שרת המשפטים

ירושלים

ג' אייר תשע"ו
11 מאי 2016

מס' מכתב: 2016-8511
פנימי: א.א

לכבוד
חה"כ ניסן סלומינסקי
יו"ר ועדת החוקה, חוק ומשפט
כנסת ישראל

שלום רב,

הנדון: טיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ו-2016

התקנות שבנדון (מצ"ב) נועדו לקבוע הסדר מעודכן, מקיף ומפורט יותר מזה הקיים כיום בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 לענין ההגנה הפיסית והלוגית על מאגרי מידע ולעניין סדרי הניהול וכללי העבודה במאגרי מידע ובקשר אליהם. ההסדר המוצע יחול על מאגרי מידע של גופים ציבוריים ושל גופים פרטיים כאחד.

כמפורט בדברי ההסבר, ההסדר המוצע בטיוטת התקנות מבוסס על תקני אבטחת מידע מקובלים בעולם. הוא כולל מנגנונים וכלים פנים ארגוניים שמטרתם להמחיש את חובותיהם ואחריותם של ארגונים בתחום אבטחת מידע אישי ולהנחיל עקרונות אבטחת מידע בתוך הארגון. כל זאת, על מנת להגן על זכויות נושאי המידע במאגר המידע מפני שימוש לרעה במידע אודותיהם, הן על ידי גורמים מחוץ לארגון והן על ידי עובדי הארגון.

טיוטת התקנות היא פרי עבודה מקצועית ממושכת, שכללה שימוע ציבורי נרחב. ההערות שהתקבלו נשקלו על ידינו, וחלקן התקבלו והוטמעו בנוסחה העדכני של הטיוטה. כן נערכו שינויים והתאמות בנוסח התקנות בהתאם להתפתחויות טכנולוגיות.

אודה להנחת טיוטת התקנות על שולחנה של ועדת החוקה, חוק ומשפט של הכנסת, לשם אישורן.

בברכה,
איילת שקד

העתק: המשנה ליועץ המשפטי לממשלה (חקיקה)
ראש הרשות למשפט, טכנולוגיה ומידע

רח' צאלח א-דין 29, ת.ד. 49029 ירושלים מיקוד 91490, טל': 02-6466527-30, פקס: 02-6285438

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ו- 2016

בתוקף סמכותי לפי סעיף 36 לחוק הגנת הפרטיות, התשמ"א-1981[1] (להלן - החוק), ובאישור ועדת חוקה חוק ומשפט של הכנסת, אני מתקינה תקנות אלה:

הגדרות	1.	בתקנות אלה -
		"אירוע אבטחה חמור" - כל אחד מאלה: (1) במאגר מידע שחלה עליו רמת אבטחה גבוהה - אירוע שנעשה בו שימוש במידע מן המאגר, לרבות אירוע בו היתה כניסה למערכות המאגר באופן שמאפשר גישה למידע שבמאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע; (2) במאגר מידע שחלה עליו רמת אבטחה בינונית - אירוע שנעשה בו שימוש בחלק מהותי מן המאגר בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר;
		"התקן נייד" - אחד מאלה:

(1) מחשב המיועד לשימוש נייד ובכלל זה רדיו טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים), התשמ"ב-1982[2];

(2) מצע אחר המשמש לאחסון חומר מחשב;

		"חומר מחשב" ו- "מחשב" – כהגדרתו בחוק המחשבים, התשנ"ה- 1995[3]; "מאגר מידע" ו-"רשם" - כהגדרתם בפרק ב' לחוק;
		"מאגרים שחלה עליהם רמת האבטחה הבינונית" - מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה;
		"מאגרים שחלה עליהם רמת האבטחה הגבוהה" - מאגרי מידע מן הסוגים המפורטים בתוספת השנייה;
		"מידע ביומטרי" – מידע המשמש לזיהוי אדם, שהוא מאפיין אנושי פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת;

[1] ס"ח התשמ"א, עמ' 128; התשע"א, עמ' 758.
[2] ס"ח התשמ"ב, עמ' 218.
[3] ס"ח התשנ"ה, עמ' 366.

		"ממונה על אבטחה" - כמשמעותו בסעיף 17ב לחוק;
		"מערכות המאגר" - מערכות המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע;
		"נושא המידע" – האדם אודותיו קיים מידע במאגר המידע;
		"עובד" - יחיד המועסק על ידי בעל מאגר או מחזיק, במישרין או בעקיפין, ואשר יש לו גישה לאחד מאלה בנוגע למאגר מידע על פי הרשאתו של בעל המאגר או המחזיק: (1) מידע; (2) מערכות המחשוב של המאגר; (3) מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו.
		"רשת ציבורית" – רשת תקשורת המאפשרת שימוש גם על ידי מי שאינו עובד.
מסמך הגדרות המאגר	2.	(א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר (להלן – מסמך הגדרות המאגר), את כל העניינים האלה לפחות:
		(1) תיאור כללי של פעולות האיסוף והשימוש במידע לצורך פעילותו (להלן – פעולות שימוש במידע);
		(2) תיאור מטרות השימוש במידע;
		(3) סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) בתוספת הראשונה;
		(4) פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר;
		(5) פירוט פעולות עיבוד מידע באמצעות מחזיק;
		(6) הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם;

			(7) שמו של מנהל מאגר המידע ושל הממונה על אבטחת מידע בו, אם מונה כזה.
			(ב) בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי בנושאים המפורטים בתקנת משנה (א), ויבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגים ארגונים או אירועי אבטחה כאמור בתקנה 11, בכל שנה עד ה- 31 בדצמבר.
			(ג) בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר .
ממונה על אבטחת מידע	3.		חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה:
			(1) בעל מאגר לא ימנה ממונה על אבטחה אלא אם כן הוא כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר ; (2) הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר ; (3) הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו ;
			(4) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה ;
			(5) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות בפסקאות (2) ו-(3), לשם ביצוע תקנות אלה, יגדירן בצורה ברורה; בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו.
נוהל אבטחה	4.		(א) בעל מאגר המידע יקבע במסמך נוהל אבטחת מידע (להלן – נוהל האבטחה) לפי מסמך הגדרות המאגר ותקנות אלה אשר יחייב את כל העובדים.
			(ב) בעל מאגר מידע ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לעובדים רק בהיקף הנדרש לצורך ביצוע תפקידיהם.
			(ג) נוהל האבטחה יכלול, בין היתר, התייחסות לכל אלה:

			(1) פרטים על העניינים המפורטים בתקנה 5 (א);
			(2) הרשאות גישה למאגר המידע, למערכות תשתיות המחשוב, תקשורת ואבטחת המידע בהתאם לתקנה 8;
			(3) תיאור של אמצעים שמטרתם הגנה על מערכות המחשוב ותשתיות התקשורת של המאגר ואופן הפעלתם לצורך כך;
			(4) הוראות למורשי הגישה למאגר המידע, מערכות תשתיות המחשוב, התקשורת ואבטחת המידע לצורך הגנה על המידע במאגר;
			(5) הסיכונים שחשוף להם המידע במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5(א), אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות רגישות הקשורות אליו;
			(6) אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11, לפי חומרת האירוע ומידת רגישות המידע;
			(7) הוראות בעניין האבטחה הפיזית והסביבתית של מיתקני המאגר כאמור בתקנה 6.
			(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל האבטחה, בנוסף לאמור בתקנת משנה (ג), התייחסות גם לכל אלה:
			(1) אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר כאמור בתקנה 10;
			(2) הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12;
			(3) הוראות לעניין גיבוי הנתונים האמורים בתקנה 18(א)(1);

			(4) הוראות לעניין עריכת ביקורות תקופתיות לוידוא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16;
			(5) הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל אלה אופן הגישה של אנשי הפיתוח לנתונים במאגר.
			(ה) בעל מאגר מידע יבחן, אחת לשנה, את הצורך בעדכון הנוהל, ובלי לגרוע מן האמור, יבחן אם יש צורך בעדכונו של הנוהל במקרים אלה:
			(1) נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע;
			(2) נודע על סיכונים טכנולוגים חדשים הנוגעים למערכות המאגר.
			(ו) ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע נוהל אבטחה כאמור בתקנה זו, במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.
מיפוי מערכות המאגר וביצוע סקר סיכונים	5.		(א) בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל אלה:
			(1) תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;
			(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;
			(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;
			(4) תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיסי של רכיבים אלה;
			(5) תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

		(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.
		(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שנתגלו, ככל שנתגלו.
		(ד) רשימת מצאי תישמר כך שפרטים ממנה יימסרו לעובדים רק בהיקף הנדרש לצורך ביצוע תפקידיהם.
		(ה) ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי כאמור בתקנת משנה (א), במסמך אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה וכן רשאי לקיים את החובות הקבועות בתקנות משנה (ב) ו-(ג) בסקר סיכונים או במבדק חדירות, לפי העניין, אחד לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת האבטחה.
אבטחה פיזית וסביבתית	6.	(א) בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א)(1) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.
		(ב) בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1) ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהם.
אבטחת מידע בניהול כח אדם	7.	(א) לא ייתן בעל מאגר מידע לעובד גישה למידע המצוי במאגר ולא ישנה היקף הרשאה שניתנה, אלא אם כן נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי העובד אינו מתאים לקבלת גישה למידע המצוי במאגר; אמצעים כאמור יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שמיועד לו העובד הנוגע בדבר, כאמור בתקנה 8.

