הרשות להגנת הפרטיות
משרד המשפטים

המדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע)

03-7634050 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL
חפשו אותנו גם בפייסבוק

תוכן עניינים

היו ערוכים ומוכנים...

לקראת כניסתן לתוקף של תקנות הגנת הפרטיות (אבטחת מידע) ב-8 במאי 2018, בידקו האם אתם ערוכים ומוכנים לכך. מדריך זה כולל מידע אודות כלל סעיפי התקנות.

מידע על תקנות המתייחסות למאגר מידע המנוהל בידי יחיד עומד לרשותכם במדריך ייעודי לעצמאים ועסקים קטנים.

מהי אבטחת מידע?

אבטחת מידע פירושה הגנה על שלמות המידע והגנה עליו מפני חשיפה, שימוש או העתקה, על ידי גורמים שאינם מורשים.

על מי חלות התקנות?

התקנות חלות על כל המשק הישראלי, והן מבקשות להגן על האנשים שמידע אודותיהם קיים במאגר המידע.

אז איך זה עובד?

על אילו מאגרים חלה רמת האבטחה הבסיסית? הבינונית או הגבוהה?

התקנות קובעות שלוש רמות של מאגרי מידע, עליהן חלות רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים.

בשלב ראשון אתם נדרשים לבחון מהי רמת האבטחה שחלה על המאגר שבבעלותכם. למסקנה זו תוכלו להגיע באמצעות ביצוע תקנה 2 כמפורט בהמשך:

על אילו מאגרים חלה רמת האבטחה הבסיסית?

מדובר במאגרים **שלא חלה** עליהם **רמת האבטחה הבינונית או הגבוהה, ואינם מאגרים המנוהלים בידי יחיד.**

מהו מאגר המנוהל בידי יחיד? מדובר במאגר מידע שמנהל יחיד או תאגיד בבעלות יחיד, ואשר רק היחיד ולכל היותר שני בעלי הרשאה נוספים רשאים לעשות בו שימוש - **ראו מדריך תקנות אבטחת מידע למאגר המנוהל בידי יחיד.**

אם המאגר שבבעלותכם אינו מאגר המנוהל בידי יחיד, עליכם לבדוק אם על המאגר חלה רמת האבטחה הבינונית או הגבוהה. אם שתי הרמות הללו לא חלות - מדובר במאגר שחלה עליו רמת האבטחה הבסיסית.

על אילו מאגרים חלה 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** (משרדי הממשלה, רשות מקומית וכו');
3. מאגר מידע הכולל מידע על **צנעת חייו האישיים של אדם, מידע רפואי, מידע גנטי, מידע על דעות פוליטיות, מידע על עבר פלילי, נתוני תקשורת, מידע ביומטרי, מידע על נכסיו של אדם וכו', הרגלי צריכה.**

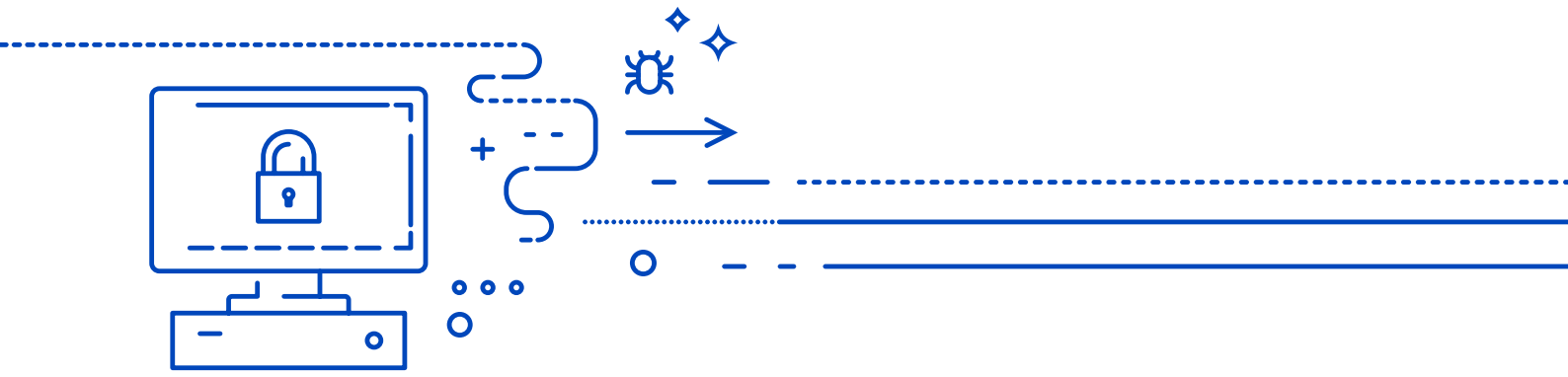
שימו לב!

