יולי 2025

לשכת המבקרים הפנימיים IIA ישראל מפרסמת בזאת קווים מנחים מטעמה ובהם הנחיות מוצעות לביצוע ביקורת פנימית בהיבטי אבטחת מידע שעל בעל שליטה במאגר ומחזיק מאגר לבצע בהתאם לחוק הגנת הפרטיות ותיקוניו (תיקון 13) ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז 2017 (להל ביחד: "החוק").

הקווים המנחים יכולים לשמש ככלי עזר להבהרת התקנות ואינם מהווים תחליף לצורך קביעת תוכנית הביקורת הלכה למעשה.

המסמך המקורי חובר ביולי 2020 ועודכן ביוני-יולי 2025 לאור שינויי חקיקה אשר כניסתו לתוקף מאוגוסט 2025, וזאת ע"י מאיה ויסמן, רו"ח איה שטיינר ורו"ח ורד ישראלוביץ, חברות הוועדה המקצועית בלשכת המבקרים הפנימיים IIA ישראל, ואושר על-ידי הוועדה המקצועית.

בברכה,

דורון רונן, רו"ח

MA, LLM, CIA, CRMA, QAR, CRISC, CSX-F, CDPSE, CFE

יו"ר הוועדה המקצועית, נשיא

לשכת המבקרים הפנימיים IIA ישראל

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

קווים מנחים מס' 2

קווים מנחים לביצוע ביקורת פנימית בראי חוק הגנת הפרטיות לרבות תיקוניו ותקנותיו

מעודכן ליולי 2025(*)

(*) ההגדרות במסמך זה רלוונטיות לחוקים, לתקנות ולפרסומים למועד כתיבתו ואינן מחליפות יעוץ משפטי בדבר סוגיות שיכול שיעלו במגוון המקרים אשר תאגידים חברות וגופים שונים עשויים להיתקל בהם בעת יישום חוק הגנת הפרטיות ותקנותיו.

מבוא

1. **<u>חוק הגנת הפרטיות התשמ"א-1981 ותיקון 13 התשפ"ד-2024</u>** (להלן החוק), קובע הוראות שונות וחובות המוטלות על גוף ציבורי (כהגדרתו בסעיף 28 בחוק), בעל השליטה במאגר מידע[1] ומחזיק המאגר, לרבות הוראות בדבר עיבוד או שימוש במאגר.

1.1 <u>היבטים מרכזיים בחוק הגנת הפרטיות:</u>

1.1.1 החובה המרכזית המפורטת הינה חובת שמירת הפרטיות, שמטרתה צמצום הסיכון לשימוש לרעה במידע אשר במאגר או פגיעה בו כך שכל ארגון וכל בעל עסק חייבים להגן ולשמור על פרטיותו של אדם, כאשר חלק מעיסוקם כרוך באיסוף מידע על לקוחות, עובדים וכדומה ושמירה עליו.

1.1.2 חובת שמירת הפרטיות מתמקדת בזכותו של כל אדם לפרטיות.

1.1.3 איסור על פגיעה בפרטיות והגדרה מה היא פגיעה כזו.

1.1.4 קביעת ענישה פלילית למי שמפר את הוראות החוק ואף איסור בבית המשפט, במקרים מסוימים, על שימוש בראיות שהושגו תוך הפרת פרטיות.

1.1.5 ההנחיות, הקשורות להיבטי אבטחת המידע, הינן מצומצמות והן הורחבו בתקנות אשר הותקנו מכוח החוק.

1.2 **<u>תיקון 13 לחוק הגנת הפרטיות, אשר כניסתו לתוקף מאוגוסט 2025</u>** - מעדכן ומרחיב באופן משמעותי את חובות הגנת המידע על ארגונים המחזיקים במאגרי מידע בהתאם לסטנדרט גלובלי (כחלק מפרויקט תאימות GDPR מול האיחוד האירופי), ובכל זאת:

1.2.1 הרחבת סמכות הפרט (נשוא המידע) בקבלת מידע אישי המוחזק בגינו והזכות להימחק (Need to be Forgotten) ועדכון תקופת ההתיישנות משנתיים לשבע שנים (עפ"י הדין הכללי), בנוגע לפניה לקבלת מידע. נשוא המידע ייודע בנושאים הבאים:

- האם חלה חובה עליו במסירת המידע או שהדבר כפוף לרצונו תוך מתן הסכמתו.
- למי יימסר המידע והסיבה.

