

המלצות הרשות להגנת הפרטיות לשימוש אחראי בסוכני בינה מלאכותית

עדכוני לקוחות

1. רקע

ביום 9.7.2026 פרסמה הרשות להגנת הפרטיות ("הרשות") [מסמך המלצות](#) לציבור בנושא "המלצות להתנהלות הציבור בשימוש אישי בסוכני בינה מלאכותית" ("המסמך"). המסמך סוקר חלק מן הסיכונים לפרטיות הנובעים משימוש בסוכני בינה מלאכותית על ידי משתמשי קצה יחידים – למטרות אישיות בלבד. אמנם המסמך מתייחס לשימוש משתמשי קצה בסוכני בינה מלאכותית למטרות אישיות אך הדברים כמובן נכונים, ואף ביתר שאת, בהקשר הארגוני.

2. כיצד פועלים סוכני בינה מלאכותית?

סוכן בינה מלאכותית נועד לפעול כדי להשיג מטרה מוגדרת עבור המשתמש, בהתאם להוראותיו ובאמצעות הכלים הזמינים לו. המסמך מתאר שלושה מרכיבים מרכזיים של סוכן בינה מלאכותית:

- **"מוח"** – רכיב הליבה של הסוכן, המבוסס לרוב על מודל שפה גדול (LLM), האחראי על הבנת הוראות, ניתוח מידע, קבלת החלטות ותכנון פעולות.
- **"זיכרון"** – מאפשר לסוכן לשמור מידע לאורך זמן. למשל, העדפות המשתמש והקשר מפעולות קודמות. כך הסוכן יכול להתאים את פעולותיו בהתאם לאינטראקציות קודמות עם המשתמש.
- **"ידיים"** – כלים וממשקים למערכות חיצוניות, המאפשרים לסוכן לגשת למשאבים דיגיטליים ולבצע פעולות בפועל, כדוגמת קביעת פגישה ביומן, שליחת דוא"ל, שליפת מסמכים, ביצוע רכישה ועוד.

בשונה ממערכות בינה מלאכותית יוצרת "רגילות", סוכני בינה מלאכותית מסוגלים לפרש מטלות, לבצע משימות מורכבות ולקבל החלטות ללא מעורבות של המשתמש, תוך ריכוז ועיבוד מידע אישי בהיקף נרחב. כאשר הסוכן מחובר ליומנים, לתיבות דוא"ל, למאגרי לקוחות, למערכות מסמכים או למערכות תפעוליות, מאפיינים אלה עלולים להעצים את הסיכונים לפרטיות ולאבטחת מידע גם בהקשר הארגוני.

3. האתגרים שסוכני בינה מלאכותית מציבים לפרטיות

- **הסוכן יודע עליכם יותר ממה שחשבתם** – סוכני בינה מלאכותית פועלים לעיתים קרובות תוך חיבור למערכות המידע של המשתמש, כגון יומנים, דוא"ל, פירוט תשלומים ומאגרי מידע נוספים. כתוצאה מכך, הסוכן עשוי לקבל גישה למידע אישי בהיקף העולה על הנדרש לביצוע המשימה הספציפית. כתוצאה מכך, הסוכן עשוי ליצור פרופיל אישיותי מקיף, הכולל הרגלים יומיומיים, קשרים חברתיים, העדפות צריכה, מצב בריאותי והתנהלות פיננסית. בהקשר הארגוני, מצב זה עלול ליצור תמונה רחבה על עובדים, לקוחות, ספקים ובעלי תפקידים, לרבות דפוסי עבודה, קשרים עסקיים, מידע פיננסי ולעיתים גם מידע רגיש. לעיתים קרובות, המשתמש אינו מבין את היקף חשיפת המידע שלו לסוכן, דבר המקשה על גיבוש הסכמה מדעת ועל בקרה אפקטיבית.

• **הסוכן פועל על בסיס מה שלמד גם כשלא מבוקש ממנו** – בשונה ממערכות בינה מלאכותית אחרות, סוכן בינה מלאכותית מסוגל לפעול על בסיס מידע שנשמר או הוסק על ידו לאורך זמן ולכן הסוכן עשוי לעשות שימוש במידע ובמסקנות שהפיק, מחוץ להקשר ושלא בהתאם לציפיית המשתמש.

