1.
פרטיות והגנת מידע
של מי המידע? פרטיות בעידן ה-AI

שמירה על פרטיות בשימוש בבינה מלאכותית דורשת מודעות, שקיפות והסכמה מדעת, לצד חינוך לשימוש אחראי וזהיר במידע אישי.

פרטיות מתחילה במודעות והבנה

פרטיות היא היכולת לשלוט על מידע אישי, להחליט מי יוכל לגשת אליו וכיצד ייעשה בו שימוש. מרבית כלי הבינה המלאכותית פועלים על בסיס מידע עליו אומנו בשילוב איסוף מידע שמוזן על ידי המשתמשים. פעולה זו מאפשרת שיפור והתאמה אישית של פלטי המערכות עבור כל משתמש. אחד האתגרים המרכזיים בשימוש בכלים אלו הוא בכך שהמידע הנשמר במערכות עלול להוות פגיעה פוטנציאלית בפרטיותם.

יש להעלות את המודעות לסכנות הקיימות בשימוש בכלים אלו לרבות הבנה מה מדיניות הפרטיות של כל כלי וכלי. ישנם הבדלים בין כלים שונים ובין גרסאות חינמיות לגרסאות בתשלום. לכן, מומלץ שהמשתמשים יבררו בכל עת מה נכון להם לחשוף לכלי מסוים – הן בהתאם למדיניות הפרטיות הנוכחית של הכלי, והן בהתחשב בסכנות של דלף עתידי, גם אם הכלי מצהיר שאינו שומר או חושף נתונים. הנגשת תכני למידה והעלאת המודעות יסייעו לצמצם חשיפה ולשמור על פרטיות המשתמשים.

שקיפות, תקשורת והסכמה

שילוב ראוי של בינה מלאכותית במערכת החינוך מחייב שקיפות והנגשה של מדיניות הפרטיות לכלל המשתמשים – תלמידים.ות, מורים.ות, והורים. יש להבהיר אילו נתונים נאספים, עבור מה ולמי ניתנת גישה אליהם, תוך ווידוא שההסכמה לשימוש בכלי הבינה מתבצעת מתוך הבנה מלאה אודות ההשלכות האפשריות.

בנוסף, חשוב להקנות לכל התלמידים.ות את המודעות לחשיבות השמירה על פרטיות ולעודד בחינה שקולה של המידע שמועבר, בדגש על מידע רגיש. קיום שיח פתוח וליווי מתמשך יסייעו לפתח הבנה של הסיכונים ולקדם אחריות אישית בנוגע לניהול מידע בעולם הדיגיטלי.

יש להקפיד על אבטחת מידע כדי להגן על פרטיות כל המשתמשים והמשתמשות, תוך יישום אמצעים ונהלים שיסייעו במניעת דליפות מידע ומתקפות סייבר.