		(ב) בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם יקיים בעל מאגר מידע הדרכות לעובדים בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע אודות חובותיהם לפי החוק ונוהל האבטחה.
		(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לעובדיו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות העובדים לפיהם; הדרכה כאמור תיערך אחת לשנה לפחות, ולגבי הסמכה של עובד לתפקיד חדש - סמוך ככל האפשר למועד תחילת הסמכתו.
ניהול הרשאות גישה	8.	(א) בעל מאגר מידע יקבע הרשאות גישה של עובדים למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.
		(ב) בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל העובדים הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).
זיהוי ואימות	9.	(א) בעל מאגר מידע ינקוט אמצעים כדי לוודא לפי רשימת ההרשאות התקפות כי הגישה למידע במאגר המידע נעשית בידי עובד המורשה לכך בלבד.
		(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ייקבעו בנוהל האבטחה גם הוראות לעניין האמצעים כאמור בתקנת משנה (א), ובכללן בנושאים אלה:

(1) אופן הזיהוי, שייעשה ככל הניתן על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה; היה אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על ששה חודשים;
(2) ניתוק אוטומטי לאחר פרק זמן של אי פעילות;

(3) אופן הטיפול בתקלות הקשורות באימות זהות.

		(ג) בעל מאגר מידע ידאג לביטול ההרשאות של עובד שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שהעובד עשוי היה לדעת, מיד עם סיום תפקידו של העובד.
בקרה ותיעוד גישה	10.	(א) במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה ינוהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת 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.
		(ב) מנגנון הבקרה לא יאפשר, ככל הניתן, ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.
		(ג) בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דו"ח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
		(ד) נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
		(ה) בעל מאגר מידע יידע את העובדים במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.
תיעוד של אירועי אבטחה	11.	(א) בעל מאגר מידע אחראי לתיעוד אירועים המעלים חשש לפגיעה בשלמות המידע לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן - אירועי אבטחה); ככל הניתן יבוסס התיעוד האמור על רישום אוטומטי.
		(ב) בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.
		(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה.

		(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור בתקנת משנה (ג) אחת לרבעון לפחות.
		(ה) ארע אירוע אבטחה חמור, יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע. (ו) ארע אירוע אבטחה חמור, רשאי הרשם להורות לבעל מאגר המידע, למעט לבעל מאגר מידע מן המנויים בסעיף 13(ה) לחוק, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.
התקנים ניידים	12.	בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד וקיומם של אמצעי הגנה מתאימים מפני סיכונים אלה; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים.
ניהול מאובטח ומעודכן של מערכות המאגר	13.	(א) בעל מאגר מידע יקפיד על ניהול ותפעול תקין של מערכות המאגר, לפי המקובל בהפעלת מערכות כאלה.
		(ב) בעל מאגר מידע יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.
		(ג) בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של המערכות והתוכנות המשמשות לגישה אל המידע במאגר המידע ולהגנה עליו, לרבות חומר המחשב הנדרש לפעולתן; לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.
אבטחת תקשורת	14.	(א) בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

					(ב) העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.
					(ג) במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש בנוסף לאמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של עובד למאגר מידע ברמה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של העובד.
מיקור חוץ	15.				(א) בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע -
					(1) יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות;
					(2) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי פסקה (1):
					(א) המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצרכי ההתקשרות;
					(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;
					(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;
					(ד) משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;
					(ה) החובות בתחום אבטחת המידע החלות על הגורם החיצוני לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;

					(ו) חובתו של הגורם החיצוני להחתים את עובדיו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);
					(ז) התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו;
					(ח) חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה;
				(3) יפרט בנוהל האבטחה של המאגר גם את העניינים המנויים בפסקה (2)(א) עד (ה), וכן יפנה בו במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו;	
				(4) ינקוט אמצעי בקרה ופיקוח כדי לוודא את עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה (1).	
			(ב) ארגון שהוא בעל כמה מאגרי מידע, המתקשר עם גורם חיצוני לצורך מתן שירות הכרוך בגישה אליהם בידי הגורם החיצוני, רשאי לקיים את הוראות תקנת משנה (א)(2) בהסכם אחד לעניין כל מאגרי המידע ובלבד שהם באותם רמת אבטחה.			
		(ג)תקנה זו לא תחול על עובד.			
ביקורות תקופתיות	16.	(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר אחראי לכך שתיערך, אחת ל- 24 חודשים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה.			

			(ב) בדו"ח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב, ויסתמך גם על ממצאים ממערכות המאגר.
			(ג) בעל מאגר המידע ידון בדוחות הביקורת שיועברו לו, ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.
			(ד) בעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה, רשאי לקיים החובה הקבועה בתקנה זו במסגרת עריכת סקר סיכונים שמתקיים בו האמור בתקנת משנה (ב).
			(ה) ארגון שהוא בעל כמה מאגרי מידע, רשאי לקיים את החובה הקבועה בתקנה זו במסגרת ביקורת אחת לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה.
שמירת נתוני אבטחה	17.		בעל מאגר מידע ישמור את הנתונים הנצברים לצורך עמידה בהוראות תקנות 6(ב), 8 עד 11, 14, 15(א)(4) ו-16 באופן מאובטח למשך 24 חודשים.
גיבוי ושחזור	18.		(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר במסמך -
			(1) נהלי עבודה לביצוע גיבוי של הנתונים הנצברים לצורך עמידה בהוראות תקנות 6(ב), 8 עד 11 14, 15(א)(4) ו- 16 באופן תקופתי שגרתי;
			(2) נהלים, כדי להבטיח שבכל עת ניתן יהיה לשחזר את הנתונים האמורים בפסקה (1) למצבם המקורי ובלבד שביצוע השחזור יהיה באישור מנהל המאגר;
			(3) כי במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע לפי התקנה האמורה, ובכלל אלה - זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

		(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל מאגר אחראי לכך שיישמר עותק הגיבוי של הנתונים האמורים בתקנה (א) ושל הנהלים כאמור בתקנת משנה (א)(2), באופן שיבטיח את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס.
חובות בעל מאגר חלות על מנהל מאגר ומחזיק בו	19.	(א) החובות החלות בתקנות אלה על בעל מאגר מידע, יחולו גם על מנהל המאגר, ולמעט החובות הקבועות בתקנות 2 ו-15(א) - הן יחולו גם על מחזיק המאגר, בשינויים המחויבים ולפי העניין.
		(ב) מי שמוטלת עליו בתקנות אלה חובה או אחריות לביצוע פעולה, נדרש לתעד באופן סביר את אופן ביצוע הפעולה לפי העניין; הרשם רשאי לתת הוראות לעניין אופן תיעוד כאמור.
סמכויות הרשם	20.	(א) הרשם רשאי לפטור מאגר מסוים, בהודעה בכתב לבעל המאגר, מחובות אבטחת מידע לפי תקנות אלה, או להחיל על מאגר מסוים חובות לפי תקנות אלה, כולן או חלקן, בין היתר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר או מספר העובדים בו; בהודעה כאמור יקבע הרשם את המועד לתחילת הפטור או ההחלה, לפי העניין, ויכול שיקבע מועדים שונים לעניין תקנות שונות.
		(ב) הרשם רשאי להורות כי מי שיעמוד בהוראות מסמך מנחה בעניין אבטחת מידע או בהנחיות של רשות מוסמכת בעניין אבטחת מידע החלות עליו, יראו אותו כמקיים הוראות תקנות אלה, כולן או חלקן, אם השתכנע כי עמידה בהוראות תקן מקובל או הנחיות רשות מוסמכת אלה, לפי העניין, באופן שהורה לפי תקנות אלה, מבטיחה את רמת האבטחה הקבועה בתקנות אלה לגבי אותו מאגר מידע; לעניין זה -
		"רשות מוסמכת" - גוף ציבורי המוסמך על פי דין לתת הנחיות בעניין אבטחת מידע;
		"מסמך מנחה בעניין אבטחת מידע" –תקן רשמי, תקן ישראלי או תקן בין-לאומי כמשמעותם בחוק התקנים, התשי"ג-1953[4], או מסמך ייחוס, שהרשם אישר לעניין זה.

