יולי 2020

לשכת המבקרים הפנימיים IIA ישראל מפרסמת בזאת קווים מנחים מטעמה ובהם הנחיות מוצעות לביצוע ביקורת פנימית בהיבטי אבטחת מידע שעל בעל מאגר ומחזיק לבצע בהתאם התקנות להגנת הפרטיות (אבטחת מידע), התשע"ז 2017 (להלן: "התקנות").

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

המסמך חובר ע"י מאיה ויסמן ורו"ח איה שטיינר 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

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

קווים מנחים מס' 2

בנושא ביצוע ביקורת פנימית בראי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז 2017

יולי 2020

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

מבוא

1. **<u>חוק הגנת הפרטיות התשמ"א-1981</u>** (להלן החוק), קובע הוראות שונות וחובות המוטלות על בעל מאגר, מחזיק מאגר ומנהל מאגר.

1.1 החובה המרכזית המפורטת בחוק 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.

1.2 חובת שמירת הפרטיות בחוק מתמקדת בזכותו של כל אדם לפרטיות.

1.3 החוק אוסר על פגיעה בפרטיות ומגדיר מה היא פגיעה כזו.

1.4 החוק קובע ענישה פלילית למי שמפר את הוראת החוק ואף אוסר במקרים מסוימים על שימוש בראיות שהושגו תוך הפרת פרטיות בבית המשפט.

1.5 ההנחיות בחוק, הקשורות להיבטי אבטחת המידע, הינן מצומצמות והן הורחבו בתקנות להלן.

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 **<u>לתקנות ישנם שני רבדים</u>**:

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

2.1.2 <u>ברובד השני</u> נדרש הארגון- לייסד 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 בהתאם לתקנות, <u>תפקיד הביקורת הפנימית בארגון</u>- הינו לבחון את הטמעתן ואופן יישומן בארגון, וזאת תוך בחינת התמונה הרחבה והתייחסות לקיומם של

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

תהליכים ונהלים מחייבים בארגון, בקרות המבוצעות ע"י הארגון, ממצאים העולים מהשטח וחשיבה צופה פני עתיד.

2.3 בהתאמה, על הארגון לבנות תוכנית רב שנתית, אשר תוביל להטמעת התקנות כחלק ממדיניות הארגון.

2.4 החל מיולי 2019 יכולה הרשות להגנת הפרטיות (שהינה הגוף המפקח על ביצוע התקנות)- לבצע פעולות ביקורת ואכיפה בגופים שונים, תוך מתן עיצומים משמעותיים לארגונים שימצאו מפירים את התקנות (קנס בסכום עד 226,000 ₪ פר עבירה וכן עד 5 שנות מאסר בפועל).

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

דגשי ביקורת מוצעים בראי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז 2017

3. <u>בתקנות מוגדרים המונחים הבאים</u>:
   א. אירוע אבטחה חמור
   ב. בעל הרשאה
   ג. התקן נייד
   ד. חומר מחשב
   ה. מחשב
   ו. מאגר המנוהל בידי יחיד
   ז. רמות האבטחה השונות של מאגרים (בסיסית / בינונית / גבוהה)
   ח. מידע ביומטרי
   ט. ממונה על אבטחה
   י. מערכות המאגר
   יא. נושא המידע
   יב. הרשות הלאומית להגנת הסייבר
   יג. רשות ציבורית

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

4. <u>להלן הדגשים המוצעים לתוכנית הביקורת</u>:

מספרי סעיפים בתקנות	נושא	דגשים מוצעים
סעיף 2	מיפוי מאגרי מידע	1) בחינת קיום תהליך ראשוני לזיהוי ומיפוי היחידות העסקיות בארגון המייצרות ומעבדות מידע בעל מאפיינים של מאגר מידע כפי שמוגדרים בחוק הגנת הפרטיות. 2) בחינת 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) בחינת תהליך לסיווג מאגרי המידע 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). *לסעיף זה יש לחזור לקראת תום ביצוע הביקורת, על מנת לבדוק- האם המידע שמצאנו בפועל אכן מוגדר במאגרים הנ"ל.
סעיף 2	הכרת בעלי התפקידים ובחינת האחריות הכוללת לאבטחת המידע במאגר	1) קיומו של מסמך הגדרת המאגר ובחינתו בהשוואה לדרישות התקנות. 2) בחינת קיום תהליך לעדכון מאגרי המידע לפחות אחת לשנה. בחינת יישום התהליך על מדגם מאגרי מידע . 3) בחינת מינוי ממונה על אבטחת מידע, כפיפות וסמכויות, לרבות כתב מינוי והגדרת סמכויות. 4) בחינת היעדר קיום ניגוד עניינים בין ביצוע תפקידו זה לתפקידים אחרים שאולי מבוצעים על ידו.
סעיף 3	ממונה אבטחת מידע	1) בחינה - האם הממונה על אבטחת המידע ביצע סקירת פערים, המהווה בסיס לתוכנית עבודה מבוססת סיכונים לצמצום הפערים שאותרו. 2) קבלה ועיון בסקירת פערים בהשוואה לתקנות הגנת הפרטיות, כפי שבוצעה בארגון או בסיוע יועץ חיצוני עבור הארגון. על המבקר לבדוק- האם קיים ניגוד עניינים בין תפקידיו הנוספים לתפקיד הממונה. האם תפקידיו מוגדרים במדיניות הארגון או במסמך דומה