בכל אחד מהמקרים הבאים תחול על המאגר רמת האבטחה **הבסיסית**, ולא הבינונית:

1. מאגר הכולל מידע רפואי או מידע על מצבו הנפשי של אדם, מידע על עבר פלילי, מידע על נתוני תקשורת ומידע ביומטרי אם מדובר בתמונות פנים בלבד, **או:** מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי וכו', בתנאי שהמידע מתייחס רק למועסקים או הספקים של בעל מאגר המידע, ומשמש לניהול העסק בלבד, ואינו כולל את המידע הבא: צנעת חייו של אדם; מידע גנטי; מידע על דעות פוליטיות; מידע ביומטרי לעניין מידע שאינו תמונת פנים והרגלי צריכה של אדם.
2. מספר בעלי ההרשאה אצל בעל מאגר המידע אינו עולה על עשרה.

על אילו מאגרים חלה רמת האבטחה הגבוהה?

מדובר במאגרי מידע שחלה עליהם רמת האבטחה הבינונית (ראו לעיל), שיש בהם **מידע על אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה בו עולה על 100.**



איך ממשיכים מכאן?

לאחר שבדקנו מהי רמת האבטחה החלה על המאגר, יש לפנות לטבלה הבאה המתייחסת לתקנות החלות על מאגרי המידע, בהתאם לרמת אבטחתם (תקנה 21):

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			

להלן יובאו הסברים על הוראות התקנות. לצד כל הסבר מופיע מספר התקנה:

תקנה 2 מסמך הגדרות המאגר

במסמך זה יש להגדיר את כל העניינים האלה:

- מה אני עושה במידע? תיאור כללי של פעולות האיסוף והשימוש במידע.
- לשם מה? תיאור מטרות השימוש במידע.
- איזה מידע יש לי בכלל? סוגי המידע השונים הכלולים במאגר המידע.
- האם המידע מועבר על ידי לחו"ל? פרטים על העברת מאגר המידע או שימוש בו מחוץ לגבולות ישראל.
- האם נעשות פעולות עיבוד מידע באמצעות אחר? (הכוונה למחזיק - קבלן חיצוני שאינו בעל המאגר, אולם מחזיק בו או רשאי לעשות בו שימוש בעבור בעל המאגר).
- מהם הסיכונים העיקריים של פגיעה באבטחת המידע.
- איך בכוונתי להתמודד עם הסיכונים האלה אם יתרחשו?
- שמם של מנהל/ת מאגר המידע, של מחזיק/ת המאגר ושל הממונה על אבטחת המידע בו.

לתשומת לבכם: את מסמך ההגדרות נדרש לעדכן אחת לשנה -

אם נעשה שינוי משמעותי באחד הפרמטרים לעיל.

אם נעשו שינויים טכנולוגיים רלבנטיים.

אם נעשו שינויים ארגוניים רלוונטיים.

אם אירע אירוע אבטחה.

מה עוד?

פעם בשנה צריך לבדוק אם לא מוחזק במאגר מידע רב מדי מזה הדרוש למטרותיו.

תקנה 3 ממונה על אבטחת מידע

לפי חוק הגנת הפרטיות, **נדרשים גופים מסוימים למנות ממונה על אבטחת מידע:**

מי שמחזיק **בחמישה מאגרי מידע** החייבים ברישום לפי החוק.

גוף ציבורי.

בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי.