[1] מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר מידע

- פרטי בעל השליטה במאגר.
- זכויותיו לעיון/ תיקון המידע או מחיקה.

1.2.2 הגדרת המונחים "בעל שליטה", "מחזיק מאגר" "עיבוד מידע" ו"מידע בעל רגישות מיוחדת" (ר' נספח א').

1.2.3 אכיפה מוגברת: לרשות להגנת הפרטיות יש סמכות להטיל קנסות ללא צורך בהליך פלילי.

1.2.4 אחריות ישירה: מנהלים ובעלי תפקידים אחראים ישירות לעמידה בהוראות החוק.

1.2.5 ביקורת מאגרי מידע: חובת בדיקה תקופתית של מאגרים והצורך ברישום מאגרי מידע בהתאם לשינויים בחוק.

1.2.6 בקרות גישה מחמירות: חובת ביצוע ביקורת הרשאות חצי-שנתית, ניהול גישה עפ"י צורך בלבד (Need to Know).

1.2.7 ניהול אירועי פרטיות: חובת דיווח על אירועים חמורים, כולל פריצה למערכות מידע.

2. **<u>תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז 2017</u>** (להלן התקנות), שנכנסו לתוקף במאי 2018, מרחיבות את חוק הגנת הפרטיות, בכך שהן מפרטות את אופן יישומה של חובת אבטחת המידע (פיזית/לוגית) המוטלת בחוק הגנת הפרטיות. תקנות אלה קובעות ומכילות מנגנונים ארגוניים ודרישות מהותיות שמטרתן – הפיכת אבטחת המידע לחלק מניהול השגרה של הארגון.

2.1 לתקנות ישנם שני רבדים:

(א) <u>ברובד הראשון נדרש בעל המאגר-</u> לקבוע מהו המידע המוגן, תחת איזו רמת אבטחה מוגדר המאגר, בהתאם לפירוט רמות האבטחה בתקנות, וכן מהם הסיכונים המיוחסים אליו.

(ב) <u>ברובד השני נדרש הארגון</u>- לקבוע מדיניות ולייסד תהליך לעמידה בהוראות החוק והתקנות, לייעד נושא משרה בארגון שקיום הוראות התקנות הן חלק מתפקידו, ועליו להיות אחראי על יישום התקנות בתוך הארגון.

2.2 בתקנות מוגדרים המונחים הבאים אשר יכול וישמשו אותנו בבניית עקרונות לדגשי ביקורת:

(א) מאגר מידע.
(ב) מאגר מידע המנוהל בידי יחיד.
(ג) מסמך מאגר מידע.
(ד) מערכות המאגר.
(ה) בעל הרשאת גישה למאגר המידע.
(ו) סיווג המאגר עפ"י 3 רמות אבטחה (בסיסית / בינונית / גבוהה) - ר' נספח ב'.
(ז) ממונה על אבטחת מידע.
(ח) ממונה על הגנת הפרטיות Data Protection Officer (DPO).
(ט) אירוע אבטחה חמור.
(י) מידע ביומטרי.
(יא) התקן נייד.
(יב) נשוא המידע.
(יג) הרשות הלאומית להגנת הסייבר.

3. **<u>הנחיית הרשות להגנת הפרטיות מספטמבר 2024</u>** - בדבר תפקידי הדירקטוריון בקיום חובת התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע), במסגרתה מוטלת על הדירקטוריון אחריות לוודא כי קיימת מדיניות ארגונית, בין היתר בדבר אופן השימוש במידע אישי וניהולו, קביעת תהליכי פיקוח, בקרה וציות אפקטיביים לגבי המדיניות (לרבות קיומה של תוכנית אכיפה פנימית).

