בתוקף סמכותי לפי סעיף 36 לחוק הגנת הפרטיות, התשמ"א-1981[1] (להלן – החוק או חוק הגנת הפרטיות), 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, 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;
		"בעל הרשאה" - יחיד אשר יש לו גישה לאחד מאלה על פי הרשאתו של בעל המאגר או המחזיק:
		(1) מידע מהמאגר;
		(2) מערכות המחשוב של המאגר;
		(3) מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו.
		על אף האמור, מחזיק שאינו יחיד או יחיד שקיבל גישה על פי הרשאה של מחזיק, לא ייחשב כבעל הרשאה של בעל המאגר;
		"התקן נייד" - אחד מאלה:
		(1) מחשב המיועד לשימוש נייד, לרבות מחשב שהוא ציוד קצה רט"ן כהגדרתו בפקודת הטלגרף האלחוטי [נוסח חדש], תשל"ב-1972;
		(2) מצע אחר המשמש לאחסון חומר מחשב;
		"חומר מחשב" ו- "מחשב" – כהגדרתו בחוק המחשבים, התשנ"ה- 1995[3];
		"מאגר המנוהל בידי יחיד" - מאגר מידע שמנהל יחיד או תאגיד בבעלות יחיד, ואשר רק היחיד ולכל היותר שני בעלי הרשאה נוספים רשאים לעשות בו שימוש ובאפשרותם לעשות בו שימוש, ולמעט מאגרי מידע כמפורט להלן:

Deleted: -

Deleted: לרבות אירוע בו היתה כניסה למערכות המאגר באופן שמאפשר גישה למידע שבמאגר,

Deleted: עובד

Deleted: המועסק על ידי בעל מאגר או מחזיק, במישרין או בעקיפין, ו

Deleted: בנוגע למאגר מידע

Deleted: ובכלל זה רדיו טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים), התשמ"ב-1982[2]

Deleted: "מאגר מידע" ו-"רשם" - כהגדרתם בפרק ב' לחוק;

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

			"מאגרים שחלה עליהם רמת האבטחה הבסיסית" – מאגרי מידע שאינם מן הסוגים המפורטים בתוספת הראשונה או השניה ואינם מאגר המנוהל בידי יחיד;
			"מאגרים שחלה עליהם רמת האבטחה הבינונית" - מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה ואינם מאגר המנוהל בידי יחיד;
			"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;
			"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;
			"הרשות הלאומית להגנת הסייבר" – הרשות הלאומית להגנת הסייבר שייעודה הגנת על מרחב הסייבר, שהוקמה על פי החלטת הממשלה ופועלת בהתאם להחלטותיה;
			"רשת ציבורית" – רשת תקשורת המאפשרת שימוש גם על ידי מי שאינו בעל הרשאה.
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;
			(2) תיאור מטרות השימוש במידע;

(1) מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר;

(2) מאגר מידע שיש בו מידע אודות 10,000 אנשים ומעלה;

(3) מאגר מידע הכולל מידע שבעל המאגר כפוף בשלו לחובת סודיות מקצועית לפי דין או לפי עקרונות של אתיקה מקצועית.

Formatted: Normal, Justified, Line spacing: 1.5 lines, No widow/orphan control, Keep lines together, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Font Alignment: Center, Tab stops: 0.43", Left + 0.87", Left

Deleted: עובד

Deleted: לצורך פעילותו (להלן – פעולות שימוש 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) פעולות עיבוד מידע באמצעות מחזיק;	Deleted: פירוט
			(6) הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם;	
			(7) שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע בו, אם מונה כזה.	
			(ב) בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי 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) ממונה אבטחה יהיה 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;	Deleted: בעל מאגר לא ימנה Deleted: על Deleted: אלא אם כן הוא
			(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;
			(6) 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) בהתאם למסמך הגדרות המאגר ותקנות אלה, אשר יחייב את כל בעלי ההרשאה בהתאם לפרטים מהנוהל שאליו הוא חשוף לפי תקנת משנה (ב).
		(ב)	בעל מאגר מידע ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.
		(ג)	נוהל האבטחה יכלול, בין היתר, את כל אלה:
			(1) הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר כאמור בתקנה 6.
			(2) הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8;
			(3) תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;
			(4) הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;
			(5) הסיכונים שחשוף להם המידע שבמאגר 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 המאגר;
			(6) אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11, לפי חומרת האירוע ומידת רגישות המידע;
			(7) הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12;