[4] ס"ח התשי"ג, עמ' 30.

תחולה וסייגים לתחולה	21.	(א) תקנות אלה יחולו על - (1) מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה ;
		(2) מאגרי מידע שחלה עליהם רמת האבטחה הבינונית - למעט תקנות 5(ב), ו-(ג), 11(ד), 16(ד) ו- 18(ב) ;
		(3) מאגרי מידע שאינם מאגרים שחלה עליהם רמת האבטחה הבינונית או הגבוהה - למעט תקנות 4(ד), 5(ב) ו-(ג), 6(ב), 7(ג), 9(ב), 10, 11(ג) עד (ו), 16 ו-18.
		(ב) על אף הוראות בתקנת משנה (א), על מאגר מידע שמנהל יחיד שאינו תאגיד ואשר הוא היחיד שמאגר המידע מצוי ברשותו, הרשאי לעשות בו שימוש ושבאפשרותו לעשות בו שימוש, לא יחולו הוראות תקנות 3, 4, 5, 6(ב), 7, 8, 9(ב), 10, 11 (ג) עד (ו) ו -18.
תחילה	22.	(א) תחילתן של תקנות אלה, למעט כאמור בתקנות משנה (ב) עד (ד), 30 ימים מיום פרסומן. (ב) תחילתן של תקנות 2, 3(1) עד (3), 10(א) , 13(ב) ו- 14– 90 ימים מיום פרסומן. (ג) תחילתן של תקנות 3(5), 5, 6(ב), 7(ב) ו-(ג), 10(ב) עד (ה), 11(א) עד (ד), 12, 13(ג), 15(א)(3), 17 ו-18 – שישה חודשים מיום פרסומן. (ד) תחילתן של תקנות 4 ו- 9(ב) – תשעה חודשים מיום פרסומן.
הוראת מעבר	23.	על אף האמור בתקנה 7(א), בנוגע לעובדים בעלי הרשאות ביום תחילתה של התקנה האמורה, בעל מאגר יבחן את מידת התאמתם לגישה למאגר מידע באמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם, וכל זאת בשים לב לרגישות המידע ולסוג הרשאת הגישה ויעדכן בהתאם לצורך את הרשאות הגישה ; העסיק בעל המאגר עד 100 עובדים כאמור, ישלים הבחינה תוך שישה חודשים מיום התחילה ; העסיק בעל המאגר מעל 100 עובדים כאמור, ישלים הבחינה תוך שנה מיום התחילה.
		תוספת ראשונה
		(תקנה 1 והתוספת השניה)

	1.	מאגרי מידע שחלה עליהם רמת האבטחה הבינונית:
		(1) מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר;
		(2) מאגר מידע שבעליו הוא גוף ציבורי כמשמעותו בסעיף 23 לחוק;
		(3) מאגר מידע הכולל מידע שהוא אחד מאלה:
		(א) מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד;
		(ב) מידע רפואי או מידע על מצבו הנפשי של אדם;
		(ג) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000 [5];
		(ד) מידע אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם;
		(ה) מידע אודות עברו הפלילי של אדם;
		(ו) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח –2007 [6];
		(ז) מידע ביומטרי;
		(ח) מידע כלכלי על אדם, לרבות אודות הרגלי הצריכה של אדם.
	2.	על אף האמור בפרט 1(3), על מאגר מידע המקיים אחד מאלה, לא חלה רמת האבטחה הבינונית;

[5] ס"ח התשס"א, עמ' 62.
[6] ס"ח התשס"ח, עמ' 72.

		(1) המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ה), (ו) ו-(ז) לעניין תמונות פנים בלבד, (ח) , אודות המועסקים או הספקים של בעל מאגר המידע, ובלבד שהמידע משמש למטרות ניהול העסק בלבד, ואינו כולל מידע מן הסוגים המפורטים בפרט1(3)(א), (ג),(ד) ו-(ז) לעניין מידע שאינו תמונות פנים;
		(2) מספר המועסקים אצל בעל המאגר אינו עולה על עשרה.
		תוספת שנייה
		(תקנה 1)
		מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה:
		(1) מאגר מידע כאמור בפרט 1(1) או (3) בתוספת הראשונה, שיש בו מידע אודות 100,000 אנשים ומעלה;
		(2) מאגר מידע כאמור בפרט 1(1) או (3) בתוספת הראשונה שמספר מורשי הגישה למידע בו עולה על 100.

_____התשע"ו
_____ 2016

(חמ 3-4469)
(2016-8515)

_____
איילת שקד
שרת המשפטים

מבוא

חוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק), קובע הוראות שונות וחובות המוטלות על בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע. אחת החובות המרכזיות היא חובת אבטחת המידע, שמטרתה צמצום החשש מפני שימוש לרעה או פגיעה בשלמות המידע. סעיף 17 לחוק הגנת הפרטיות קובע כי:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע."

ואילו "אבטחת מידע" מוגדרת בסעיף 7 לחוק באופן הבא:

"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;"

מטרת התקנות המוצעות לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע במאגרי מידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם. בשונה מאבטחת מידע באופן כללי, שמטרתה להגן על המידע של ארגון כנכס של אותו ארגון, המטרה של ההסדר המוצע היא מימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע, מפני שימוש לרעה במידע אודותיהם הן על ידי גורמים מחוץ לארגון והן על ידי העובדים. ניתן לומר כי עמידה בעקרונות המוצעים בתקנות אלה, תבטיח כי ניהול המידע בארגון באופן כללי - יהיה תקין.

התקנות מבקשות לקבוע מנגנונים וכלים פנים-ארגוניים, שמטרתם הפיכת אבטחת המידע במאגר המידע, בהתאם למאפייני המאגר, לחלק משגרת ניהול הארגון בכלל וניהול המידע בפרט. מטרת המנגנונים להמחיש בצורה ברורה יותר את חובותיהם ואחריותם של ארגונים בתחום אבטחת המידע.

המנגנונים המוצעים נחלקים למספר רבדים: ברובד הראשון נדרש בעל המאגר לקבוע מהו המידע המוגן ומהם הסיכונים הקשורים אליו. ברובד השני, נדרש הארגון לקבוע נהלים בתחום אבטחת המידע, שיסדירו בצורה מפורטת וברורה יותר את ההיבטים האלה. החובה לכתוב מסמכים המפרטים את הנהלים נגזרת מעקרונות יסוד של אבטחת מידע ושל ניהול תקין, ומאפשרת הנחלה של עקרונות אלה בתוך הארגון.

בנוסף, הנהלים מאפשרים לארגון גם להציג לצדדים שלישיים – לקוחותיו, ספקיו, בתי משפט, רשם מאגרי המידע ורגולטורים אחרים, את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט באמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה.

הרובד השלישי בתקנות המוצעות כולל הוראות מהותיות בתחום ניהול אבטחת המידע.

במישור האחריות הארגונית, ובהתאם להוראות סעיף 17 לחוק, נקבע כי האחריות הכוללת לעמידה בתקנות היא של בעל מאגר המידע (כלומר הגוף הציבורי או הפרטי שלמטרותיו ולצרכיו המידע נאסף ומעובד) ומנהל המאגר (כלומר מנכ"ל הגוף או בכיר אחר שהוא הסמיך לכך). כמו כן, רוב החובות יחולו באופן דומה גם על המחזיק במאגר מידע. כמו כן, נדרש כי ממונה אבטחת המידע יהיה כפוף ישירות לנושא משרה בכירה, באופן שיבטיח את עצמאותו המקצועית.

בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה ככל שהארגון הוא ארגון שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותיות יותר. תפיסה זו, של חובות מודולריות נגזרת ישירות מעקרון היסוד של אבטחת מידע שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטויה גם במסמכים דומים בעולם.