לתשומת לבכם:

אם מונה ממונה על אבטחת המידע (ולא משנה מדוע נעשה המינוי), יש לפעול כך:

1. הממונה יהיה כפוף ישירות למנהל מאגר המידע או המחזיק, למנהל בכיר אחר הכפוף לו, או למנכ"ל הארגון (תקנה 3(1)).
2. הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור ההנהלה הבכירה של הארגון (תקנה 3(2)).
3. הממונה יכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, יבצע אותה ויודיע להנהלת הארגון ולמנהל המאגר על ממצאיו (תקנה 3(3)).
4. הממונה על האבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו (תקנה 3(4)).
5. אם בעל מאגר המידע הטיל על ממונה האבטחה משימות נוספות שאינן קשורות בנוהל אבטחת המידע והבקרה השוטפת עליו להגדירן בצורה ברורה (תקנה 3(5)).
6. בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו (תקנה 3(6)).

תקנה 4 נוהל אבטחה

תקנה 4(א) | התקנה מחייבת את בעל מאגר המידע לקבוע במסמך נוהל אבטחה ארגוני, שמטרתו לייצר מדיניות אבטחה ארגונית להתמודדות עם סיכוני האבטחה להם חשוף המידע.

תקנה 4(ב) | בעל המאגר נדרש לשמור את נוהל האבטחה כך שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

תקנה 4(ג) | הנוהל צריך לכלול לפחות את הנושאים הבאים:

- הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר (כאמור בתקנה 6).
- הרשאות גישה למאגרי המידע ולמערכות המאגר (בהתאם לתקנה 8).
- תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך.
- הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר.
- הסיכונים שחשוף להם המידע שבמאגר.
- אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11.
- הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12.

תקנה 4(ד) | רגע, רגע, אם מדובר במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, צריך נוהל האבטחה לכלול התייחסות גם לאלה:

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 לווידוא קיומם ותקינותם של אמצעי האבטחה כאמור בתקנה 16.
4. הוראות לעניין גיבוי הנתונים האמורים בתקנה 18(א)(1).
5. הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר.

תקנה 4(ה) | חשוב: אחת לשנה יש לבחון את הצורך בעדכון הנוהל -

- אם נעשו שינויים מהותיים במערכות המאגר או בתהליכי עיבוד המידע
- אם נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

תקנה 4(ו) | אם יש בבעלותכם כמה מאגרי מידע, אתם רשאים לקבוע נוהל אבטחה במסמך אחד המתייחס לכל מאגרי המידע, המצויים באותה רמת אבטחה.

תקנה 5 מיפוי מערכות המאגר וביצוע סקר סיכונים

תקנה 5(א) | על בעל מאגר המידע להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכוללת את הפרטים הבאים:

- תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע.
- מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטורו ולאבטחתו.
- תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן.
- תרשים הרשת שבה פועל המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של הרכיבים.
- תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

תקנה 5(ב) | פרטי המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

תקנה 5(ג) ו-5(ד) | חשוב: במאגר מידע שחלה עליו **רמת האבטחה הגבוהה**, חלה חובה:

לערוך סקר לאיתור סיכוני אבטחת מידע (סקר סיכונים) אחת ל-18 חודשים לפחות. בעל מאגר המידע ידון בתוצאות הסקר ויפעל לתיקון הליקויים, אם התגלו.

לערוך מבדקי חדירות למערכות המאגר אחת ל-18 חודשים לפחות - על מנת לבחון עמידותן בפני סיכונים פנימיים וחיצוניים.

תקנה 5(ה) | ארגון שהוא בעל כמה מאגרי מידע, רשאי לקבוע את רשימת המצאי במסמך אחד לגבי כל מאגרי המידע, המצויים באותה רמת אבטחה, וכן רשאי לקיים את החובות לגבי סקר סיכונים ומבדק חדירות אחד לגבי כל מאגרי המידע, המצויים באותה רמת אבטחה.

תקנה 6 אבטחה פיזית וסביבתית

תקנה 6(א) | התקנה מחייבת שמירה פיזית של תשתיות ומערכות החומרה המשמשות את המאגר, במקום מוגן המונע כניסה אליו ללא הרשאה. זאת לאור העובדה כי הגדרות הליבה של המערכת ואמצעי ההגנה הלוגיים שלה כפופים לסיכון של שינוי ועדכון באמצעות גישה פיזית, כך גם לגניבת אמצעי אחסון פיזיים.

