




הרשות
להגנת
הפרטיות



משרד המשפטים

מדריך תקנות הגנת הפרטיות (אבטחת מידע) לעצמאים ולעסקים קטנים



PPA@justice.gov.il  | 02-6467064  | 03-7634050 
WWW.PPA.JUSTICE.GOV.IL | 6107202 תל אביב, 7360, ת.ד.

חפשו אותנו גם בפייסבוק 

היו ערוכים ומוכנים...

תקנות הגנת הפרטיות (אבטחת מידע) ייכנסו לתוקף ב-8 במאי 2018. ודאו שאתם ערוכים לכך בעזרת המדריך הבא.

מהי אבטחת מידע?

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



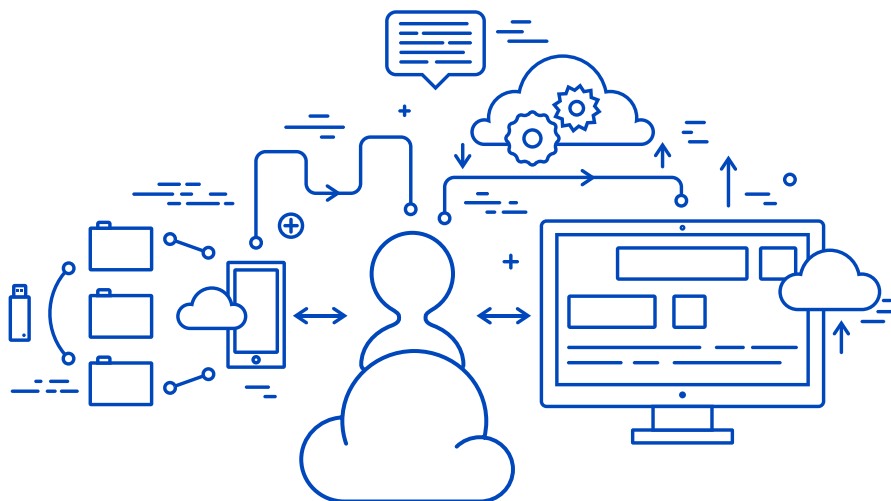
על מי חלות התקנות?

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



על איזה מידע חלות התקנות?

התקנות חלות על מידע המכיל נתונים על מעמדו האישי של אדם (כגון סטטוס משפחתי, אילן יוחסין, קשרים משפחתיים), מצבו הכלכלי, הכשרתו המקצועית ועוד. דוגמה נוספת למידע שיש להגן עליו היא מספר תעודת הזהות של אדם.

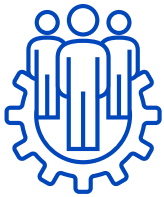


מהו מאגר המנוהל בידי יחיד?

זהו מאגר מידע שמנהל יחיד בעצמו או תאגיד בבעלות יחיד ("חברת אני"), ואשר הגישה למידע שבו מותרת רק לאותו יחיד ולכל היותר לעוד שני בעלי הרשאה נוספים. לדוגמה, ברשותי חנות פרחים, שבה אני מנהל מאגר לקוחות הכולל פרטים כמו תאריכי לידה, קשרי משפחה ועוד. למאגר זה יכולים לגשת גם העובדים המסייעים לי בחנות. ואם יש לי בחנות שלושה עובדים ויותר? אז כבר לא מדובר במאגר יחיד. במקרה זה יחולו חובות אחרות, המפורטות במדריך המלא לתקנות הגנת הפרטיות (אבטחת מידע).

אבל רגע רגע - יש חריגים

קיימים שלושה סוגי מאגרים שלמרות שהם מנוהלים על ידי יחיד, לא ייחשבו כ"מאגר המנוהל בידי יחיד":



מאגר מידע שיש בו מידע לגבי 10,000 אנשים ומעלה.



מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר.



כאשר בעל המאגר כפוף לחובת סודיות מקצועית לפי דין או לפי עקרונות של אתיקה מקצועית. לדוגמה, עורך דין או פסיכיאטר.

אם מאגר המידע שלכם שייך לאחד מהשלושת הסוגים הללו - אין מדובר ב"מאגר המנוהל בידי יחיד", ועליכם לבחון איזו רמת אבטחה חלה על המאגר שלכם, בהתאם לאמור בתקנות.