4. **<u>תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א 2001</u>** - בהתאם לתקנות, תפקיד הביקורת הפנימית בארגון- הינו לבחון את הטמעתן ואופן יישומן בארגון, וזאת תוך בחינת התמונה הרחבה והתייחסות לקיומם של תהליכים ונהלים מחייבים בארגון, בקרות המבוצעות ע"י הארגון, ממצאים העולים מהשטח וחשיבה צופה פני עתיד. בהתאמה, על הארגון לבנות תוכנית רב שנתית, אשר תוביל להטמעת התקנות כחלק ממדיניות הארגון.

5. **הרשות להגנת הפרטיות (שהינה הגוף המפקח על עמידה בהוראות החוק והתקנות)** - רשאית לבצע פעולות ביקורת ואכיפה בגופים שונים, תוך השתת עיצומים משמעותיים על ארגונים שיימצאו מפירים את התקנות ו/או החוק בגין אי רישום מאגר, הפרת זכויות של נשוא המידע, הפרות בניהול המאגר, ובמאגר מידע בעל רגישות מיוחדת - לפי מכפלת מספר נושאי המידע כתלות בסוג המאגר ואף אפשרות להטיל עונש עד 3 שנות מאסר בפועל.

דגשי ביקורת מוצעים בנושא הגנת הפרטיות

תת תהליך	הדגשים המוצעים לביקורת
קביעת מדיניות פרטיות ארגונית	1) האם הוגדרה מדיניות ארגונית בדבר פרטיות לרבות כללים לשמירה והגנה על המידע, תקופת שמירת נתוני המאגר לרבות הפחתה וצמצום, לפי השלבים במחזור חיי המידע ל-3 הקטגוריות הבאות: • איסוף המידע והכנה לשימוש. • שימוש במידע. • בקרה על השימוש במידע. 2) האם נִתנה התייחסות במדיניות לטיפול בפניה של נשוא המידע לעיין במידע אישי או לבקש תיקון שלו? 3) האם הוגדרה מדיניות בדבר תהליך זיהו מאגרי מידע חדשים? 4) האם קיים ממונה פרטיות בארגון אשר יביא מדיניות זו לבחינה תקופתית?
מיפוי וזיהוי מאגרי מידע	1) קיום תהליך ראשוני לזיהוי ומיפוי היחידות העסקיות בארגון המייצרות ומעבדות מידע בעל מאפיינים של מאגר מידע כפי שמוגדרים בחוק הגנת הפרטיות. 2) קיום תהליך של זרימת מידע תקופתי לגבי יחידות עסקיות חדשות ו/או מאגרי מידע פוטנציאלים חדשים לבעל תפקיד בארגון. 3) לגבי מאגרי מידע שזוהו בארגון - קבלת רשימה של סוגי מאגרי המידע הקיימים, לרבות מסמכי הרישום ובחינת רלוונטיות הנתונים המופיעים אצל הרשם למדגם מאגרים. 4) האם תהליך סיווג מאגרי המידע נעשה עפ"י הכללים הכמותיים והאיכותיים שנקבעו בתקנות הגנת הפרטיות? עפ"י סיווג זה נגזרות הדרישות לרמת האבטחה הנדרשת (מאגר המנוהל ע"י יחיד, רמה בסיסית, בינונית או גבוהה).
רישום מאגר המידע או הודעה לרשם	1) האם מאגרי המידע שזוהו ונמצאים שברשות הארגון חייבים ברישום? 2) אם כן, האם נרשמו? 3) אם חייב רישום אך לא נרשם – האם מתבצע עיבוד נתונים? 4) האם מאגר המידע מועבר לחו"ל? אם כן, לאילו מדינות?
ניהול מאגר מידע ועיבוד חוקי של מידע אישי	1) קיומו של מסמך הגדרת המאגר והתאמתו לדרישות התקנות. 2) קיום תהליך לעדכון מאגרי המידע לפחות אחת לשנה. יישום התהליך על מדגם מאגרי מידע 3) האם המידע שבמאגר נצבר בהסכמת נשוא המידע, באילו אמצעים ניתנה ההסכמה? 4) האם המידע נאסף ומעובד בהתאם למטרה שלשמה הוקם? 5) האם ניתנה הרשאה מתועדת לעיבוד המידע מבעל השליטה במאגר המועבר לאחרים? 6) האם מתקיים תהליך צמצום מידע עפ"י המדיניות שהוגדרה? יש לסקור את התהליך ולבחון את איכותו ואת התאמתו לדרישות *לסעיף 6 - יש לחזור לקראת תום ביצוע הביקורת, על מנת לבדוק-האם המידע שמצאנו בפועל אכן מוגדר במאגרים הנ"ל. 7) האם הגיעה פנייה מנשוא מידע לעיון במידע או מחיקה, אם כן כיצד טופלה?