תקנה 6(ב) | במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה - יש לתעד את הכניסות והיציאות של העובדים מאתרים בהם מצויות המערכות, וכן לתעד הכנסת ציוד אל מערכות המאגר והוצאת ציוד מהן. למשל באמצעות התקנת מצלמות, מערכת זיהוי ביומטרי וכו'.

תקנה 7 אבטחת מידע בניהול כוח אדם

תקנה 7(א) | לנוכח העובדה שהגורם האנושי מהווה גורם סיכון משמעותי בתחום אבטחת המידע, יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע עובדים המתאימים לעבודה זו, לאחר שננקטו אמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם. יש לקחת בחשבון את רגישות המידע שבמאגר ואת היקף הרשאות הגישה לתפקיד שמיועד לו המועמד לתפקיד. אמצעים סבירים הם למשל מבחני התאמה במכונים מקצועיים, המלצות ממעבידים קודמים, ואמצעים נוספים בהתאם כאמור לרגישות המידע.

לתשומת לבכם, עליכם לבחון גם את מידת התאמתם של <u>העובדים הקיימים</u> בארגון לגישה למאגר המידע.

תקנה 7(ב) | יש לקיים הדרכות לבעלי ההרשאות בנושא החובות לפי חוק הגנת הפרטיות והתקנות, בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם.

תקנה 7(ג) | שימו לב! במאגר שחלה עליו רמת אבטחה בינונית או גבוהה, יש לקיים פעילות הדרכה תקופתית אחת לשנתיים לפחות לבעלי ההרשאות.

תקנה 8 ניהול הרשאות הגישה

תקנה 8(א) | יש לקבוע הרשאות גישה למאגר לכל עובד, רק במידה הנדרשת לו לצורך ביצוע תפקידו.

תקנה 8(ב) | יש לנהל רשימת הרשאות מעודכנת.

תקנה 9 זיהוי ואימות

תקנה 9(א) | יש לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולכן יש לאמת את זהותו באמצעים מקובלים בנסיבות העניין. או בקיצור, לפחות באמצעות *סיסמה*.

תקנה 9(ב) | שימו לב! במאגר שחלה עליו רמת האבטחה הבינונית או הגבוהה -

1. אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. למשל תעודה המכילה חתימה אלקטרונית מאובטחת, token.
2. בנוהל האבטחה יש לקבוע גם את:

- אופן הזיהוי. אם אופן הזיהוי מבוסס על סיסמאות - הנוהל יתייחס לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על 6 חודשים.
- ניתוק אוטומטי לאחר פרק זמן של אי-פעילות.
- אופן הטיפול בתקלות הקשורות באימות זהות.

תקנה 9(ג) | בעל המאגר ידאג לביטול ההרשאות של בעל ההרשאה שסיים את תפקידו, ובמידת האפשר לשינוי סיסמאות, מיד עם סיום תפקידו של בעל ההרשאה.

תקנה 10 בקרה ותיעוד גישה

***** התקנה רלוונטית למאגרי מידע שחלה עליהם רמת אבטחה בינונית או גבוהה -**

תקנה 10(א) | יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (מנגנון בקרה), אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

תקנה 10(ב) | על מנגנון הבקרה להיות עצמאי, לפעול באופן רציף, וככל הניתן ללא אפשרות להתערבות חיצונית שתביא לביטול או שינוי בהפעלתו. אם בוצעו שינויים או ביטולים בהפעלת המנגנון, על המנגנון לאתר אותם באופן אוטומטי ולהפיץ התראות לאחראים.

תקנה 10(ג) | בעל מאגר המידע נדרש לקבוע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דו"ח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן. על מנת לעמוד בחובתו של בעל המאגר לאתר אירועי אבטחה בזמן אמת מומלץ ליישם מנגנונים אוטומטיים להתראה.

תקנה 10(ד) | נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות.

תקנה 10(ה) | בעל המאגר יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

תקנה 11 תיעוד של אירועי אבטחה

מטרת התקנה ליצור "זיכרון ארגוני" ביחס לאירועי אבטחה, על מנת להפיק מהם לקחים לעתיד.

מהו אירוע אבטחה? פגיעה בשלמות המידע, שימוש במידע ללא הרשאה או חריגה מהרשאה.

