רגיש "בהיקף ניכר".

<u>תפקידיו:</u>

- מוקד ידע וסמכות מקצועית.
- הכנת תוכנית בקרה ומעקב אחר ביצועה.
- אחריות לקיומם של מסמכים שחובה להחזיק.
- איש קשר לפניות נושאי מידע ורשויות.

<u>היעדר ניגוד עניינים:</u> מנכ"ל , מנמ"ר / CTO / מנהל IT וממונה אבטחת מידע.


אכיפה,
אכיפה
ואכיפה

חיזוק מעמדו של הרגולטור והרחבת סמכויותיו

הסדרת מעמד הרשות להגנת הפרטיות:

- הרחבת סמכויותיה לבצע פעולות פיקוח וחקירה.
- הקניית הסמכות להורות על הפסקת שימוש במאגר מידע.
- הרחבת המסגרת הפלילית.

סמכויות להטיל עיצומים כספיים:

- עיצומים כספיים "פיקס" בגין הפרות מסוימות (עד 320K).
- עיצומים כספיים כנגזרת של כמות נושאי המידע.
- עיצומים כפולים במקרה של הפרה חוזרת או מתמשכת.

דוגמאות לעיצומים כספיים

- פנייה לאדם בבקשה למסירת מידע מבלי מתן גילוי מלא כנדרש בסעיף 11 לחוק, או שליחת דיוור שיווקי שלא כדין - בין 50-100 ש"ח לכל נושא מידע.

- "הכנת מסמך הגדרות המאגר..." או "עדכון מסמך הגדרות המאגר" אחת לשנה - עד 320K בהתאם להיקף מאגר המידע.

- מתן גישה למידע אישי או שינוי היקף הרשאה (מעבר בין תפקידים) ללא מתן הדרכה מתאימה לעובד - עד 160K.