דברי הסבר

תקנה 1 – הגדרות

ההגדרות העיקריות בתקנות המוצעות הן אלה:

"**אירוע אבטחה חמור**" – ההגדרה של 'אירוע אבטחה חמור' רלוונטית לחובה המוטלת על בעל המאגר, הקבועה בתקנה 11, לדווח לרשם על קרות אירוע אבטחה חמור וכן להודיע, אם כך יורה הרשם, לנושא המידע העלול להיפגע מן האירוע. ההגדרה תלויה ברמת האבטחה שחלה על מאגר המידע והיא משקפת שקלול של מידת הנזק שייגרם כתוצאה מאירוע האבטחה. לגבי מאגר מידע שחלה עליו רמת האבטחה הבינונית, ההגדרה קובעת כי מדובר על אירוע שנעשה בו שימוש ללא הרשאה או בחריגה מהרשאה בחלק מהותי מן המאגר או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר, בעוד שבמאגר מידע שחלה עליו רמת האבטחה הגבוהה, מדובר על כל שימוש ללא הרשאה או בחריגה מהרשאה במידע מן המאגר או בפגיעה בשלמות המידע. ברמת האבטחה הגבוהה, כניסה למערכות המאגר באופן שמאפשר גישה למידע שבמאגר ללא הרשאה או בחריגה מן ההרשאה, תיחשב אף היא לאירוע אבטחה חמור. כך למשל, אירוע בו גורם שאינו מורשה נכנס למערכות המאגר ושתל בו תוכנה זדונית, וזאת גם אם טרם הוכח שימוש בפועל במידע. כאשר מזוהה גישה למערכות המאגר, לבעל מאגר המידע אין בהכרח דרך לדעת מהי מידת החשיפה של הגורם הבלתי מורשה למידע המצוי במאגר, מהו משך הזמן שבו הייתה קיימת גישה למערכות המאגר ולמאגר המידע עצמו, מה הן הפעולות אותן ביצע הגורם הבלתי מורשה, או אילו רוגלות או נוזקות הותקנו במערכת.

"**התקן נייד**" – ההגדרה כוללת בין היתר מחשב נייד ומחשב כף-יד, רט"ן, ואמצעי אחסון נתיקים אחרים כגון: תקליטורים, כונני פלאש למיניהם, כונני גיבוי ניידים.

"**מאגרים שחלה עליהם רמת האבטחה הבינונית**" – מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה. מאגרים אלה הינם מאגרים בעלי רגישות בינונית, שנקבעה בהתאם להערכת סיכון האבטחה שהם מייצרים, הנגזר מהיקף המועסקים וסוג המידע המעובד. הפרמטר הארגוני נבחר כפרמטר כמותי מוביל משום שהיקף מורשי הגישה למידע בארגון, הוא שקובע במידה רבה את היקף החשיפה של המידע, ובהתאם לכך מהווים אינדיקציה למידת הסיכון שבתפעול המאגר, ולצורך בהתמודדות עם סיכון זה באמצעות כלים בתחום אבטחת המידע.

"**מאגרים שחלה עליהם רמת האבטחה הגבוהה**" – אלה הם מאגרים שרגישותם נקבעה בהתאם לשילוב של פרמטרים המשקפים את הסיכון האבטחתי, היקף מורשי הגישה למידע, היקף נושאי המידע במאגר וסוג המידע המעובד. ההנחה היא כי סיכונים מערכתיים, לאוכלוסיות גדולות, ממוקדים במאגרים מסוג זה.

"**עובד**" – מטרת ההגדרה להתמקד בחובות הנוגעות למי שיש לו גישה למידע במסגרת פעילותו בארגון (למשל, ניהול הרשאות גישה, הדרכה וכו'), ולצורך כך המבחן הוא פונקציונאלי וגמיש. הוא אינו נשען על מבחנים מתחום דיני העבודה, אלא מתייחס למכלול בעלי ההרשאות לגישה למאגר שגישתם למידע נקבעת בידי הארגון בעל המאגר, ללא קשר למתכונת המשפטית של העסקתם, לרבות עובד קבלן.

"**רשת ציבורית**" – רשת תקשורת המאפשרת שימוש באופן שאינו מוגבל לעובד של בעל המאגר או המחזיק.

תקנה 2 – מסמך הגדרות המאגר

תקנות משנה (א) ו-(ב)

מטרת התקנה לייצר תהליך עבודה שיביא לכך שבעל מאגר המידע יגדיר את פעילות עיבוד המידע המבוצעת על ידו, תכליותיה, את סוגי המידע המצוי במאגר, רמת הרגישות שלו, ויבחן את הסיכונים השונים הנגזרים מפעילות זו ואופן ההתמודדות איתם. הגדרה ברורה של הנהלת הארגון בנושא זה משמשת נקודת מוצא חיונית לקבלת החלטות ומימוש האחריות הניהולית של בעל המאגר. זה הטעם לכך שחובה זו הוטלה על בעל המאגר, אשר הוא הקובע את תכליות איסוף ועיבוד המידע, ולא על המחזיק.

יצוין כי כבר היום, בהתאם לסעיף 9 לחוק, נדרש בעל מאגר שחלה עליו חובת רישום לכלול חלק מפרטים אלה בבקשת רישום המאגר.

תקנת משנה (ג)

הוראה זו קובעת כי על בעל המאגר לבחון אחת לשנה, אם המידע הנאסף והנשמר על ידו אינו מעבר לנדרש לצורך מימוש מטרות המאגר וזאת כדי להפחית את הסיכונים למידע.

תקנה 3 – ממונה על אבטחת מידע

לפי סעיף 17ב לחוק נדרשים גופים מסוימים למנות "ממונה אבטחה" שהינו בעל הכשרה מתאימה. התקנה המוצעת מבקשת לקבוע כללים יסודיים בעניינו של הממונה על אבטחת המידע, אשר יאפשרו לו למלא את חובתו לפי החוק. בכלל זה, התקנה קובעת כי ממונה האבטחה יהיה כפוף ישירות לנושא משרה בכירה, וזאת כדי להבטיח את בכירותו בארגון ואת עצמאות שיקול הדעת שלו; כי הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים, כגון מנהל מערכות המידע של הארגון (מנמ"ר) וכי יוקצו לו המשאבים הדרושים לשם מילוי תפקידו.
כמו כן נקבע כי ממונה האבטחה יכין נוהל אבטחת מידע שיאושר על ידי בעל המאגר, כאמור בתקנה 4, וכן תכנית לבקרה שוטפת על העמידה בהוראות התקנות, ולאחר ביצועה יודיע לבעל המאגר ולמנהל המאגר על ממצאיו.

התקנה חלה גם על ממונה על אבטחה שמונה בידי בעל מאגר, אף אם לא חלה עליו חובה למנות ממונה לפי סעיף 17ב לחוק.

תקנה 4 – נוהל אבטחה

התקנה מחייבת את בעל מאגר המידע לקבוע במסמך נוהל אבטחה ארגוני. מטרתו של הנוהל היא לייצר מדיניות אבטחה ארגונית אחידה ידועה ומחייבת, המתמודדת עם סיכוני האבטחה להם חשוף המידע במסגרת הפעילות השוטפת של בעל מאגר המידע, לקבוע כללים ונהלים המחייבים את כלל עובדי הארגון, וליצור מודעות לנושא.

נוהל האבטחה ייקבע לפי מסמך הגדרות המאגר והתקנות, ברמת פירוט ובהיקף משתנים בהתאם לרמת האבטחה החלה על מאגר המידע.

על הנוהל להיות מעודכן ותואם, בין היתר, את מצב מערכות המאגר, את הסיכונים הטכנולוגיים הקיימים ואת התקנות.

תקנה 5 – מיפוי מערכות המאגר וביצוע סקר סיכונים

תקנת משנה (א)

על מנת לאבטח את מאגר המידע כנדרש בחוק ובתקנות אלה, באופן ההולם את מאפייני המאגר הפרטני ואת הסיכונים שיוצרת פעילות עיבוד המידע בארגון, על בעל מאגר המידע למפות את מבנה המאגר וכן את מכלול רכיבי המערכות המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע (להלן - מערכות המאגר) שלו. כמו כן עליו להחזיק מסמך מעודכן של המיפוי, כאמור.

לכן בשלב הראשון נדרש בעל מאגר לערוך רשימת מצאי מסודרת של מערכות המאגר לרבות ציוד מחשב וסוגי ציוד תקשורת ואבטחת מידע (רכיבי החומרה), ותוכנות מחשב (רכיבי התוכנה), כמפורט להלן:

- מערכות החומרה כוללות בין היתר: מחשבי שולחן, שרתים, תחנות עבודה, מדפסות, אמצעי מיתוג, בקרה ואבטחת מידע כגון - התקני חומת-אש מבוססי חומרה, נתבים, מתגים, ומודמים, התקנים ניידים המתחברים לרשת כמו מחשבים ניידים, מחשבי כף יד, ואמצעי זיכרון ניידים.
- מערכות התוכנה כוללות בין היתר: מערכות הפעלה, יישומים (אפליקציות) לגישה לנתונים שבבסיסי הנתונים במאגר, יישומים לעיבוד נתונים, יישומי תקשורת נתונים ומערכות הגנה כגון: אנטי-וירוס, חומת-אש ותוכנות הגנה מפני תוכנות זדוניות.