תקנה 11(א) | אירע אירוע אבטחה? נא לתעד. ככל האפשר, יש להתבסס על רישומים אוטומטים אודות אירועי אבטחה במערכות המאגר של הארגון, כגון syslog snmp.

תקנה 11(ב) | בנוהל האבטחה יש לקבוע הוראות לעניין התמודדות עם אירועי אבטחת מידע ואופן הדיווח לבעל המאגר.

תקנה 11(ג) | במאגר שחלה עליו רמת אבטחה בינונית - בעל המאגר יקיים דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה. **במאגר שחלה עליו רמת האבטחה הגבוהה -** ייערך דיון כאמור אחת לרבעון לפחות.

תקנה 11(ד) | מהו אירוע אבטחה חמור וכיצד עלי לפעול במקרה זה?

במאגר מידע שחלה עליו רמת אבטחה גבוהה - אירוע אבטחה חמור הוא אירוע שנעשה בו שימוש במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע;

לתשומת לבכם: "שימוש" מוגדר בחוק הגנת הפרטיות גם כ"גילוי, העברה ומסירה". כלומר, גם אם מישהו צפה במאגר, אך לא ביצע פעולה אקטיבית אחרת (כמו העתקה)- מדובר באירוע אבטחה חמור.

במאגר מידע שחלה עליו רמת אבטחה בינונית - אירוע אבטחה חמור הוא אירוע שנעשה בו שימוש **בחלק מהותי** מן המאגר, בלא הרשאה או בחריגה מהרשאה, או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר. ככלל, אירוע שנעשה בו שימוש ב"חלק מהותי מן המאגר" יהיה חריג בחומרת הסיכונים שייצור, בשל היקף המידע שיימצא בסיכון כתוצאה מהאירוע (שימוש בכמות ניכרת של מידע, להבדיל משימוש ברשומה אחת בלבד, או מידע על מספר רב של אנשים). אחת הדרכים העומדות בפני בעל המאגר לבחון האם נעשה שימוש בחלק מהותי היא באמצעות בחינת מספר המערכות וסוג המערכות שנפגעו ונעשה בהם שימוש ללא הרשאה, משך זמן האירוע, כל מקרה לפי נסיבותיו.

תקנה 11(ד)(1) | במקרה של אירוע אבטחה חמור, יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע.

תקנה 11(ד)(2) | במקרה של אירוע אבטחה חמור, רשאי הרשם להורות לבעל מאגר המידע, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושאי מידע שעלולים להיפגע מן האירוע (למעט חריגים מסוימים).

תקנה 12 התקנים ניידים

התקן נייד הוא מחשב או התקן אחסון המיועד לשימוש נייד. לדוגמה: מחשב נייד, התקן זיכרון נייד, כונן חיצוני וטלפון סלולרי חכם.

כיוון שמדובר בהתקנים ניידים, הניתנים להעברה ממקום למקום, קיים סיכון כי מידע מהמאגר עלול לדלוף החוצה באופן לא מורשה, או שחיבור ההתקן הנייד יגרום נזק למערכות המאגר בשל נוזקה המותקנת בו.

חשוב להגביל את האפשרות לחבר התקנים ניידים למערכות המאגר, בשים לב לרגישות המידע שבו.

אם אפשר לחבר התקנים ניידים למערכת, חשוב להגן על המידע המועתק אליהם. הצפנת המידע, על ידי שימוש בשיטות הצפנה מקובלות, תיחשב נקיטת אמצעים סבירים.

תקנה 13 ניהול מאובטח ומעודכן של מערכות המאגר

תקנה 13(א) | יש להקפיד על ניהול ותפעול תקין של מערכות המידע.

תקנה 13(ב) | התקנה מחייבת את בעל המאגר להפריד ככול האפשר בין מערכות המשמשות את מאגר המידע, כמו השרת שעליו מותקן המאגר, ותחנות הקצה בעלות גישה למאגר, משאר מערכות המחשבים הארגוניות שלא נדרש לגשת מהם למאגר המידע. קיימות מספר שיטות להפרדה זו, למשל, מערכת Fire Wall (חומת אש) פנימית.

תקנה 13(ג) | בעל המאגר נדרש לעדכן באופן שוטף את מערכות המאגר, חומרה ותוכנה בהתאם להנחיות היצרן על מנת לנטרל פגיעויות וחולשות המתגלות מעת לעת.