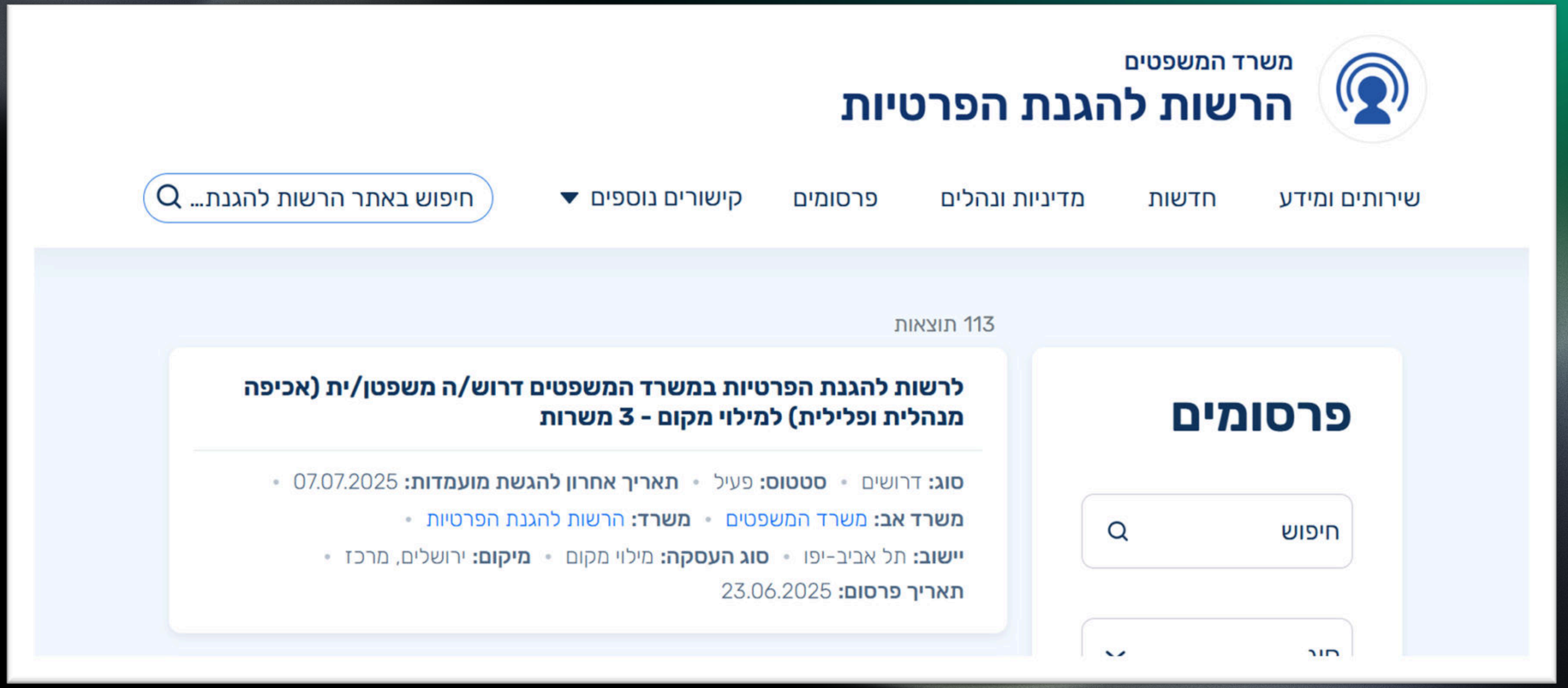
סכומי העיצומים - עונשי מינימום

"ראש הרשות אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים לפי סימן זה, אלא במקרים, בנסיבות ובהתאם לשיקולים המפורטים בתוספת החמישית ובשיעורים הקבועים בה".

דוגמאות מתוך התוספת החמישית:
"המפר הפסיק את ההפרה מיוזמתו ודיווח עליה לראש הרשות - בשיעור של 30%".

"ראה ראש הרשות, לגבי מפר שהוא יחיד, שההפרה נגרמה בשל נסיבות אישיות המצדיקות הפחתה של העיצום הכספי או שהתקיימו נסיבות אישיות קשות המצדיקות שלא למצות את הדין עם המפר, רשאי הוא להפחית למפר את סכום העיצום הכספי המוטל על המפר בשיעור של 20%".

עדיין לא השתכנעתם?



צילום: Shutterstock

הרשות להגנת הפרטיות קנסה את [redacted]: אספו ת"ז בניגוד לחוק

לאחר שברשות להגנת הפרטיות מצאו כי משרדי רואי החשבון מבצעים איסוף של תעודות זהות וסריקתן כתנאי לכניסת אורחיהן לבניין, הוחלט להטיל עליהן עיצום כספי של 15 אלף שקל

איתן גרסטנפלד | 11:46 25/03/2025

(1)

חברת האופנה [redacted] הציבה מצלמות ליד תאי הלבשה בלי ליידע הלקוחות – ונקנסה

על פי הרשות להגנת הפרטיות, החברה הציבה מצלמות בסניפים בקניון רמת אביב ובקניון שבעת הכוכבים, בין היתר בסמוך לתאי ההלבשה. הרשות קבעה כי מדובר בהפרה של חוק הגנת הפרטיות - מאחר שלא יידעה את הלקוחות על הצבת המצלמות

אורנה יפת 12:12, 06.07.25


CHALLENGE

"ייעוץ משפטי" VS "ניהול הציות"

הנושא משפטי, אך דורש שיתוף פעולה, מודעות ומידע שנמצאים אצל גורמים אחרים בארגון, והחובות משלבות בין:

- היבטים משפטיים - מסמכי מדיניות, הסכמות, הסכמים מול ספקים וכו'.
- היבטים טכניים - אבטחת מידע, ניהול נכסי טכנולוגיה, ניהול IT ובקרות וכו'.
- היבטים ארגוניים - נהלים, מסמכי מיפוי ושליטה, הדרכות, תרגול אירועי אבטחה וכו'.