• **הסוכן לא רק קורא הוא גם מוחק, עורך ומשנה** – סוכני בינה מלאכותית הם לא רק צרכני מידע. הם מסוגלים לפעולה אקטיבית ואוטונומית ולבצע עריכה, עדכון, מחיקה או העברה של מידע אישי במערכות שאליהן הם מחוברים. פעולה אוטונומית זו עלולה שלא לעלות בקנה אחד עם רצון המשתמש ובהקשר הארגוני, יכולת זו עלולה להביא לשינוי של מסמכים, רשומות, תכתובות או נתונים עסקיים באופן שאינו תואם את נהלי הארגון או מדיניותו.

4. המלצות לשימוש אחראי בסוכני בינה מלאכותית

• **צמצום הגישה למידע אישי** – יש להגדיר באופן ספציפי את המידע הזמין לסוכן, ולהימנע מחיבורו למאגרי מידע שלמים. עדיף לספק לסוכן תת-קבוצה רלוונטית של נתונים בלבד, בהתאם למשימה הקונקרטית. כמו כן, מומלץ להעדיף פתרונות המאפשרים עיבוד זמני, ללא שמירת היסטוריה ומבלי שהמידע האישי ישמש לאימון המודל. בארגונים, עיקרון זה חשוב במיוחד כאשר נשקל חיבור הסוכן למערכות עיבוד מסמכים, למאגרי לקוחות, לתיבות דוא"ל או למערכות משאבי אנוש.

• **צמצום חשיפת מידע אישי וניהול ממשקים חיצוניים** – יש לוודא כי הסוכן אינו מעביר מידע לגורמים שלא אושרו על ידי המשתמש, וכי בכל מקרה היקף המידע המועבר אינו עולה על הנדרש.

• **צמצום הרשאות גישה** – יש להעניק לסוכן רק את ההרשאות ההכרחיות לביצוע המשימה. ככל שההרשאות מצומצמות יותר, כך קטן הסיכון לנזק במקרה של טעות, תקלה, או אירוע אבטחת מידע. מומלץ להעדיף הרשאות צפייה וקריאה בלבד, ולהימנע מהרשאות עריכה ושינוי כאשר אין בהן הכרח.

• **בקרה וניטור** – מומלץ לדרוש אישור מפורש של המשתמש לפני ביצוע פעולות מסוימות. כמו כן, מומלץ לדרוש מהסוכן להציג את רצף השלבים המתוכננים לפני ביצועם, ולנהל תיעוד של הפעולות שביצע, כך שניתן יהיה לוודא שהסוכן פעל בהתאם לציפיות ולהרשאות שניתנו לו.

• **גיבוי ושחזור** – עם הרשאות מתאימות, סוכני בינה מלאכותית יכולים לערוך, למחוק או לשנות מידע במהירות ובהיקף רחב. לכן, מומלץ לגבות את המידע הרלוונטי לפני מתן הרשאות לסוכן, כדי לאפשר את שחזורו במקרה הצורך. בארגונים, המלצה זו חשובה במיוחד כאשר הסוכן עשוי לפעול על מאגרי מידע משותפים, מערכות ליבה או תהליכים קריטיים לפעילות העסקית.

לסיכום, המסמך מבטא את עמדת הרשות כי השימוש בסוכני בינה מלאכותית מציב אתגרים משמעותיים לפרטיות. אף שהמסמך מתייחס לשימוש אישי, העקרונות הנזכרים בו הנוגעים לצמצום מידע, הגבלת הרשאות, בקרה וגיבוי, רלוונטיים במידה רבה גם לחברות וארגונים הבוחנים שילוב של סוכני בינה מלאכותית בפעילותם.

עבור חברות, הטמעה של סוכני בינה מלאכותית אינה רק שאלה טכנולוגית, אלא גם שאלה של ממשל תאגידי, ניהול סיכונים וציות לדרישות רגולטוריות. חיבור סוכן בינה מלאכותית ליומנים, לתיבות דוא"ל, למערכות מסמכים, למאגרי לקוחות או למערכות תפעוליות מחייב בחינה מוקדמת של היקף ההרשאות, זרימות המידע, מנגנוני האישור, דרישות התיעוד ומערכי הגיבוי והשחזור.

קבוצת הסייבר והפרטיות במשרדנו מייעצת למגוון חברות וארגונים בהיבטים הנוגעים להטמעה של טכנולוגיות בינה מלאכותית ושימוש בהן, תוך התייחסות לסיכונים פרטיות ואבטחת מידע וצמצום החשיפות המשפטיות.

אנו מזמינים אתכם לפנות אלינו בכל שאלה או התייעצות בנושא.

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.

אנשי קשר



עידו ילין
עורך דין



רבקה גניס שפטובסקי
שותפה



אסף הראל
שותף