לא יעשה שימוש במערכות (חומרה או תוכנה) שהיצרן שלהן הפסיק את התמיכה בהיבטי האבטחה שלהן.

תקנה 14 אבטחת תקשורת

אם מערכות המאגר מחוברות לרשת האינטרנט או לרשת ציבורית אחרת, נוצר סיכון של גישה חיצונית ולא מורשית אליהן. לכן יש להקפיד על הכללים הבאים:

תקנה 14(א) | התקנת אמצעי הגנה מפני חדירה לא מורשית, או תוכנות מזיקות. כגון: תוכנת אנטי-וירוס, תוכנת Fire Wall (חומת אש) והתקן חומת אש פיזי. את אמצעי ההגנה יש ליישם הן בממשק של מערכות המאגר לרשת האינטרנט או הרשת החיצונית, הן בממשקים בין המערכות ככול שקיימים והן בממשק בין מערכות הקצה הניגשות למערכות המאגר.

תקנה 14(ב) | העברת מידע ממאגר המידע, ברשת הציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

תקנה 14(ג) | במאגר מידע שניתן לגשת אליו מרחוק ("חיבור מהבית" למשל), ייעשה שימוש באמצעים שמזהים את המתקשר והמאמתים את זהותו.

לתשומת לבכם: במאגרים ברמת האבטחה הבינונית והגבוהה יש לעשות שימוש באמצעי פיזי, הנתון לשליטתו הבלעדית של בעל ההרשאה, כגון כרטיס חכם.

תקנה 15 מיקור חוץ

תקנה 15(א) | מתן גישה לגורם חיצוני יוצרת סיכונים מיוחדים, ולכן מצריכה בחינת סיכוני אבטחת המידע האפשריים הכרוכים בהתקשרות עימו. **הוראת התקנה דומה ברובה להנחיית רשם מאגרי מידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי"**

יש להקפיד על ההוראות הבאות:

- לבחון, לפני ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות, ואם הם גבוהים מדי בהתחשב ברגישות המידע, להימנע ממיקור החוץ לחלוטין.
- לקבוע במפורש בהסכם את כל אלה, בשים לב לסיכוני אבטחת המידע:

1. מהו המידע שהגורם החיצוני רשאי לעבד ולאלו מטרות?
2. לאלו מערכות הוא רשאי לגשת?
3. מהו סוג העיבוד שאותו הוא רשאי לבצע?
4. מהו משך ההתקשרות ומה יהיה אופן השבת המידע לידי הבעלים בסיום ההתקשרות?
5. אופן יישום הוראות תקנות אבטחת מידע.
6. חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע.

7. אם בעל המאגר התיר לגורם החיצוני לתת את השירות באמצעות גורם נוסף - חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו (תקנה 15).
8. חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.

תקנה 15(3) | יש לפרט בנוהל האבטחה של המאגר גם את העניינים שפורטו מעלה בסעיפים א' עד ה', ולהפנות במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו.

תקנה 15(4) | יש לנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות, בהיקף הנדרש ובשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות.

תקנה 15(ב) | מה הדין לגבי ארגון בעל כמה מאגרי מידע? ארגון שהוא בעל כמה מאגרי מידע רשאי לקיים את הוראות התקנה בהסכם אחד לעניין על מאגרי המידע, ובלבד שהם באותה רמת אבטחה.

תקנה 16 ביקורות תקופתיות

תקנה 16(א) | במאגר מידע שחלה עליו רמת **האבטחה הבינונית או הגבוהה - אחת ל-24 חודשים לפחות** יש לערוך ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, על מנת לוודא עמידתו בהוראות התקנות.

תקנה 16(ב) | בדו"ח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.

תקנה 16(ג) | בעל המאגר ידון בדו"חות הביקורת שיועברו לו, וייבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.

תקנה 16(ד) | במאגר שחלה עליו רמת האבטחה הגבוהה - בעל המאגר רשאי לקיים את החובה הקבועה בתקנה 16 במסגרת עריכת סקר סיכונים ובלבד שמתקיים בו האמור בתקנת משנה (ב). סקר הסיכונים נדרש במטרה לזהות ולהעריך את רמת הסיכון לפגיעה באבטחת מידע הקיימת בכל אחד מרכיבי מערכות המאגר, בעוד שביקורת כאמור, מעבר לבחינת אמצעי האבטחה המיושמים, בוחנת את עמידתו של בעל המאגר בנוהל האבטחה ובתקנות בכלל.