Deleted: לפי
Deleted: את כל העובדים
Deleted: לעובדים
Deleted: התייחסות ל
Deleted: ¶
[1] ...
Deleted: ,
Deleted: תשתיות המחשוב, תקשורת ואבטחת המידע
Deleted: המחשוב ותשתיות התקשורת של
Deleted: ,
Deleted: תשתיות המחשוב, התקשורת ואבטחת המידע
Deleted: רגישות הקשורות אליו

			(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל האבטחה, בנוסף לאמור בתקנת משנה (ג), התייחסות גם לכל אלה:	
			(1) אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9;	
			(2) אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר כאמור בתקנה 10;	
			(3) הוראות לעניין עריכת ביקורות תקופתיות לוידוא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16;	
			(4) הוראות לעניין גיבוי הנתונים האמורים בתקנה 18(א)(1);	
			(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;	

Deleted: הוראות בעניין האבטחה הפיזית והסביבתית של מיתקני המאגר כאמור בתקנה 6.

Formatted: No bullets or numbering

Formatted: Indent: Left: 0", Line spacing: single, Widow/Orphan control, Don't keep lines together, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.43" + 0.87"

D ... [2] ¶

D ... [3] ¶

			(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) המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.
			(ג) 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 מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.
			(ד) 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.
			(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 (ג) ו-(ד) 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.

D: ¶ ... [4]

Deleted: ב

Deleted: ג

		(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.	
Deleted: לעובד	אבטחת מידע בניהול כח אדם	7. (א) לא ייתן בעל מאגר מידע 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 בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר; אמצעים כאמור יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקיד שמיועד לו הנוגע בדבר, כאמור בתקנה 8.	
Deleted: העובד			
Deleted: העובד			
Deleted: לעובדים		(ב) בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם יקיים בעל מאגר מידע הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע אודות חובותיהם לפי החוק ונוהל האבטחה.	
Deleted: לעובדיו		(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור תיערך אחת לשנתיים לפחות, ולגבי הסמכה של בעל הרשאה לתפקיד חדש - סמוך ככל האפשר למועד תחילת הסמכתו.	
Deleted: העובדים			
Deleted: לשנה			
Deleted: עובד			
Deleted: עובדים	ניהול הרשאות גישה	8. (א) בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.	
Deleted: העובדים		(ב) בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).	
Deleted: לפי רשימת ההרשאות התקפות	ניהול ואימות	9. (א) בעל מאגר מידע ינקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות.	
Deleted: למידע במאגר המידע			
Deleted: עובד			
Deleted: , ייקבעו בנוהל האבטחה גם הוראות לעניין האמצעים כאמור בתקנת משנה (א), ובכללן בנושאים אלה:		(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה –	

(1) אופן הזיהוי, ייעשה ככל הניתן על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה;

(2) ייקבעו בנוהל האבטחה גם הוראות לעניין האמצעים כאמור בתקנת משנה (א), ובכללן בנושאים אלה:

(א) אופן הזיהוי; 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;

(ב) ניתוק אוטומטי לאחר פרק זמן של אי פעילות;

(ג) אופן הטיפול בתקלות הקשורות באימות זהות.

		(ג) בעל מאגר מידע ידאג לביטול ההרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.
בקרה ותיעוד גישה	10.	(א) 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.
		(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 בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

Deleted: ש

Deleted: 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;

Deleted: עובד

Deleted: שהעובד

Deleted: העובד

Deleted: בקרה ו

Deleted: העובדים

תיעוד של אירועי אבטחה	11.	(א) בעל מאגר מידע אחראי לתיעוד כל מקרה בו התגלה אירוע המעלה 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; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות.
		(ד) ארע אירוע אבטחה חמור –
		(1) יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע;
		(2) 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 ואת קיומם 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 באותו מאגר המידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.