תת תהליך	הדגשים המוצעים לביקורת
מינוי ממונה על הגנת הפרטיות	1) האם הגוף המבוקר נכלל בגופים החייבים במינוי ממונה על הגנת הפרטיות (DPO) "בעל שליטה", גוף ציבורי" בנק, חברת ביטוח, חברה העוסקת בדירוג ובהערכה של אשראי? 2) אם כן – האם מונה בעל תפקיד לעניין? האם ניתן כתב מינוי רשמי הכולל הגדרת תפקיד וסמכויות? האם הכין תוכנית הדרכה לעובדים? האם הכין תוכנית לבקרה שוטפת על העמידה בהוראות החוק? האם קיים ניגוד עניינים? 3) האם קיים יישום מלא של כללים אלה ואופן ביצועם?
מינוי ממונה על אבטחת מידע	1) מינוי ממונה על אבטחת מידע, כפיפות וסמכויות, לרבות כתב מינוי והגדרת סמכויות. 2) היעדר קיום ניגוד עניינים בין ביצוע תפקידו זה לתפקידים אחרים שאולי מבוצעים על ידו 3) האם הממונה על אבטחת המידע ביצע סקירת פערים, המהווה בסיס לתוכנית עבודה מבוססת סיכונים לצמצום הפערים שאותרו? 4) קבלה ועיון בסקירת פערים בהשוואה לתקנות הגנת הפרטיות, כפי שבוצעה בארגון או בסיוע יועץ חיצוני עבור הארגון. בדיקה- האם קיים ניגוד עניינים בין תפקידיו הנוספים לתפקיד ממונה על אבטחת מידע
נוהל אבטחת מידע	<u>במאגרים בעלי כל רמות האבטחה</u> 1) קיומו של נוהל אבטחת מידע כנדרש בתקנות. 2) ניסוח מסמך הגדרות המאגר כמוגדר בתקנות. 3) תדירות עדכון המסמך והתאמתו – נתמך בתיעוד. <u>במאגרים בעלי רמת אבטחה בינונית או גבוהה</u> בדיקה כי הנוהל מתייחס גם לנושאים הבאים: 1) שיטות בקרה על השימוש במאגר, אבטחת התקשרות אל המאגר וממנו, ניהול אמצעי אחסון והתקנים ניידים. התייחסות לגיבוי ושמירת מידע, התייחסות לביצוע ביקורת תקופתית כמוגדר בתקנות. 2) עדכניות הנוהל – נתמך בתיעוד, לרבות התאמת הנוהל הקיים לדרישות התקנות. 3) האם הנוהל מאושר ע"י בעל המאגר?
מיפוי וביצוע של סקר סיכוני אבטחת מידע	1) ביצועו של סקר תקופתי של סיכוני אבטחת מידע, תוך התייחסות לכלל הדרישות בתקנות. אם מדובר במאגר שחלה עליו רמת אבטחה גבוהה, יש לבדוק, כי אחראי האבטחה ובעל המאגר קיבלו את הנתונים, בחנו אותם ובנו תוכנית לתיקון ליקויים עפ"י מדיניות ניהול הסיכונים של הארגון. 2) יישום התוכנית לתיקון הליקויים.
התייחסות לאבטחה פיזית	<u>במאגרים בעלי כל רמות האבטחה</u> אופן השמירה הפיזית של שרתי המאגר והתאמתם לדרישות התקנות. <u>במאגרים בעלי רמת אבטחה בינונית או גבוהה</u> קיומם של אמצעי אבטחה ותיעוד הגישה לאתרים הפיזיים- הן לוגי (למשל, מסדי נתונים) והן פיזי (למשל ניירות וכד').
ניהול אבטחת התקשורת	1) אילו אמצעי הגנה קיימים בארגון? כיצד בוחנים את התאמתם ועדכונם באופן שוטף? 2) מה אופן מתן ההרשאה לגישה מרחוק, מי בעלי ההרשאה, מי מוסמך לתת הרשאה לעבודה מרחוק? האם יש סקירה תקופתית של הרשאות גישה מרחוק?