תקנה 16(ה) | מה הדין לגבי ארגון בעל כמה מאגרי מידע? ארגון שהוא בעל כמה מאגרי מידע רשאי לקיים את הוראות התקנה במסגרת ביקורת אחת לעניין כל מאגרי המידע, המצויים באותה רמת אבטחה.

תקנה 17 משך שמירת נתוני האבטחה

תקנה 17(א) | יש לשמור את הנתונים "הטכניים" הנצברים במסגרת יישום תקנות 6(ב), 8-11, 14, 15(א)(4) ו-16 באופן מאובטח למשך 24 חודשים (נתוני בקרה על כניסה ויציאה מאתרי המערכות, הכנסה והוצאה של ציוד אל מערכות המאגר ומהן, ניהול הרשאות גישה, זיהוי ואימות, בקרה ותיעוד גישה, תיעוד של אירועי אבטחה, אבטחת תקשורת, אמצעי בקרה ופיקוח על הגורם החיצוני בעל גישה למאגר וביקורות תקופתיות) .

תקנה 17(ב) | במאגר שחלה עליו רמת האבטחה הבינונית או הגבוהה - יש לגבות את הנתונים שנשמרו, באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי.

תקנה 18 גיבוי ושחזור נתוני אבטחה

***** התקנה רלוונטית למאגרים שחלה עליהם רמת האבטחה הבינונית והגבוהה.**

תקנה 18(א) | יש לקבוע במסמך את הנהלים הבאים:

- נהלים לביצוע גיבוי נתוני אבטחה באופן תקופתי שגרתי.
- נהלים שיבטיחו שניתן יהיה לשחזר את הנתונים כאמור בתקנה 17(ב) באופן יעיל ומהיר, ובלבד שביצוע השחזור יהיה באישור מנהל המאגר.
- במסגרת תיעוד אירועי אבטחה, כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע, ובכלל זה - זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

תקנה 18(ב) | חשוב! במאגר שחלה עליו **רמת האבטחה הגבוהה** חלה דרישה נוספת - בעל המאגר אחראי לכך שיישמר עותק הגיבוי של הנתונים הנ"ל באופן שיבטיח את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס. למשל שמירת הגיבוי באתר פיזי אחר.

תקנה 19 האחריות לאבטחת המידע

תקנה 19(א) | חוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על בעל המאגר, המנהל והמחזיק. בהתאם לכך, קובעת תקנה 19(א), כי החובות החלות על בעל מאגר המידע תחולנה גם על מנהל המאגר וגם על מחזיק המאגר, בשינויים המחויבים ולפי העניין, למעט החובות הקבועות בתקנות 2 ו-15(א) (מסמך הגדרות המאגר ומיקור חוץ).

תקנה 19(ב) | כל מי שמוטלת עליו חובה או אחריות לביצוע פעולה, נדרש לתעד את ביצועה.

תקנה 20 רגולציה ותקנים מקבילים

תקנה 20(א) | לרשם יש סמכות לפטור מאגרים ספציפיים מחובות אבטחת מידע לפי התקנות, או לחילופין להטיל על מאגר ספציפי חובות נוספות מן התקנות, לפי נסיבות העניין, ובהתחשב בגודל המאגר, סוג המידע שנמצא בו וכו'.

תקנה 20(ב) | הרשם רשאי להורות כי מי שיעמוד בהוראות מסמך מנחה בעניין אבטחת מידע (תקן רשמי, ישראלי או בינ"ל) או בהנחיות של רשות מוסמכת (גוף ציבורי המוסמך לתת הנחיות בעניין אבטחת מידע), יראו אותו כמקיים את הוראות התקנות, כולן או חלקן, אם השתכנע כי עמיד בהוראות המסמך או ההנחיות מבטיחה את רמת האבטחה הקבועה בתקנות.

האמור הינו מידע כללי בלבד, ואינו מחליף ייעוץ המותאם לצרכים האישיים.

03-7634050 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL
חפשו אותנו גם בפייסבוק