Deleted: ים
Deleted: ים
Deleted: .
Deleted: ¶ (ד)
Deleted: בתקנת משנה (ג)
Deleted: ה
Deleted: ,
Deleted: .
Deleted: (ו) ארע אירוע אבטחה חמור,

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 מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן; לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.			Deleted: המערכות והתוכנות המשמשות לגישה אל המידע במאגר המידע ולהגנה עליו
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 בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה.			Deleted: עובד Deleted: ה Deleted: 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) אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;	Deleted: החלות על הגורם החיצוני
				(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);	Deleted: עובדיו
				(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 על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה (1).	Deleted: כדי לוודא את

			(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 התקשרות של בעל מאגר עם יחיד.
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.
			(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 את 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.		(א) בעל מאגר מידע ישמור את הנתונים הנצברים במסגרת יישום הוראות תקנות 6(ב), 8 עד 11, 14, 15(א)(4) ו-16, ככל שתקנות אלה חלות עליו, באופן מאובטח למשך 24 חודשים.
			(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר יגבה את הנתונים שנשמרו כאמור בתקנת משנה (א), באופן שיבטיח שניתן יהיה, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי.
גיבוי ושחזור	18.		(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר במסמך -
			(1) נהלים לביצוע גיבוי באמור בתקנה 17(ב), באופן תקופתי שגרתי;

Deleted: עובד

Deleted: , ויסתמך גם על ממצאים ממערכות המאגר

Deleted: לצורך עמידה

Deleted: ב

Formatted: Numbered + Level: 1 + Numbering Style: א, ב, ג, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.43" + Indent at: 0"

Deleted: עבודה

Deleted: של הנתונים הנצברים לצורך עמידה בהוראות תקנות 6(ב), 8 עד 11, 14, 15(א)(4) ו- 16

			(2) נהלים, להבטחת שחזור הנתונים כאמור בתקנה 17(ב), ובלבד שביצוע השחזור יהיה באישור מנהל המאגר;
			(3) כי במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע, 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)(1) 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 שאינה יצירת מסמך, נדרש לתעד באופן סביר את אופן ביצוע הפעולה לפי העניין; הרשם רשאי לתת הוראות לעניין אופן תיעוד כאמור.
סמכויות הרשם	20.		(א) (1) הרשם רשאי, אם ראה כי קיימים טעמים שמצדיקים זאת, לפטור מאגר מסוים מחובות אבטחת מידע לפי תקנות אלה, או להחיל על מאגר מסוים חובות לפי תקנות אלה, כולן או חלקן, לפי נסיבות העניין, ובין היתר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר או מספר בעלי ההרשאות בו; (2) פטור מחובות או החלת חובות לפי פסקה (1) ייעשה בהודעה בכתב לבעל המאגר; 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 המסמך המנחה בעניין אבטחת מידע או בהנחיות הרשות המוסמכת, לפי העניין, באופן שהורה לפי תקנות אלה, מבטיחה את רמת האבטחה הקבועה בתקנות אלה לגבי אותו מאגר מידע; לעניין זה –

Deleted: כדי להבטיח

Deleted: שבכל עת ניתן יהיה לשחזר את הנתונים האמורים בפסקה (1) למצבם המקורי

Deleted: לפי התקנה האמורה

Deleted: , בהודעה בכתב לבעל המאגר,

Deleted: העובדים

Deleted: תקן מקובל

Deleted: אלה

			"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.
תחולה וסייגים לתחולה	21.	בתקנות אלה -	
			(1) על מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה יחולו כל הוראות התקנות;
			(2) על מאגרי מידע שחלה עליהם רמת האבטחה הבינונית – יחולו תקנות 1 עד 4, 5(א), (ד) ו-(ה), 6 עד 10, 11 עד 15, 16(א), (ב), (ג) ו-(ה), 17, 18(א), 19, 20, 22 ו-23);
			(3) על מאגרים שחלה עליהם רמת האבטחה הבסיסית - יחולו תקנות 1 עד 3, 4(א), (ב), (ג), (ה) ו-(ו), 5(א), (ד) ו-(ה), 6(א), 7(א) ו-(ב), 8, 9(א) ו-(ג), 11(א) ו-(ב), 12 עד 15, 17, 19, 20, 22 ו-23.
			(4) על מאגר המנוהל בידי יחיד יחולו תקנות 1, 2, 6(א), 9(א), 11(א), 12 עד 14, 20 ו-22.
תחילה	22.	(א) תחילתן של תקנות אלה – שנה מיום פרסומן.	
הוראת מעבר	23.	על אף האמור בתקנה 7(א), בנוגע למי שהם 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 בעלי הרשאות כאמור, ישלים הבחינה תוך שישה חודשים מיום התחילה; העסיק בעל המאגר מעל 100 בעלי הרשאות כאמור, ישלים הבחינה תוך שנה מיום התחילה.	
ביטול	24.	תקנות 2, 3, 9, 10, 12, 13, 14 ו-15 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986 – בטלות.	
יחס לחיקוקים אחרים	25.	תקנות אלה יחולו בנוסף להוראות בעניין אבטחת מידע בחיקוקים אחרים, זולת אם יש סתירה ביניהם.	