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

מספרי סעיפים בתקנות	נושא	דגשים מוצעים
סעיף 4	נוהל אבטחה	<u>במאגרים בעלי כל רמות האבטחה</u> 1) בחינת קיומו של נוהל אבטחת מידע כנדרש בתקנות. 2) בחינת ניסוח מסמך הגדרות המאגר כמוגדר בתקנות. 3) בחינת תדירות עדכון המסמך והתאמתו – נתמך בתיעוד. <u>במאגרים בעלי רמת אבטחה בינונית או גבוהה</u> יש לבדוק 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) בחינת עדכניות הנוהל – נתמך בתיעוד, לרבות התאמת הנוהל הקיים לדרישות התקנות. 3) האם הנוהל מאושר ע"י בעל המאגר.
סעיף 5	מיפוי וביצוע של סקר סיכונים	1) בחינת ביצועו של סקר סיכונים תקופתי 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) בחינת יישום התוכנית לתיקון הליקויים.
סעיף 6	התייחסות לאבטחה פיזית במתקן	<u>במאגרים בעלי כל רמות האבטחה</u> 1) בחינת אופן השמירה הפיזית של שרתי המאגר והתאמתם לדרישות התקנות. <u>במאגרים בעלי רמת אבטחה בינונית או גבוהה</u> 1) בחינת קיומם של אמצעי אבטחה ותיעוד הגישה לאתרים הפיזיים- הן לוגי (למשל, מסדי נתונים) והן פיזי (למשל ניירות וכד').
סעיפים 7- 10	אבטחת מידע לגבי ניהול משאבי אנוש וניהול הרשאות גישה	<u>במאגרים בעלי כל רמות האבטחה</u> בחינת תהליך מתן ההרשאות תוך התייחסות ל: 1) קליטת העובדים, התאמתם לגישה למידע והדרכתם בהתאם לתקנות. 2) חתימת עובדים על הסכם סודיות בכל הנוגע למאגר מידע.

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

מספרי סעיפים בתקנות	נושא	דגשים מוצעים
		3) קבלת רשימת עובדים שסיימו העסקתם בשנה האחרונה, ובדיקה האם נותקו ממאגרי המידע והרשאתם נמחקה. <u>במאגרים בעלי רמת אבטחה בינונית או גבוהה</u> 1) בחינת 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. 3) בחינה, כי 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.
סעיף 11	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 המקרה. להלן הדגשים המוצעים: 1) בחינת אירועי אבטחת מידע שאירעו 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)- שיאפשר את כל הנ"ל.
סעיף 12	ניהול העברת מסמכים והתקנים ניידים	1) בחינת עמידת הארגון בהוראות התקנות והגבלת השימוש בהתקנים ניידים. 2) בחינת דיווחים על אובדן התקנים ניידים ואופן הטיפול באירוע.

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

מספרי סעיפים בתקנות	נושא	דגשים מוצעים
		3) בחינת קיומם של אמצעי ניטור אחר התקנים ניידים. התאמה למדיניות הארגון באשר למניעת הכנסת התקנים במקרים מסוימים.
סעיפים 13- 14	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? 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?
סעיף 15	בחינת התקשרויות עם מיקור חוץ	1) בחינת מדגם הסכמים על-מנת לאשר, כי הממונה לאבטחת מידע מעורב בתהליך ההתקשרות עם מיקור החוץ ואישורו בהתייחס למערכות מידע נדרשות. 2) בחינת נוסח נספח אבטחת מידע והתאמתו למתבקש בתקנות. 3) 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. 4) האם מוגדר תהליך להחזרת המידע וגניזתו בתום ההתקשרות? כיצד מוודאים שהדבר מתבצע? א) מחיקה בתוך הארגון, כגון מ- mailing list או רשימות שיווק אחרות למשלוח הודעות SMS ב) מחיקה מחוץ לארגון. מחוץ לארגון אין שליטה. צריך לשאוף לכסות זאת בהצהרה של נותן השירות שכך ביצע
סעיף 15	מחיקת מידע מהמאגר	1) בחינת תהליך מחיקת הנתונים מהמאגר והשמדתם בעת סיום עבודה עם המאגר או בהתאם למוגדר בדין הספציפי הרלבנטי. 2) ככל שבוצעו כאלה בעבר- יש לקבל תיעוד בהתאם למדיניות החברה
סעיף 16	ביצוע מעקב אחר ביקורת תקופתית	<u>במאגרי מידע בעלי רמה בינונית וגבוהה בלבד</u>

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201

מספרי סעיפים בתקנות	נושא	דגשים מוצעים
		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.
סעיף 17	שמירת נתוני אבטחה	1) על המבקר לבדוק 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.
סעיף 18	בחינת יכולת הגיבוי, שחזור והתאוששות	<u>במאגרי מידע בעלי רמה בינונית וגבוהה בלבד</u> בדיקת תהליכי העבודה הקיימים עבור גיבוי ושחזור של נתונים בהתאם ל: 1) קיומה של תוכנית עבודה לגיבוי בהתאם לדרישות בתקנות ולפי מדיניות אבטחת המידע של הארגון. 2) בחינת תדירות אימות הנתונים בהתאם לדרישות ותיעוד הפעולות. 3) בחינת אירועי אבטחה מהעבר, תוך בחינת התיעוד של מבצעי הפעולות. 4) שמירת עותק גיבוי של המאגר מחוץ למתקני הארגון, תוך התייחסות לאופן הגישה אליו במקרה של אסון; האם מוגדר בנוהלי שעת חירום.

www.theiia.org.il | office@theiia.org.il | טל' 03-5116617 | ת"ד 29281 תל אביב 6129201