תת תהליך	הדגשים המוצעים לביקורת
	3) קבלת העתקים של מבחני החדירה האחרונים. מה תדירות ביצוע מבחני חדירה ואילו אמצעים המבחנים כוללים. האם תואמים לתקנות? 4) האם מבחני החדירה שולבו בתוכנית הרב שנתית של הארגון?
ניהול העברת מסמכים והתקנים ניידים	1) עמידת הארגון בהוראות התקנות והגבלת השימוש בהתקנים ניידים. 2) דיווחים על אובדן התקנים ניידים ואופן הטיפול באירוע. 3) קיומם של אמצעי ניטור אחר התקנים ניידים. התאמה למדיניות הארגון באשר למניעת הכנסת התקנים במקרים מסוימים.
שמירת נתוני אבטחה	1) האם מסמכים הקשורים לפעילות הנוגעת לאבטחת המידע של המאגרים (סקרים, טיפול בפערים, מסמכי מדיניות ונהלים, תיעוד וגיבוי, מבחני חדירה וכו') נשמרים לכל הפחות שנתיים? 2) האם כלל הנתונים גובו ו/או ניתנים לשליפה מהארכיון במידת הצורך?
בחינת יכולת הגיבוי, שחזור והתאוששות	<u>במאגרי מידע בעלי רמה בינונית וגבוהה בלבד</u> 1) בדיקת תהליכי העבודה הקיימים עבור גיבוי ושחזור של נתונים. 2) קיומה של תוכנית עבודה לגיבוי בהתאם לדרישות בתקנות ולפי מדיניות אבטחת המידע של הארגון. 3) תדירות אימות הנתונים בהתאם לדרישות ותיעוד הפעולות. 4) בחינת אירועי אבטחה מהעבר, תוך בחינת התיעוד של מבצעי הפעולות. 5) שמירת עותק גיבוי של המאגר מחוץ למתקני הארגון, תוך התייחסות לאופן הגישה אליו במקרה של אסון; האם מוגדר בנוהלי שעת חירום.
מחיקת מאגר מידע ומחיקת מידע מהמאגר	1) האם נמחקו מאגרים שנרשמו בעבר? בדיקת רישומים אצל הרשם אל מול המאגרים שזוהו ע"י הארגון. 2) תהליך מחיקת הנתונים מהמאגר והשמדתם בעת סיום עבודה עם המאגר או בהתאם למוגדר בדין הספציפי הרלבנטי. 3) ככל שבוצעו כאלה בעבר- יש לקבל תיעוד בהתאם למדיניות הארגון
ניהול המשאב האנושי והרשאות הגישה	<u>במאגרים בעלי כל סוגי רמות האבטחה</u> 1) תהליך מתן ההרשאות תוך התייחסות ל: • קליטת העובדים, התאמתם לגישה למידע והדרכתם בהתאם לתקנות. • חתימת עובדים על הסכם סודיות בכל הנוגע למאגר מידע 2) קבלת רשימת עובדים שסיימו העסקתם בשנה האחרונה, ובדיקה - האם נותקו ממאגרי המידע והרשאתם נמחקה? <u>במאגרים בעלי רמת אבטחה בינונית או גבוהה</u> 1) קיומה של פעילות הדרכה תקופתית כמתבקש בתקנות והתייחסות לתוכנית עבודה שנתית – יש לבדוק תוכנית הדרכה שנתית, את תכניה ואופן הביצוע. 2) מיהם בעלי התפקידים בעלי ההרשאות למאגרי מידע, מה תקפות הרשאות הגישה ומתי בוצע עדכון אחרון? יש לבדוק הימצאותם של גורמים אשר אינם רשאים לגשת למידע ברשומות אלה, ככל שלא עודכנו.