לא מדובר בייעוץ אד הוק, אלא בניהול של ציות ובקרות בשגרה ובשוטף - נושא הגנת הפרטיות אינו רק רספונסיבי, אלא חייב להיות פרואקטיבי.

מטעמי יעילות, יש לקחת בחשבון רגולציות מקבילות (GDPR, US STATE LAWS, HIPAA) סרטיפיקציות קיימות (ISO 27001, SOC2) והליכי ארגוניים קיימים כדוגמת SOX ובקרות ITGC.

A P M
& C O
AMIT, POLLAK, MATALON

טכנולוגי

דרוש פרוייקטור

משפט

הפרויקט

הפרויקט - מבנה

<u>מיפוי:</u>

- זיהוי נכסי המידע מול כלל היחידות הארגוניות: מוצר ופיתוח, שיווק, מש"א, תמיכה, ביטחון וכו'.
- מיפוי טכנולוגי ומחשוב - ניהול IT .

<u>ריכוז כלל הממצאים ובניית תוכנית עבודה:</u>

- זיהוי הפערים.
- התאמת הפעולה המתקנת לכל פער - פתרונות משפטיים, ארגוניים וטכנולוגיים.

<u>יישום והטמעה:</u>

- ניהול התהליך והשלמת כלל הפעולות המתקנות.
- בניית כלל הדוקומנטציה המשפטית הנדרשת (בהמשך).
- פגישות סטאטוס עד להשלמה.

הפרויקט - מחויבות ומעורבות ארגונית

- פגישת הנעה למול גורמי ההנהלה הרלבנטיים:
  - תיאום ציפיות לגבי התהליך ושלביו
  - הבטחת שיתוף הפעולה מצד כולם
  - זיהוי כלל הדומיינים והתחומים הארגוניים - עם מי מדברים ועל מה?

- "אגרת מנכ"ל" לעובדים - ערך הצהרתי אבל גם מעלה את רמת המודעות הכללית לנושא.

- בסיום התהליך - פגישת הנהלה מסכמת, הצגת הצעדים שבוצעו ובארגונים רלבנטיים - הצגה לדירקטוריון.

הפרויקט - חלוקת תפקידים ותחומי אחריות

לאחר השלמת שלב המיפוי והבנת כל הפערים, מומלץ להכין תוכנית עבודה מסודרת וביחס לכל "ממצא ופעולה מתקנת" להגדיר מיהו בעל התפקיד הפנימי המוביל את הטיפול:

	תקנה / סעיף חוק רלבנטיים	ממצא	פעולה לביצוע	אחריות לביצוע
משפטי ונהלים	תקנה 2 לתקנות הגנת הפרטיות (אבטחת מידע), 2017 ("התקנות")	לא קיימים בחברה מסמכי הגדרות המאגר והמסמכים אינם מעודכנים מטבע הדברים אחת לשנה כנדרש בתקנות אבטחת מידע	יש להכין מסמכי הגדרות המאגר בחברה, לכל הפחות ביחס למאגר המצלמות, העובדים ומאגר הלקוחות בהתאם לפורמטים שפירסמה רשות הגנת הפרטיות.	x
	תקנה 5 לתקנות	לא קיים מסמך מיפוי מערכות המאגר כדרישת התקנות. קיימות רשימות מצאי אולם יש להשלים את כל הנדרש לרבות תרשים טופולוגיית רשת.	החברה באמצעות מחלקת המחשוב, על החברה להחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה: (1) תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע; (2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;	x
ספקים חיצוניים	תקנה 15 לתקנות אבטחת מידע והנחיה 2/2011 של רשות הגנת הפרטיות	הרגולציה מחייבת כל ספק חיצוני לחתום על הסכם עיבוד מידע לפי תקנה 15 והנחיה 2/2011 של רשות הגנת הפרטיות. החברה עושה שימוש במערכת ERP תפעולית של Comax עם שמירת מידע בענן הספק. המידע האישי הרלבנטי בסיסי.	יש להכין ולהחתים את הספק על הסכם עיבוד מידע - סיכון יחסית מתון בשל אופי המידע האישי.	x
	תקנה 15 לתקנות אבטחת מידע והנחיה 2/2011 של רשות הגנת הפרטיות	הרגולציה מחייבת כל ספק חיצוני לחתום על הסכם עיבוד מידע לפי תקנה 15 והנחיה 2/2011 של רשות הגנת הפרטיות. החברה עושה כיום שימוש במערכת תפעולית של NCR. מערכת זו כיום אינה מכילה מידע אישי אבל אמורה בעתיד לשמש לניהול מועדון הלקוחות ומאגר לקוחות החברה	בעתיד וטרם תחילת שמירת מידע אישי במערכת - יש להכין ולהחתים את הספק על הסכם עיבוד מידע.	x
אבטחת מידע	תקנה 13(ג) לתקנות אבטחת מידע	בחברה קיים שימוש במערכות הפעלה (עמדות ושרתים) ישנות שאינן נתמכות בהיבטי אבטחה על ידי יצרן המערכת. מדובר בחולשת אבטחה מהותית ובהפרה של התקנות.	יש לבנות תוכנית סדורה להחלפת ועדכון המערכות הישנות - החלופה - סגרגציה לרשת מבודדת	x
	תקנות 8 ו- 9 לתקנות אבטחת מידע	הרגולציה דורשת סיסמא אישית בכניסה למערכות מחשב וכן החלפה תקופתית. לא ברור האם במערכות התפעוליות הדבר קיים.	יש לוודא בשתי המערכות קיומן של סיסמאות גישה אישיות עם החלפה תקופתית.	x
מודעות עובדים	תקנה 7 לתקנות אבטחת	התקנות מחייבות ביצוע הדרכה ראשונית לעובד טרם קבלת גישה למשאבי מחשוב. כיום אין הדרכה.	יש לשלב הדרכה ראשונית בתליך הקליטה	x
	תקנה 7 לתקנות אבטחת	התקנות מחייבות ביצוע הדרכת אבטחה לכלל עובדי הרשת המקבלים גישה למשאבי מחשוב, לכל הפחות אחת ל- 24 חודש. הרשת אינה עושה היום הדרכות אבטחה.	יש לוודא כי אחת לשנתיים מבוצע הדרכה לכלל העובדים ונשמר תיעוד לגבי המשתתפים	x
	תקנה 3 לתקנות אבטחת מידע	הרגולציה מצפה כי בארגון תהיה קיימת תוכנית עבודה סדורה לפרטיות ואבטחת מידע הכוללת בקרות והליכים תקופתיים. בחברה לא קיימות תוכנית כתובה.	מומלץ להטמיע גאנט פעילות שנתית בתחום	x


אז על מה בעצם
עוברים?

חובת מינוי DPO

בחינת החובה בהתאם לפעילות הארגון והמידע שהוא מחזיק:

"מי שעיסוקיו העיקריים כוללים פעולות עיבוד מידע או כרוכים בפעולות כאמור, אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם....".

"עיבוד מידע בהיקף ניכר יהיה בין השאר בשים לב למספר בני האדם שמידע מעובד לגביהם, לשיעורם באוכלוסייה מסוימת, להיקף המידע, לכמותו ולטווח של סוגי המידע המעובד, למשך ולתדירות של פעולות העיבוד, למשך שמירת המידע ולתחום הגאוגרפי של פעולות העיבוד".

חובת מינוי DPO

איתור בעל תפקיד מתאים / התקשרות עם גורם חיצוני - "ובכלל זה ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע והיכרות עם תחומי פעילותו של הגוף..." - נדרש סופרמן!

האם ממונה אבטחת מידע יכול לכהן גם כממונה על הגנת הפרטיות?