קיומה של רשימת מצאי מסודרת של רכיבי החומרה ורכיבי התוכנה, מסייעת לאחראי על האבטחה במאגר, לבצע מעקב מתמיד אחר כל רכיבי מערכות המאגר, ללא חשש להשמטת אחד מהרכיבים. התמונה הכללית המתקבלת מהרשימה המלאה מעניקה לאחראי "מבט על" המאפשר זיהוי נקודות תורפה וסיכונים ונקיטת אמצעי אבטחה הולמים לטיפול בהם.

לתרשים הרשת, הכולל את מיקומם הפיזי של רכיבי המערכת השונים ואת הקשרים ביניהם, יש חשיבות רבה, מאחר שהוא מאפשר זיהוי של תהליכי העבודה במערכת, ובמקרה של ליקוי אבטחה, מאפשר לזהות את מקורו ואת תחומי השפעתו.

על מנת שלא לייצר סיכון אבטחת מידע, רשימת המצאי תישמר כך שפרטים ממנה יימסרו לעובדים רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

תקנת משנה (ב)

התקנה קובעת כי במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה, אין להסתפק בדרישות תקנת משנה (א), אלא יש לבסס את אבטחת המידע על מסמך מקיף ומעמיק יותר – "סקר הסיכונים". הכוונה בביטוי "סקר סיכונים" לסקר הנערך בידי אדם בעל הכשרה מתאימה במטרה לזהות ולהעריך את רמת הסיכון לפגיעה באבטחת מידע הקיימת בכל אחד מרכיבי מערכות המאגר,

תוצאות סקר הסיכונים תועברנה לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו. סקר הסיכונים יבוצע בתדירות של אחת לשמונה עשר חודשים לפחות, באופן שיתן מענה לשינויים שחלו במערכת ולאיומים חדשים.
מערכות תוכנה וחומרה נתונות באופן מתמיד לאפשרויות שדרוג, עדכון, ושינוי רכיבים. כל שינוי כזה במערכת החומרה או התוכנה, משפיע באופן ישיר על רכיבים אחרים במערכת אשר תלויים ברכיב שהשתנה או שהוא תלוי בהם. ההשפעה של כל שינוי עלולה לייצר סיכוני אבטחה חדשים, או ליצור שינוי במבנה המערכת, המחייב התייחסות בראי אבטחת המידע.

בנוסף, איומי אבטחה נוצרים חדשים לבקרים, עם גילוי פרצות או חשיפות במערכות נפוצות. לכן, יש צורך לקיים בחינה חוזרת של מבנה המערכת ורכיביה, כדי להפיק תמונת מצב עדכנית.

תקנת משנה (ג)

התקנה קובעת כי במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערכו גם מבדקי חדירות למערכות המאגר בתדירות של אחת לשמונה עשר חודשים לפחות. מדובר בשיטת הערכה של אבטחת מערכות המאגר על ידי סימולציה של התקפה ממוחשבת מחוץ לסביבת הבדיקה או מתוכה. מטרת מבדקי החדירות היא זיהוי החולשות הפוטנציאליות של מערכות המאגר, העלולות להיות מנוצלות לרעה על ידי תוקף אמיתי. תוצאות מבדקי החדירות תועברנה לבעל מאגר המידע שידון בהן ויפעל לתיקון הליקויים שנתגלו, ככל שנתגלו. התדירות, כאמור לעיל, נועדה לאתר מצבים יש שינוי במערכות התוכנה ו/או החומרה שעלול לגרום לסיכון אבטחה חדש או עקב איומי אבטחה חדשים שנוצרים שמצריכים בדיקה מחודשת של עמידות המערכת בסיכונים.

תקנה 6 – אבטחה פיזית וסביבתית

התקנה מחייבת שמירה על מידור פיזי של תשתיות ומערכות החומרה המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע. המערכות תמצאנה במקום מוגן, שכניסה אליו מתאפשרת רק לעובדים בעלי הרשאה מתאימה.

הקפדה על אבטחה פיזית של המערכות מונעת גישה של גורמים לא מורשים אל מערכות המידע. מניעת גישה זו חשובה מאוד לאור העובדה שהגדרות הליבה של המערכת ואמצעי ההגנה הלוגיים שלה ניתנים לשינוי ועדכון בשיטות שונות המתאפשרות על ידי הגישה הפיזית. גישה פיזית אף עלולה לאפשר גניבת אמצעי האחסון הפיזיים ובכך שימוש לא מורשה במידע.

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יש לתעד את הכניסות והיציאות של העובדים מאתרים בהם מצויות המערכות לעיל, וכן לתעד הכנסת ציוד אל מערכות המאגר והוצאת ציוד מהן. תיעוד מלא מאפשר מעקב ובקרה במקרה של כשל אבטחתי. באמצעות התיעוד ניתן להצביע על גורם הכשל, ולנקוט באמצעי פתרון מתאימים.

תקנה 7 – אבטחת מידע בניהול כח אדם

הגורם האנושי הינו גורם סיכון משמעותי בתחום אבטחת מידע. תובנה מקובלת המבוססת על לימוד של אירועי אבטחה, מלמדת כי שיעור גבוה של אירועי אבטחה נובע מהתנהלות בעייתית של כח האדם בארגון.

כחלק ממערך הצעדים הננקטים על מנת לשמור על אבטחת המידע שבמאגר, יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע, עובדים המתאימים לעבודה זו, מבחינת אמינותם ויושרם, וזאת באמצעות נקיטת אמצעים סבירים המקובלים בהליכי מיון ושיבוצם. סוג האמצעים שיינקטו והיקפם יהיה בשים לב לרגישות המידע שבמאגר ולהיקף הגישה שתהיה למועמד במסגרת הגדרת התפקיד אליו הוא מיועד. את האמצעים הסבירים, כאמור, יש לנקוט גם לגבי שינוי הרשאה שניתנה. אמצעים סבירים במקרה זה יכולים לכלול, למשל, שיחה עם מעסיקים קודמים, בדיקת המלצות וכו'. יצוין כי חובה זו תחול לפי הוראת המעבר הקבועה בתקנה 23 גם לעניין עובדים קיימים.

לאחר שהוחלט כי המועמד אכן מתאים לעבודה הנוגעת למאגרי המידע, בטרם מתן הגישה למאגר המידע או בטרם שינוי היקף הרשאה שניתנה, יש להדריך את העובד בנושא

חובותיו לפי חוק הגנת הפרטיות, לפי התקנות ולפי נוהל האבטחה ומסמך הגדרות המאגר. ההדרכות יכולות להיות מועברות על ידי ממונה על אבטחת המידע, או על ידי גורם מתאים אחר, ורצוי אף לצרף להדרכה חוברת מידע בסיסית המבהירה נושאים אלו בכתב. מובן כי היקף העיסוק בנושא משתנה בין ארגונים בהתאם לסיווג התפקיד.

בנוסף על האמור לעיל, במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יחויב בעל המאגר לערוך פעילויות הדרכה תקופתיות, לפחות פעם בשנה, על מנת "לרענן" את מודעות העובדים להוראות החוק. פעילויות ההדרכה יכללו סקירה של מסמכי האבטחה המחייבים בארגון בהיקף הנדרש לצורך ביצוע תפקידיהם של העובדים: הגדרות המאגר, נוהל האבטחה, וחובות אבטחת המידע לפי החוק והתקנות.

במסגרת ההדרכות יש להתייחס לסיכונים שונים למידע במאגר, ובין היתר גם לסיכון שגורמים שונים ינסו להשיג מידע אישי או גישה למידע אישי בדרכי מרמה או התחזות.

תקנה 8 – ניהול הרשאות גישה

התקנה מחייבת לוודא כי הגישה למאגר המידע ולמערכות המאגר תתאפשר רק לאותו עובד אשר נדרש לכך בהתאם להגדרת תפקידו. דרישה זו מתבצעת על ידי ניהול הרשאות גישה ורישומן. לכל תפקיד נקבעת רמת הרשאה מתאימה, המאפשרת לו את היקף הגישה הנדרש למילוי תפקידו, ולא מעבר לכך, בהתאם לגישת "הצורך לדעת" ("need to know").