תת תהליך	הדגשים המוצעים לביקורת
	3) זיהוי ואימות כניסת עובדים למאגרים נעשה באמצעים המוגדרים בתקנות. 4) קיומו של מנגנון תיעוד כמתבקש בתקנות, לכלל מערכות הארגון ושמירת הנתונים ע"פ התקופה שנקבעה.
אירועי אבטחה ותיעודם	חובת הודעה מורחבת חלה על אירוע שנעשה בו שימוש בחלק כלשהו (לא רק חלק מהותי) מתוך המידע שבמאגר. יש לבדוק- האם היו אירועים כאלה, האם הארגון דיווח עליהם, איזה תחקיר שורש בוצע ומהן המסקנות שהוסקו, ובאילו אמצעים משתמשים על מנת למנוע את הישנות האירוע? להלן הדגשים המוצעים: 1) האם היו אירועי אבטחת מידע בשנתיים האחרונות. ככל שזוהו כאלה- האם תועדו ודווחו בהתאם לדרישות התקנות? 2) האם בעקבות האירועים נבחן הצורך בעדכון הרשאות המאגר ע"פ המוגדר בתקנות? 3) כיצד הארגון נערך לזיהוי ודיווח על אירועי אבטחת מידע עתידיים? 4) לוודא את קיומו של תהליך כזה בארגון (לרבות נוהל- Incident Response) שיהא זמין בקרות אירוע.
בחינת התקשרויות עם מיקור חוץ	1) האם נקבעה מדיניות ע"י הארגון לאופן בחירת הצדדים השלישיים (שרשרת אספקה) להם תבוצענה ביקורות תקופתיות? 2) דגימת הסכמים - האם קיים נספח אבטחת מידע החתום ע"י הממונה לאבטחת מידע, והאם בוצעו ביקורות אבטחת מידע בחצרות ספק? 3) האם נוסח נספח אבטחת מידע תואם למתבקש בתקנות? 4) כיצד הארגון מבטיח לעצמו קיום של תהליכי הבקרה על עמידתו של הספק בהוראות התקנות? יש לשאוף לניסוח נספח להתקשרות (אשר יתקבל מהספק בכל שנה) על מחויבותו של הספק לעמידה בהוראות החוק והתקנות כנותן השירות של הארגון. 5) סקירת ממצאים שעלו בביקורות שבוצעו לצדדים שלישיים (שרשרת אספקה) ומעקב אחר יישומם אצל צד ג' 6) האם מוגדר תהליך בסיום ההתקשרות - להשמדת המידע וגניזתו בתום ההתקשרות? כיצד מוודאים שהדבר מתבצע? • מחיקה בתוך הארגון, כגון מ- mailing list או רשימות שיווק אחרות למשלוח הודעות טקסט • מחיקה מחוץ לארגון: הואיל ומחוץ לארגון אין שליטה, צריך לשאוף לכסות זאת בהצהרה של נותן השירות שכך ביצע
תביעות ועיצומים כספיים	1) פניות הציבור בנושא פרטיות, האם היו תביעות בנושא ואילו לקחים הופקו? 2) האם היו ביקורות של הרשויות והאם הפערים שזוהו טופלו? 3) האם הוטלו עיצומים כספיים?
ביצוע מעקב אחר ביקורת תקופתית	<u>במאגרי מידע בעלי רמה בינונית וגבוהה בלבד.</u> 1) ביצוע ביקורת פנימית או חיצונית, לפחות אחת לשנתיים ע"י גורם מוסמך בתחום אבטחת מידע. 2) בדיקה, כי המלצות הביקורת שיושמו, תורגמו לתוכנית עבודה לתיקון ליקויים. בדיקה- מהו הליך העבודה והאם הנושא עלה לדיון ותועד. 3) בדיקה- האם הופקו מסקנות מהדוח לשנים הבאות, ככל שיש צורך בעדכון המערכות.