בדקתי ואני נחשב למאגר יחיד - אילו חובות חלות על מאגר המידע שלי?

הכנת "מסמך הגדרות המאגר". המסמך יתייחס לנושאים הבאים:

- מה אני עושה במידע? תיאור כללי של פעולות השימוש במידע.
- בשביל מה? מטרות השימוש במידע.
- איזה מידע יש לי בכלל? סוגי המידע השונים הכלולים במאגר המידע.
- האם אני מעביר את המידע לאחרים בחו"ל? פרטים על העברת מאגר המידע או שימוש בו מחוץ לגבולות ישראל.
- האם נעשות פעולות עיבוד מידע באמצעות אחר (הכוונה לקבלן חיצוני שאינו בעל המאגר, אולם מחזיק בו או רשאי לעשות בו שימוש עבור בעל המאגר).
- האם יש סיכונים? מהם הסיכונים העיקריים של פגיעה באבטחת המידע.
- איך אני מתכוון להתמודד עם הסיכונים האלה אם חס וחלילה יתרחשו?
- שמו של מנהל מאגר המידע (היי, זה אני!) ושל מחזיק המאגר.

חשוב: את מסמך ההגדרות נדרש לעדכן -

- אם נעשה שינוי משמעותי באחד מהפרמטרים לעיל.
- אם נעשו שינויים טכנולוגיים רלוונטיים.
- אם נעשו שינויים ארגוניים רלוונטיים.
- אם אירע אירוע אבטחה.



מה עוד?

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



אבטחה פיזית

עליכם להפריד בין החומרה המשמשת את המאגר לחומרות אחרות המשמשות את בעל המאגר. את החומרה יש לשמור במקום מוגן, המונע כניסה אליו ללא הרשאה. כן, אם לבית שלך יש דלת ומנעול – סביר שהמקום ייחשב למקום מוגן.



זיהוי ואימות

עליכם לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולכן יש לאמת את זהותו באמצעים מקובלים בנסיבות העניין. או בקיצור – סיסמה.



אירע אירוע אבטחה? לתעד בבקשה

מהו אירוע אבטחה? פגיעה בשלמות המידע, שימוש במידע ללא הרשאה. בהתקיים אירוע, עליכם לנהל רישום פנימי שלו על מנת לשמר יידע ביחס לאירועי אבטחה שקרו. עליכם להתבסס ככל הניתן על רישום באמצעות תוכנה העוקבת ומתעדת כל פעולה במידע או גישה אליו.



התקנים ניידים

בהתקן נייד הכוונה לאמצעי נייד לאחסון נתונים, כמו מחשב נייד, disc on key וטלפון סלולרי חכם. חשוב להגביל את האפשרות לחבר התקנים ניידים למערכות המאגר, בשים לב לרגישות המידע שבו. אם אפשר לחבר התקנים ניידים למערכת, חשוב להגן על המידע. למשל להצפין אותו באמצעות סיסמה.



ניהול מאובטח ומעודכן של מערכות המאגר

עליכם להקפיד על ניהול ותפעול תקין של מערכות המידע.

חשוב להפריד בין המערכות שמהן ניתן לגשת למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר. לדוגמה, מערכת firewall (חומת אש) פנימית, מערכת לחלוקת רשתות ועוד.

חשוב לעדכן את המערכות באופן שוטף, כדי להימנע משימוש במערכות שהיצרן שלהן הפסיק לתמוך בהיבטי האבטחה שלהן.



אבטחת תקשורת

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

⦿ התקנת אמצעי הגנה מפני חדירה לא מורשית או תוכנות מזיקות, כגון: תוכנת אנטי-וירוס, תוכנת הגנה מפני תוכנות זדוניות, תוכנת חומת אש והתקן חומת אש פיזי.

⦿ העברת מידע ממאגר המידע תיעשה תוך שימוש בשיטות הצפנה.

⦿ במאגר מידע שניתן לגשת אליו מרחוק ("חיבור מהבית" למשל) עליכם להשתמש באמצעים שמזהים את המתקשר ומאמתים את זהותו.



האמור הינו מידע כללי ותמציתי בלבד, ואינו מחליף ייעוץ המותאם לצרכים האישיים של כל מנהל מאגר.