תקנה 9 – זיהוי ואימות

תקנת משנה (א)

כדי לוודא שמי שניגש למידע במאגר המידע הינו אכן עובד מורשה ובהתאם להרשאה שניתנה לו ועל מנת למנוע גישה של גורמים עוינים מחוץ לארגון או שימוש לרעה מתוך הארגון, יש לאמת את זהותו של המורשה.

קיימים מספר מנגנונים המאפשרים אימות זהות של משתמש: שם משתמש וסיסמה, אמצעי חומרה פיזי (כגון כרטיס חכם), זיהוי ביומטרי, או שילוב של שניים או יותר מהאמצעים הללו.

תקנת משנה (ב)

במאגרי מידע שחלה עליהם רמת אבטחת המידע הבינונית או הגבוהה, על הארגון לקבוע בנוהל האבטחה הוראות לעניין האמצעים, כאמור בתקנה משנה (א), ובכללן בנושא אופן הזיהוי, אשר מומלץ כי יתבצע על בסיס אמצעי פיזי, הנתון לשליטתו הבלעדית של העובד. היה ונקבע כי אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל, בין היתר, ל"חוזק" סיסמאות. סיסמה "חזקה" היא סיסמה שקשה לפרוץ אותה, הואיל והיא ארוכה, מורכבת ממחרוזת תווים אקראית, ומשלבת סוגים שונים של תווים. לעומתה, סיסמה חלשה תהיה לרוב קצרה, בעלת היגיון פנימי (כמו רצף מספרים), או קשורה לבעלים שלה (כמו מספר הטלפון, תאריך לידה או מספר תעודת זהות). הקריטריונים יחייבו את העובדים להחליף סיסמה ראשונית שניתנה, ככל שניתנה, וליצור סיסמה מספיק חזקה לצורך הגישה שלהם למידע.

כמו כן, יקבע הנוהל את מספר הניסיונות להזנת סיסמה שגויה לפני שהמערכת חוסמת את אותו משתמש מגישה למערכת. חסימה זו מיועדת למנוע מצב של פיצוח הסיסמה על ידי ניסיונות חוזרים ונשנים של צירופים שונים.

בנוסף נדרש שהנוהל יקבע תדירות החלפת סיסמאות. התקנה מחייבת כי החלפת הסיסמאות תתבצע לפחות פעם בחצי שנה. בעת גישה למידע רגיש, החלפת הסיסמה היא אמצעי חיוני לצמצום הסיכון לשימוש לא נאות בסיסמה, שהרי גם במקרה שהסיסמה תיחשף באופן כלשהו, טווח הנזק יצומצם לזמן שיחלוף עד להחלפתה בלבד.
נוסף על כך, הנוהל יקבע ניתוק אוטומטי של משתמש לאחר זמן בו לא היה פעיל וכן את אופן הטיפול בתקלות שונות הקשורות באימות זהות.

תקנת משנה (ג)

במקרה של עזיבת עובד את מקום העבודה, התקנה מחייבת את בעל מאגר המידע לדאוג לביטול ההרשאות המוקצות לו, וכן לשנות במידת האפשר סיסמאות למאגר ולמערכות התומכות במאגר, שהעובד עשוי היה לדעת, מיד עם סיום תפקידו של העובד. זאת כדי למזער את הסיכון לגישה בלתי מורשית.

תקנה 10 – בקרה ותיעוד גישה

תקנת משנה (א)

במאגרי מידע שחלה עליהם רמת אבטחת המידע הבינונית או הגבוהה, מחייבת התקנה כי ינוהל מנגנון המתעד אוטומטית נתונים המצוינים בתקנה, בין היתר את זהות המשתמש ואת התאריך והשעה של ניסיון הגישה, כגון מנגנון שמירת לוגים פנימי המשולב בתוכנות ובמערכות הפעלה שונות, וזאת כדי לאפשר בקרה וביקורת על הגישה למערכות המאגר.

תקנת משנה (ב)

על המנגנון להיות עצמאי, לפעול באופן רציף, וככל הניתן ללא אפשרות התערבות חיצונית, כולל התערבות של מפעילו. באופן כזה, יישמרו אמינותו של המנגנון, ואמינות התיעוד. בהתקני Firewall פיזיים למשל, משולב מנגנון כזה במערך הניהול של ההתקן. אם בכל זאת בוצעו שינויים או ביטולים בהפעלת מנגנון הבקרה, הוא יאתרם ויפיץ התראות לאחראים.

תקנת משנה (ג)

התקנה מחייבת את בעל מאגר המידע לקבוע נוהל בדיקה שגרתי של נתוני התיעוד שהפיק מנגנון הבקרה. על בעל מאגר המידע מוטלת החובה לבחון את התיעוד באופן מקצועי ומעמיק. עליו להתייחס לא רק לניסיונות כניסה שהמערכת דחתה, אלא אף לניסיונות כניסה שאושרו, על מנת לנסות לאתר כניסות שאינן מורשות או שימושים לרעה בהרשאות הגישה. במידה שהבחינה אכן גילתה ליקויים, על בעל מאגר המידע לערוך דו"ח מסודר המפרט את הבעיות שנמצאו, ואת הצעדים שננקטו בעקבותיהן.

תקנת משנה (ד)

התקנה מחייבת לשמור את נתוני התיעוד האמור למשך שנתיים לפחות. באופן כזה תתאפשר בחינה מדוקדקת של התיעוד במקרה של אירוע נקודתי שהתגלה בטווח של עד שנתיים מאוחר יותר.

תקנת משנה (ה)

התקנה מחייבת את בעל מאגר המידע ליידע את עובדיו בדבר קיום התיעוד של פעולות הגישה שלהם למערכות המאגר ואת מאפייניו. יידוע זה נועד להבטיח את מודעותו של העובד למעקב אחר פעולותיו במערכות המאגר, וכן ליצור הרתעה.

תקנה 11 – תיעוד של אירועי אבטחה

תקנת משנה (א)

מטרת תקנה זו ליצור "זיכרון ארגוני" ביחסי לאירועי אבטחה, על מנת להפיק מהם לקחים לעתיד. ככלל מנחה שנועד להקל על תחקור כאמור, יש להתבסס ככל הניתן על רישומים אוטומטים אודות אירועי אבטחה במערכות המאגר של הארגון, כגון syslog snmp.

תקנת משנה (ב)

התקנה קובעת כי בנוהל האבטחה יקבע בעל מאגר הוראות לגבי התמודדות עם אירועי אבטחת מידע וכן לגבי דיווח להנהלת בעל המאגר אודות אירועי אבטחה ועל פעולות שננקטו בעקבותיהם. מטרת תקנה משנה זו להבטיח כי בקרות אירוע אבטחת מידע, יהיו בידי הארגון הכלים הנכונים והיעילים להתמודדות מהירה, וכן להבטיח כי אירועי האבטחה יובאו לידיעת ההנהלה הבכירה, שתוכל לקיים בקרה על כך שננקטו הפעולות המתאימות בעקבותיהם.

תקנות משנה (ג) ו-(ד)

לגבי מאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, קובעות תקנות המשנה את התדירות בה על בעל מאגר המידע לערוך דיון לעניין אירועי האבטחה.

החובה לערוך דיון מטרתה, בין היתר, למנוע הישנות אירועי אבטחה כאלה ולבחון אם מאפייני האירועים (כגון: כניסה בלתי מורשית למאגר, ניסיונות חדירה חיצוניים חוזרים ונשנים, שימוש חריג של עובד בהרשאתו לצורך גישה למשאבים ייחודיים), היקפם או חומרתם, מעוררים צורך לשנות את נוהל האבטחה.

תקנות משנה (ה) ו-(ו)

התקנה מחייבת את בעל מאגר המידע ליידע את הרשם באופן מיידי בקרות אירוע אבטחה חמור וכן לדווח לו על הצעדים שנקט בעקבות האירוע. הרשם במקרה כזה רשאי, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להורות לבעל מאגר המידע להודיע על האירוע לנושא המידע שעלול להיפגע ממנו, וזאת בין היתר על מנת למנוע את הפגיעה בו או לצמצמה.

בהתאם להחלטת הממשלה 2444 מיום 15.02.15 בנושא קידום ההערכות הלאומית להגנת הסייבר, הוקמה רשות לאומית להגנת הסייבר, אשר תפקידה לעסוק במכלול ההיבטים האופרטיביים הקשורים בהגנה בסייבר, ובכלל זה טיפול תגובה והכלה של אירועים בזמן אמת. מרכיב מרכזי ברשות הינו מרכז סיוע מרכז לסיוע בהתמודדות עם איומי סייבר (ה-CERT הלאומי) עבור כלל המשק, שתפקידו בין היתר לסייע בטיפול באיומי סייבר ואירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק ולהוות נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק.