- בעל תפקיד שמחזיק בידע הדרוש לשני התפקידים (משפטי-ארגוני-טכנולוגי).
- העדר ניגוד עניינים ודיווח ישיר לרמת מנכ"ל/סמנכ"ל.
- "בארגונים גדולים או ארגונים בעלי היקף גדול של פעילות עיבוד מידע אישי, תפקיד הממונה על אבטחת המידע נושא באחריות כבדה ומצריך את תשומת ליבו המלאה של בעל התפקיד, באופן שלא יאפשר לו ככלל למלא בצורה נאותה גם את תפקיד הממונה על הגנת הפרטיות".

לא לשכוח - הוצאת כתב מינוי או לחלופין תיעוד בכתב של הניתוח המשפטי שהוביל להחלטה לא למנות.

מוצר/שירות - היבטים כלליים ומשפטיים

איזה מידע נאסף?
פרטי קשר, מידע משתמשים, מידע מהותי הקשור לשימושיות המוצר, מידע רגיש או אודות ילדים, אנליטיקה וכו'.

באיזה כובע?

- B2B VS B2C.
- בעל שליטה (קונטרולר) VS מחזיק (פרוססור).

מה עושים במידע? האם קיים שימוש שניוני?
מגבלות על שימוש נובעות הן מהוראות החוק והן מהמסגרת החוזית מול הלקוחות (עסקיים או פרטיים).

מדיניות פרטיות / הסכם עיבוד מידע לטובת הלקוחות

פרקי שמירת המידע (RETENTION)?

מוצר/שירות - ספקים ואבטחת מידע

- היכן המידע מאוחסן ובאילו מדינות? תקנות העברת מידע
- מהם הספקים המעורבים בתהליך? לרבות שימוש בצוותי פיתוח חיצוניים (OFFSHORING)
- PRIVACY BY DESIGN
- שמירת לוגים - תקנה 10 חלה גם על מחזיק בצורה ישירה
- הליכי פיתוח מאובטח ו- SSDLC

שיווק

<u>מהם ערוצי איסוף המידע ומהן הפרקטיקות השיווקיות?</u>
פרסום כללי, פנייה ישירה, רכישת מאגרי מידע וכו'.

<u>באילו כלים משתמשים?</u>
CRM ארגוני, מערכות דיוור וכו'.

<u>אתר האינטרנט:</u>
- עדכון מדיניות פרטיות בהתאם לסעיף 11 החדש.
- טיפול בנושא הקוקיז שנכנס בהגדרת "מידע אישי" לאחר התיקון - בוובינר שהעבירה הרשות באפריל הודגש כי לאחר התיקון יחולו על קוקיז דרישות החוק לעניין הסכמה - כיצד ובאיזה אופן? לרגולטור פתרונות.

דיוור שיווקי ומועדוני לקוחות

- מי הקהל המדובר? מהו מקור "רשימות הדיוור"?
- האם קיים תיעוד למקור של כל הרשימות?
- דרישות צורה - לוודא שמבוצע בהתאם לדרישות הצורה שבחוק עם תיעוד וניהול "הסרה" כנדרש.
- ככל ומסתמכים על החריג המאפשר שליחת דיוור ללקוח קיים ב- OPT OUT - לוודא שניתנים הגילויים כנדרש.
- מועדוני לקוחות:
  - האם ניתן גילוי כדין - האם קיימת מדיניות פרטיות המכסה את הליך הרישום למועדון?
  - מהן מטרות השימוש - להקפיד על עיקרון "צמידות המטרה" (המופיע גם בחריג לסעיף 30א לחוק הבזק).

שיווק

יש לזכור שעל מאגרי המידע הכוללים מידע שמקורו באירופה עלולות לחול גם תקנות הגישור:

- חובת מחיקה לבקשת נושא המידע - הרחבת החובה שחלה כיום רק לגבי דיוור ישיר.
- חובת יידוע - חובת הגילוי מורחבת ביחס לדין הקיים.
- מחיקת מידע עודף - (להלן)
- חובת דיוק המידע - באמצעות מנגנון ארגוני ייעודי, גם ללא פנייה מצד נושא המידע.