תת תהליך	הדגשים המוצעים לביקורת
	קיימות דרישות נוספות לעמידה טכנולוגיות כגון ניהול לוגים ודרישות אחרות כנגזרת של סיווג המאגר: ר' נספח ג' – מיפוי הדרישות בתקנות עפ"י סיווג המאגר. ר' הפניה לקישור למסמך של הרשות להגנת פרטיות בנושא: https://www.gov.il/BlobFolder/guide/data_security_guide/he/NEW_GUIDE.pdf

נספח א' – עדכון הגדרות:

"בעל שליטה" במאגר מידע (controller) – מי שקובע לבדו אם עם אחר, את מטרות עיבוד המידע שבמאגר המידע (לשעבר בעל מאגר מידע)

מחזיק (processor) – צד ג' המעבד מידע אישי עבור בעל שליטה (ולא רק בדרך קבע)

"עיבוד" – כל פעולה שנעשית על מידע אישי, לרבות איסוף, קבלה שמירה, אחסון, העתקה, עיון, גילוי, חשיפה, העברה, מתן גישה, ניתוח ועוד

"מידע רגיש"—עדכון ההגדרה והמונח שונה ל- "מידע בעל רגישות מיוחדת".

- מידע על צנעת חייו של אדם (התנהגות אדם ברשות היחיד, מצב משפחתי, נטייה מינית).
- מצב בריאותי, לרבות מידע רפואי ומידע גנטי.
- מזהה ביומטרי, המשמש או נועד לשמש לזיהוי אדם באופן ממוחשב (טביעת אצבע, זיהוי קול, חתימת אצבע דיגיטלית, זיהוי דפוס הליכה).
- מוצאו של אדם.
- עבר פלילי.
- מידע אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם או השקפת עולמו.
- הערכת אישיות מקצועיות.
- נתונים אודות מיקומו של אדם שיש בהם כדי ללמוד על מידע בעל רגישות מיוחדת ונתוני מיקום ונתוני תעבורה (שנוצרו על ידי ספק מורשה), כאמור בחוק סדר הדין הפלילי (סמכויות אכיפה- נתוני תקשורת), התשס"ח-2007.
- נתוני שכר של אדם ופעילותו הפיננסית.
- מידע שחל עליו חובת סודיות בדין.
- מידע על חברות בארגון עובדים (או כל מידע אחר שיתווסף לתוספת השנייה לחוק; חל ביחס למידע שהועבר למאגר המידע מחוץ לגבולות ישראל ובאותו מקום חלות הוראות מיוחדות על סוג המידע).

נספח ב' – סיווג המאגר עפ"י 3 רמות אבטחה:

סיווג מאגר המידע	כמות רשומות	כמות מורשי גישה	רגישות המידע	חובת מינוי ממונה פרטיות על הגנת הפרטיות
בסיסי	עד 10,000 רשומות	עד 5 מורשים	מידע שאינו רגיש, כמו נתונים כלליים	גוף ציבורי גוף ביטחוני
בינוני	בין 10,000 ל-100,000 רשומות	בין 5 ל-50 מורשים	מידע רגיש, כגון מידע אישי מזהה או פיננסי	גוף ציבורי גוף ביטחוני
גבוה	מעל 100,000 רשומות	מעל 50 מורשים	מידע רגיש במיוחד כמו רפואי, פיננסי או ביומטרי	גוף ציבורי גוף בטחוני כל גוף אחר

נספח ג' – התקנות החלות עפ"י סיווג רמות האבטחה של מאגרי המידע

התקנות החלות	רמת האבטחה הבסיסית	רמת האבטחה הבינונית	רמת האבטחה הגבוהה	מאגר המנוהל בידי יחיד
	תקנות 3-1	תקנות 4-1	תקנות 20-1	תקנות 2-1
	4 (א), (ב), (ג), (ה), (ו)	5 (א), (ב), (ה)		6 (א)
	5 (א), (ב), (ה)	6-15		9 (א)
	6 (א), 7 (א), (ב)	16 (א), (ב), (ג), (ה)		11 (א)
	8	17		12-14
	9 (א), (ג),	18 (א)		20
	11 (א), (ב)	19		
	12-15	20		
	17			
	19			
	20			