ההיוועצות בראש רשות הגנת הסייבר הלאומית נדרשת כדי לקבל נקודת מבט רחבה יותר משום שלעתים אירוע אבטחה במאגר ספציפי הינו חלק ממכלול פעילות הקשורה להגנת הסייבר במרחב האזרחי, שרשות הסייבר מכירה היבטים נוספים שלו.

תקנה 12 –התקנים ניידים

התקנים ניידים כוללים לעניין תקנות אלה: מחשבים ניידים ומחשבי כף-יד, ואמצעי אחסון נתיקים כגון: תקליטורים, כונני פלאש למיניהם, כונני גיבוי ניידים וכיו"ב. התקנים אלה, מעצם טבעם כניידים, דורשים התייחסות מיוחדת, מאחר שככלל מדובר בהתקנים קטנים

יחסית, הניתנים להעברה ממקום למקום, ולפיכך קיים סיכון כי מידע עלול לדלוף החוצה באופן לא מורשה על ידי שימוש בהם. כדי למנוע מצב כזה מוצע לחייב נקיטה באמצעי הגנה סבירים על המידע המצוי על ההתקן הנייד, על מנת להקשות על שימוש בו בידי מי שאינו מורשה במקרה של אובדן ההתקן או גניבתו. קיימות שיטות שונות להגן על מידע בהתקנים ניידים. התקנה קובעת כי הצפנת המידע על ההתקן הנייד, על ידי שימוש נכון בשיטות הצפנה מקובלות, תיחשב נקיטת אמצעים סבירים.

בנוסף קיים סיכון גם **בעצם השימוש** בהתקנים ניידים, בשל החשש מנוזקות שיוחדרו למערכות המאגר באמצעות התקן נייד חיצוני, יפגעו בשלמות המידע במאגר או יגרמו לדליפת המידע לגורמים חיצוניים או פנימיים בלתי מורשים. לכן בשים לב לרגישות המידע, למטרת המאגר ולאמצעי הגנה המופעלים בו, על בעל המאגר לשקול את האפשרות להקשיח את מערכות המאגר באופן שיגביל או, במידת האפשר, ימנע לחלוטין חיבור התקנים ניידים למערכת.

תקנה 13 – ניהול מאובטח ומעודכן של מערכות המאגר

תקנת משנה (א)

התקנה קובעת כי על בעל מאגר להקפיד על ניהול ותפעול תקין של מערכות המידע המשמשות לביצוע פעולות במאגר. ניהול תקין, בין היתר, קובע סטנדרט תפעול אחיד ומקטין בכך את הסיכונים למערכות המידע.

תקנת משנה (ב)

גם אם מאגר המידע נמצא על מחשב אחד בלבד, הנעול בחדר מיוחד, אין פירושו כי המאגר מוגן מפני גישה לא מורשית. העובדה כי המחשב מחובר ברשת לשאר המחשבים, גורמת סיכון של כניסה למחשב באמצעות הרשת.

התקנה מחייבת את בעל המאגר להפריד ככל האפשר בין המערכות המשמשות את מאגר המידע, כמו השרת שעליו מותקן המאגר, ותחנות הקצה בעלות גישה למאגר, משאר מערכות המחשבים הארגוניות. זאת, על מנת למנוע קישוריות בלתי רצויה, אל מחשבים או מערכות אשר לא נזקקים להשתמש במאגר המידע. קישוריות זו, עלולה לגרום שימוש לא נאות במאגר המידע.

קיימות מספר שיטות להפרדה זו, ובהן: מערכת חומת אש פנימית, מערכת לחלוקת רשתות, ועוד.

תקנת משנה (ג)

מאחר שאיומי אבטחה נוצרים באופן שוטף, ומתגלות חולשות ופגיעויות חדשות מעת לעת, יש צורך בעדכון שוטף של מערכות ההגנה.

תקנה 14 – אבטחת תקשורת

תקנת משנה (א)

בהמשך לסכנות שנמנו בתקנה הקודמת, במידה ומערכות המאגר מחוברות לרשת האינטרנט או לרשת ציבורית אחרת, נוצר סיכון של גישה חיצונית מתוך רשת האינטרנט או הרשת הציבורית אל מערכות המידע של הארגון.

על מנת להקטין למינימום את הסיכון, התקנה מחייבת כי במידה ומערכות המאגר מתחברות לרשת האינטרנט, יש להתקין על גבי המערכות אמצעי הגנה מתאימים מפני חדירה לא מורשית, או תוכנות מזיקות. אמצעי ההגנה הנפוצים היום כוללים אמצעים אלה, ככל שהם מעודכנים : תוכנת אנטיוירוס, תוכנת הגנה בפני תוכנות זדוניות, תוכנת חומת אש, והתקן חומת אש פיזי.

מאחר שמערכות מידע רבות מתחברות לרשת האינטרנט, כולל בארגונים קטנים, חלה תקנה זו על מכלול בעלי המאגרים

תקנת משנה (ב)

העברת מידע באמצעות רשת האינטרנט עלולה להיות חשופה להתחקות ומעקב על ידי גורם זר המעוניין בהעתקת המידע ובשימוש בו. מידע הנשלח באמצעות רשת האינטרנט, עובר בדרכו, עד הגיעו ליעדו, תחנות רבות, אשר לבעל מאגר המידע אין אפשרות להבטיח את רמת האבטחה בהן. לכן, התקנה מחייבת להצפין בשיטת הצפנה מקובלת את המידע הנשלח באמצעות האינטרנט או רשת ציבורית אחרת.

תקנת משנה (ג)

מטרת תקנת משנה ג' לוודא כי לסיכונים שנוצרים בעת אפשרות של גישה מרחוק של עובדי הארגון, ספקיו ולקוחות, למערכות הארגון, יימצא פתרון, ולא תהיה פגיעה ברמת האבטחה הכוללת בשל כך. לצורך כך נדרש הארגון להפעיל מנגנונים שיבטיחו כי רק למורשים תהיה גישה למידע ובהיקף שניתן להם. לגבי מאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יש לעשות שימוש באמצעי פיזי, הנתון לשליטתו הבלעדית של העובד, כגון כרטיס חכם.

תקנה 15 - מיקור חוץ

כללי

מטרת התקנה להבהיר את חובות בעל המאגר בעת ביצוע פעולות במיקור חוץ, הכרוך במתן גישה למאגר המידע. מאחר שמתן הגישה למאגר המידע לגורם החיצוני לארגון יוצרת סיכונים מיוחדים משל עצמה, על בעל המאגר להתמודד עם סיכונים אלה. בהתאם לכך, על בעל המאגר לבחון את סיכוני אבטחת המידע הכרוכים בהתקשרות. על פי ההסדר המוצע, מעטפת אבטחת המידע של בעל המאגר תחול גם על המחזיק, תוך עיגון הוראות מתאימות בהסכם בין בעל המאגר והקבלן-המחזיק. על המחזיק תחול חובה לעמוד במסגרת זו.

תקנת משנה (א)

כאמור לעיל, בהסכם ההתקשרות בין הצדדים תהא התייחסות מפורשת לסוגיית אבטחת המידע. ההתייחסות תכלול, בין היתר, את סוג המידע אליו רשאי הגורם החיצוני לגשת, מטרות השימוש המותרות לו לצרכי ההתקשרות ובאמצעות אילו מערכות ; תכלית השימוש במידע, סוג העיבוד אותו הגורם החיצוני רשאי לבצע, ציון מפורש של משך תקופת ההתקשרות, חובות אבטחת המידע של הגורם החיצוני והתחייבות עובדיו לעמוד בהן.

לאחר עריכת ההסכם בין הצדדים, מחייבת התקנה את עדכון נוהל האבטחה של בעל המאגר, תוך ציון ההרשאות שניתנו לגורם החיצוני, והפניה למסמך שנחתם בין הצדדים. עדכון זה מאפשר פיקוח יעיל יותר על ביצוע פעילותו של הגורם החיצוני בתחום המוגדר לו, ועל עמידתו בהוראות התקנות וההסכם, כפי שמחייבת התקנה.

תקנת משנה (ב)

התקנה מבהירה כי הוראות התקנה לא חלות על עובד, דהיינו תכליתה להתמודד עם מיקור חוץ של פעילות מחוץ לארגון.