מחיקת לידים:

- קהל ישראלי - לוודא מחיקה של מידע "רב מן הדרוש" לצורכי תקנה 2ג.
- קהל אירופאי/מעורב - "בעל מאגר מידע יפעיל מנגנון ארגוני, טכנולוגי או אחר, שמטרתו להבטיח כי במאגר המידע לא מוחזק מידע שאינו נחוץ עוד למטרה שלשמה נאסף או הוחזק או למטרה אחרת שלשמה מותר להחזיקו לפי כל דין".

מחשוב

האם קיימים המיפויים הנדרשים כהוראת תקנה 5 - מיפוי מערכות המאגר?

חובות כלליות לאבטחת מידע בהתאם ל- BEST PRACTICES:

- "אחראי לאבטחת המידע שבמאגר" (סעיף 17 לחוק).
- "ינקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו" (תקנה 9).
- "...בשים לב לסיכונים" (בכמה וכמה תקנות).

ולצד זה חובות פרטניות, כדוגמת סיסמא מורכבת עם החלפה תקופתית, ניתוק אוטומטי באי פעילות (שומר מסך ו- SESSION TIMEOUT), ניהול הרשאות גישה, אבטחה פיזית, אבטחה לוגית, מדיניות שימוש ב- USB וכו'.

הדרכות, מודעות עובדים, מבדקי פישינג וכו'.

תקנה 10 - שמירת לוגים ותיעוד

תקנה 10 - חובת שמירת לוגים ותיעוד:
"במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו - מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה".

הנחיית הרשות (מדריך פעולה) מספטמבר 2024 מרחיבה מאוד את החובה:

- מהו היקף החובה? כוללת לא רק את מאגר המידע אלא גם את מערכת ההפעלה וכל מערכות הניהול והאבטחה.
- התקנה דורשת "נוהל בדיקה שגרתי" בעוד שהנחיית הרשות בפועל שואפת למערכת SIEM/SOC הכוללת ניטור רציף.
- הנחיית הרשות דורשת אחסון מקומי (??) במשך 6 חודשים.

ניהול עובדים

מערכות ניהול מידע עובדים - שכר, נוכחות, ניהול תיקי עובד, ESOP, פנסיה וזכויות סוציאליות וכו'.

גילוי לעובדים (סע' 11) - במסגרת הסכם ההעסקה או מדיניות פרטיות לעובדים.

ניהול נוכחות ביומטרית - הנחיית הרשות (איסוף ושימוש במידע ביומטרי לדיווח ולבקרת נוכחות עובדים במקום העבודה).

מעקב אחר עובדים:

- הלכת איסקוב לעניין חדירה למייל
- הנחיית הרשות לעניין בקרה על עבודה מרחוק
- רכבי עבודה

גיוס והשמת מועמדים לעבודה

האם קיימת מערכת גיוס?

- האם נעשה שימוש בחברות השמה חיצוניות - האם נחשבות למעבד מידע או בעל שליטה עצמאי (האם נדרש הסכם)?
- ביצוע בדיקות רקע למועמדים
- גילוי מתאים למועמד

הנחיית הרשות לעניין "הליכי מיון לקבלה לעבודה ופעילות מכוני מיון":

- מחיקת קורות חיים שנפסלו
- שמירה ושימוש למשרות עתידיות
- זכות העיון במידע הקשור לגיוס

מצלמות וביטחון

- הנחיית הרשות לעניין צילום במרחב הציבורי - מיפוי מצלמות, נוהל ותהליך מתועד וכו' - האם הקב"ט בכלל מכיר? האם קיים נוהל?
- חובת שילוט ויידוע
- הנחיית הרשות לעניין שימוש במצלמות מעקב במקום העבודה - היעדר צילום של עובדים ב"משרד" ויידוע
- לכמה זמן התמונות נשמרות? מתכתב עם זכות העיון
- שימוש במצלמות הכוללות ניטור או זיהוי ביומטרי

ספקים חיצוניים - תקנה 15 והנחיה 2/2011

- זיהוי כלל הספקים הרלבנטיים - רלבנטי לכלל הגורמים והתחומים - חשוב בהליך המיפוי להבין מכל אחד עם אילו מערכות הוא עובד, באיזו תצורה וכו'.