[4] ס"ח התשי"ג, עמ' 30.

Deleted: יחולו על
Deleted: למעט
Formatted: Right: 0"
Deleted: -
Deleted: (ג), (ה)-(ו), 12
Deleted: 5(ב), ו-(ג), 11(ד), 16(ד) ו-18(ב)
Deleted: מאגרי מידע שאינם מאגרים שחלה עליהם רמת האבטחה הבינונית או הגבוהה
Formatted: Right: 0"
Deleted: 10,
Deleted: למעט תקנות 4(ד), 5(ב) ו-(ג), 6(ב), 7(ג), 9(ב), 10, 11(ג) עד (ו), 16 ו-18
Deleted: -(ב)
Deleted: (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.
Deleted: <#>תחילתן של תקנות אלה, למעט כאמור בתקנות משנה (ב) עד (ד), 30 ימים מיום פרסומן.¶ <#>תחילתן של תקנות 2, 3(1) עד (3), 10(א) , 13(ב) ו- 14– 90 ימים מיום פרסומן.¶ <#>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. ¶
Deleted: 4 ו- 9(ב)
Deleted: תשעה חודשים
Deleted: לעובדים
Deleted: עובדים
Deleted: עובדים

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, אף אם לא התקיימו בו הוראות פסקה (1) או (3);		
(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 על נכסיו של אדם, התחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם;		
(ט) הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים (א) עד (ז) או על אישיותו של אדם, אמונתו או דעותיו.		

Deleted: כלכלי על אדם,

Deleted: לרבות אודות

Deleted: ה

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

	2.	על אף האמור בפרט 1(3), על מאגר מידע המקיים אחד מאלה, לא חלה רמת האבטחה הבינונית אלא רמת האבטחה הבסיסית;
		(1) המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ה), (ו), (ז) לעניין תמונות פנים בלבד ו-(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 בעלי ההרשאה 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, לרבות מאגר של גוף ציבורי כמשמעותו בסעיף 23(1) לחוק המקיים את האמור בפרטים (1) או (3), שיש בו מידע אודות 100,000 אנשים ומעלה;
		(2) מאגר מידע כאמור בפרט 1(1) או (3) בתוספת הראשונה, לרבות מאגר של גוף ציבורי כמשמעותו בסעיף 23(1) לחוק המקיים את האמור בפרטים (1) או (3), שמספר בעלי ההרשאה בו עולה על 100.

Deleted: ו-

Deleted: ,

Deleted: המועסקים

Deleted: מורשי הגישה למידע

התשע"ו_____

2016 _____

(חמ 3-4469)

(2016-8515)

_____

איילת שקד

שרת המשפטים

Page 4: [1] Deleted **הלשכה המשפטית - אלעזר שטרן** **10/31/2016 11:57:00 AM**

			פרטים על העניינים המפורטים בתקנה 5 (א) ;

Page 5: [2] Deleted **הלשכה המשפטית - אלעזר שטרן** **10/31/2016 11:59:00 AM**

			הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12 ;

Page 5: [3] Deleted **הלשכה המשפטית - אלעזר שטרן** **10/31/2016 3:56:00 PM**

			הוראות לעניין עריכת ביקורות תקופתיות לוידוא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16 ;

Page 6: [4] Deleted **הלשכה המשפטית - אלעזר שטרן** **10/31/2016 3:57:00 PM**

			רשימת מצאי תישמר כך שפרטים ממנה יימסרו לעובדים רק בהיקף הנדרש לצורך ביצוע תפקידיהם.