תקנה 16 – ביקורות תקופתיות

תקנת משנה (א)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תחול על בעל מאגר מידע חובת עריכת ביקורת, אחת לשנתיים לפחות, שבמסגרתה ייבחנו, בין היתר, אמצעי האבטחה המיושמים, תוך בדיקה האם הם עומדים בנוהל האבטחה ובתנאי התקנות.
הביקורת יכולה להיות פנימית – באמצעות עובדי הארגון (אך לא על ידי ממונה האבטחה של המאגר), או חיצונית – באמצעות גורם חיצוני, ועל הגורם, המבצע את הביקורת, להיות בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע. לעניין בעל מאגר מידע שחלה עליו רמת האבטחה הגבוהה, רשאי הוא לקיים את החובה במסגרת סקר הסיכונים, ובלבד שיעמוד בדרישות המהותיות של תקנת משנה (ג).

תקנת משנה (ג)

דוח הביקורת יכלול את מסקנות עורך הביקורת לגבי יעילות אמצעי האבטחה והתאמתם לנוהל האבטחה ולתקנות, וכן את מסקנותיו לגבי ליקויי אבטחה, אם נמצאו, והצעותיו לפתרונם. כמקובל, על דוח כאמור להסתמך גם על ממצאים ישירים ממערכות המאגר.

תקנה 17 – שמירת נתוני אבטחה

יישום החובות המוטלות בתקנות מביא לצבירת נתונים כגון נתוני בקרה על כניסה ויציאה, נתוני תיעוד של מנגנון הבקרה וכו'. על כלל הנתונים האלה להישמר באופן מאובטח, משני טעמים. האחד - על מנת לאפשר בדיקה בדיעבד של אירועי אבטחה או ליקויים אחרים, יש להבטיח כי נתונים אלה יהיו זמינים. השני - על מנת למנוע זליגה של נתונים אלה, שעלולה כשלעצמה לסכן את אבטחת המידע.
אין באמור כדי לגרוע מכך, שנתונים המהווים "מידע" הנצברים ב"מאגר מידע" כהגדרתם בסעיף 7 לחוק, כפופים לשאר הוראות התקנות.

תקנה 18 – גיבוי, שחזור

מערכות מחשב עלולות לקרוס באופן פתאומי בעטיים של גורמים שונים: התיישנות המערכת, תקלה טכנית, התקפה יזומה על ידי גורם זר, וירוס אלים ועוד. במקרה של אבדן נתונים השמורים במערכת , שחזור הנתונים כרוך בהשקעת משאבים רבים, ולעיתים אף אינו אפשרי.

לפיכך מוצע בתקנה זו כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה תהיה חובה לקבוע במסמך נהלי עבודה לשמירת גיבויים של הנתונים הנצברים ונהלי שחזור מתאימים.

תקנה זו מחייבת את בעל מאגר המידע לקבוע במסמך נהלי גיבוי לביצוע גיבויים באופן תקופתי שגרתי ("גיבוי" משמעותו: יצירת עותק נוסף של המידע המגובה, עדכני לזמן שבו נוצר הגיבוי). אם נמחקים הנתונים או שהמערכת קורסת, ניתן לגשת לאותו גיבוי, ולהפיק ("לשחזר") ממנו את הנתונים הנצברים. כמו כן, על בעל מאגר המידע לקבוע במסמך נהלים לשחזור המערכת במקרה של אבדן הנתונים האמורים.

הליך השחזור יתועד ברישום אירועי האבטחה לפי תקנה 11.

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, חלה דרישה נוספת שלפיה עותק גיבוי של המידע ושל נהלי השחזור יישמר באופן שיבטיח את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס, כגון במיקום נפרד מהאתר בו מוחזק המאגר.

תקנה 19 – חובות בעל מאגר החלות על מנהל מאגר ומחזיק בו

תקנת משנה (א)

סעיף 17 לחוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על בעל המאגר, המנהל והמחזיק. בהתאם לכך, התקנה קובעת כי החובות החלות על בעל מאגר המידע תחולנה גם על מנהל המאגר ובשינויים המחויבים לפי העניין, גם על מחזיק המאגר (למעט החובות הקבועות בתקנות 2 ו – 15(א)).

תקנת משנה (ב)

כחלק מניהול תקין ומאחריותיות (Accountability), כל מי שמוטלת עליו חובה או אחריות לביצוע פעולה, נדרש לתעד את ביצועה. תיעוד זה יאפשר, בין היתר, הצגת ביצוע הפעולה לצדדים שלישיים וכן בקרה ופיקוח.

תקנה 20 – סמכויות הרשם

תקנת משנה (א)

התקנות מציגות מסגרת בסיסית המכילה את העקרונות לאבטחת המידע במאגרי מידע, לפי רמות אבטחה. לעתים ישנם מאגרי מידע שבשל מאפיינים שונים שלהם - גודלם, היקף פעילותם, מספר העובדים המועסקים בהם או בשל סוג המידע הכלול בהם, יש מקום להקל את דרישות אבטחת המידע המוטלות עליהם לפי התקנות או לחילופין להחיל עליהם חובות לפי התקנות. לפיכך מוצע לתת לרשם סמכות לפטור מאגרים מסוימים מחובות אבטחת המידע לפי התקנות או לחילופין להחיל חובות, כאמור, על בסיס אמות המידה האמורות.

תקנת משנה (ב)

ישנם מסמכים מנחים שונים בעניין אבטחת מידע - תקנים רשמיים, תקנים ישראליים, תקנים בינ"ל או מסמכי ייחוס, שהרשם אישר לעניין זה, אשר עמידה בתנאיהם תיראה כקיום רמת אבטחת מידע ראויה, שיש בה כדי להתמודד באופן ראוי עם הסיכונים הקשורים בתחום זה, אף אם אינם תואמים אחת לאחת את הוראות תקנות אלה. לשם הקלה על הנטל הבירוקרטי המוטל על בעלי המאגרים, יעילות, אחידות וחיסכון במשאבים, מוצע לתת לרשם סמכות להורות שעמידה בהוראות מסמך מנחה בעניין אבטחת מידע או בהנחיות של רשות מוסמכת בעניין אבטחת מידע, תפטור מתחולת התקנות כולן או חלקן, אם השתכנע כי עמידה בהוראות או בהנחיות, כאמור, באופן שהורה לפי תקנות אלה, מבטיחה את רמת האבטחה הקבועה בתקנות אלה לגבי אותו מאגר מידע.

תקנה 21 – תחולה וסייגים לתחולה

כאמור לעיל במבוא, בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה, ככל שמאגר המידע הוא מאגר שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותית יותר ותוחלת הנזק גדולה יותר, הן בשל רגישות המידע, הן בשל היקף נושאי המידע והן בשל היקף מורשי גישה. לפיכך רמות האבטחה לפי התקנות המוצעות מחולקות לשלוש קבוצות שונות של מאגרי מידע כאמור לעיל בדברי ההסבר לתקנה 1. תפיסה זו, של חובות מודולריות נגזרת כאמור ישירות מעקרון היסוד של אבטחת מידע, שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטויה גם במסמכים דומים בעולם.

כמו כן מוצע כי מאגר מידע אשר רק לאדם אחד שאינו תאגיד יש גישה אליו (נורמטיבית ומעשית) והוא בעל המאגר, אזי יהיה בעל המאגר פטור מהוראות התקנות, בשל הסיכון המופחת הנובע מכך שאין צורך לנהל את המורשים למאגר ולפקח עליהם, זאת למעט מספר הוראות בסיסיות של אבטחת מידע שיש להחיל על כל מאגר מידע שהוא.

תקנה 22 – תחילה

התקנה קובעת תקופות תחילה שונות, בשים לב לנטל הארגוני ולצורך בהיערכות לצורך יישום כל תקנה ותקנה.

תקנה 23 – הוראת מעבר

תקנה 7(א) מטילה חובה על בעל מאגר לנקוט באמצעים סבירים, המקובלים בהליכי מיון עובדים, כדי לוודא את התאמת העובד לקבלת גישה למידע במאגר, וזאת בטרם תינתן ההרשאה. תחילתה של תקנה זו 30 יום מפרסום התקנות.
ואולם, לגבי עובדים קיימים שכבר קיבלו הרשאות גישה לפני יום התחילה, לבעל המאגר יעמדו חצי שנה או שנה (בהתאם למספר העובדים בעלי הרשאות הגישה ביום התחילה), על מנת לבדוק את מידת התאמתם לקבלת הגישה. הבדיקה תעשה במסגרת האמצעים הסבירים המקובלים בהליכי מיון עובדים ושיבוצם, וזאת בהתאם למידת רגישות המידע ולסוג הרשאת הגישה.