- קיומם של הסכמי עיבוד מידע עם כלל הספקים הרלבנטיים.

- קיומו של הליך ההתקשרות לפי הנחיה 2/2011 באופן מתועד.

- קיומם של הליכי בקרה תקופתיים ומתועדים.

היבטים ייחודיים לארגון

- קיומה של פעילות ריטייל או הפעלת אתרי מסחר מקוון
- עיבוד מידע רגיש - רפואי, עובדים, פיננסי וכו'
- הפעלת חנויות ו/או שטחים ציבוריים בהיקף נרחב (מלונאות, קניונים, רשתות וכו')
- חפיפה לרגולציות סקטוריאליות - בנקאות, ביטוח, רפואה וכו'

נהלים - פרקטיים למול "נהלי מדף"

- "מדיניות אבטחת מידע" - נוהל האמור לכסות את מרבית הנדרש בתקנה 4
- "נוהל אבטחת משאבי אנוש" - הליכי גיוס, קליטת עובדים, סיום העסקה, ניוד בין תפקידים ומודעות ארגונית
- "נוהל אירועי אבטחת מידע"
- נוהל התקשרות עם ספקים"
- נוהל מענה לנושאי מידע"
- "נוהל מצלמות"

הצ'קליסט

מסמכי חובה ותיעוד נדרש

- מסמכי הגדרות המאגר (תקנה 2) - חובה לעדכן לכל הפחות אחת לשנה כולל התייחסות לתקנה 2ג וחובת מחיקת מידע עודף
- מיפוי מערכות המאגר (תקנה 5)
- מיפוי ספקים ותיעוד של הליכי התקשרות ובקרה תקופתיים
- הסכמי עיבוד מידע עם כלל הספקים
- נוהל אבטחת מידע (תקנה 4) - כולל מעקב שינויים ותאריכי עדכון (שנתי)
- טפסי טיולים קליטת עובדים, סיום העסקה ומעבר בין תפקידים
- תיעוד הדרכות, לרבות תוכן ההדרכה ורשימת משתתפים
- פרוטוקולים של דיונים תקופתיים
- כתבי מינוי עבור ממונה אבטחת מידע ו/או הגנת הפרטיות
- תיעוד הליכי בקרה תקופתית, מבדקי חדירות וסקרי סיכונים, הטיפול בהם והצגתם להנהלה
- תיעוד של כל אירוע אבטחת מידע

תוכנית עבודה שנתית

- גאנט שנתי, המתייחס לכלל הפעילות בתחום לאורך שנה, עם חלוקת תפקידים ותחומי אחריות.
- בקרות שוטפות תקופתיות - בתחום ה- IT, קליטת עובדים וסיום העסקה, מודעות והדרכת עובדים, בקרה על אתרי האינטרנט וכו'.
- מבדקים תקופתיים (24 חודש), סקרי סיכונים ומבדקי חדירות (18 חודש).
- עדכון שנתי של מסמכים - מסמכי הגדרות מאגר ונוהל אבטחת מידע.
- דיונים תקופתיים - שנתי/רבעוני באירועי אבטחה כנדרש בתקנות.
- דיון הנהלה ודירקטוריון - מצגת לצורך רתימה וקיום חובת הפיקוח לפי הנחיית הרשות בעניין.

תודה רבה!

שמרו על קשר

 itamarc@apm.law