17 בפברואר, 2026

אמצעים מקובלים לאימות זהות בגישה למאגרי מידע – טיוטת הנחיה חדשה של הרשות להגנת הפרטיות

עדכוני לקוחות

לאחרונה פרסמה הרשות להגנת הפרטיות ("**הרשות**") טיוטה להערות הציבור בנושא "אמצעים מקובלים" לניהול הרשאות גישה לפי תקנה 9(א) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("**התקנות**"). מטרת המסמך היא להגדיר את האמצעים הטכנולוגיים שעל בעלי מאגרי מידע ומחזיקים בהם לנקוט כדי להבטיח שרק גורמים מורשים יוכלו לגשת למידע, וזאת בהתאם לרגישות המידע ומאפייני הסיכון.

חשיבות העמידה בדרישות התקנות גוברת נוכח **כניסתו לתוקף של תיקון 13 לחוק הגנת הפרטיות, תשמ"א-1981 (להלן: "החוק") באוגוסט 2025**, אשר העניק לרשות סמכויות אכיפה נרחבות, לרבות הטלת עיצומים כספיים משמעותיים על הפרת הוראות החוק והתקנות. ספציפית, אי עמידה בדרישות תקנה 9(א) עלולה לחשוף את הארגון לעיצומים כספיים שעשויים להגיע עד 160,000 ש"ח.

בעדכון זה נסקור את עיקרי הטיוטה ונציע צעדים פרקטיים להיערכות הארגון.

הגדרת "אמצעים מקובלים" ושיטות אימות

תקנה 9(א) לתקנות קובעת חובה כללית לנקוט "אמצעים מקובלים" לאבטחת הגישה למאגר, אך אינה מפרטת מהם. הרשות מבהירה בטיוטה כי אמצעים אלו צריכים להתבסס על תקנים בינלאומיים (כגון תקני NIST) ועל המקובל בשוק. שיטות האימות העיקריות שנסקרות במסמך מחולקות לשלוש קבוצות:

- **"משהו בידיעתך":** אימות המבוסס על מידע הידוע רק למשתמש כמו סיסמה או קוד; מספר תעודת זהות כשלעצמו אינו נחשב גורם אימות.
- **"משהו בבעלותך":** אימות שמבוסס על רכיב פיזי או דיגיטלי מאובטח שבבעלות המשתמש כגון טלפון נייד (לקבלת קוד OTP), אפליקציית אימות או כרטיס חכם.
- **"משהו שאתה"**: אימות שמבוסס על תכונות פיזיולוגיות או התנהגותיות כגון טביעת אצבע, זיהוי פנים או זיהוי קולי.

אימות רב-גורמי (MFA) ורמות אימות

הרשות מדגישה את חשיבות השימוש באימות רב-גורמי (MFA), המשלב לפחות שני גורמי אימות בלתי תלויים, ככלי להפחתת הסיכון לגישה לא מורשית. הטיוטה מגדירה שלוש רמות אימות בהתאם למתודולוגיית NIST:

- **רמת אימות 1 (ביטחון בסיסי)**: דורשת הוכחת בעלות על אמצעי אימות אחד.
- **רמת אימות 2 (ביטחון גבוה)**: דורשת שימוש בשני אמצעי אימות לפחות המוגנים מפני התחזות (Phishing-Resistant Authentication).

- **רמת אימות 3 (ביטחון גבוה מאוד)**: דורשת MFA המבוסס על מפתח קריפטוגרפי שאינו ניתן לייצוא, המקנה הגנה מרבית מפני התחזות או עקיפת זהות.

<u>דרישות קונקרטיות לפי רמת אבטחת המאגר</u>

הרשות מציגה בטיוטה טבלה המפרטת את הסטנדרט המצופה בכל הנוגע לאורך סיסמה, תדירות החלפתה וחובת MFA, בהתאם לרמת אבטחת המאגר (בסיסית, בינונית או גבוהה) וזהות הגורם הניגש:

- **במאגרים ברמת אבטחה בינונית:** נדרש MFA עבור בעלי הרשאה הניגשים מחוץ לארגון, עבור לקוחות בגישה מרחוק ועבור מנהלי מערכת.
- **במאגרים ברמת אבטחה גבוהה:** נדרשת רמת אימות 3 (המחמירה ביותר) עבור בעלי הרשאה הניגשים מחוץ לארגון ועבור מנהלי מערכת.
- **אורך סיסמה:** ככלל, יש לדרוש סיסמה של 15 תווים לפחות, או 8 תווים בצירוף אמצעי זיהוי נוסף.

<u>צעדים מעשיים ליישום</u>

לאור המגמה של הגברת האכיפה והחשיפה המשפטית, אנו ממליצים על הצעדים הבאים:

- **מיפוי מאגרי המידע והרשאות הגישה:** סיווג המאגרים לפי רמות האבטחה הקבועות בתקנות ובחינת זהות הגורמים הניגשים אליהם (עובדים, לקוחות, מנהלי מערכת).
- **בחינה ושדרוג של מנגנוני האימות:** וידוא כי מנגנוני האימות בארגון עומדים בסטנדרטים המפורטים בטבלה שבטיוטת ההנחיה, ובפרט הטמעת MFA בגישה מרחוק ובגישות של מנהלי מערכת.
- **עדכון נהלי אבטחת מידע:** עדכון הנהלים הפנימיים בארגון בנוגע למדיניות סיסמאות וניהול הרשאות בהתאם להנחיות החדשות.

הרשות מבהירה כי ייתכנו אמצעים נוספים מעבר לאלה המפורטים בטיוטת ההנחיה, בין היתר נוכח ההתפתחויות הטכנולוגיות והשתנות הסטנדרטים המקובלים, ובהתאם לכך המסמך עשוי להתעדכן מעת לעת. עם זאת, ככל שייבחרו פתרונות אחרים מהמוצעים בטיוטת ההנחיה, **האחריות לבחון ולקבוע כי אמצעי הגישה מקובלים ומתאימים בנסיבות העניין מוטלת על בעל השליטה או המחזיק במאגר**.

טיוטת ההנחיה פתוחה להערות הציבור עד ליום 22.2.26, באמצעות כתובת הדוא"ל ppa@justice.gov.il.

אנו עומדים לרשותכם בכל שאלה או הבהרה בנושא.

אנשי קשר

אסף הראל
שותף

אביטל חייטוביץ'
שותפה

אלה שרק
מתמחה