

תמוז תשפ"ו

יולי 2026

## המלצות להתנהלות הציבור בשימוש אישי בסוכני בינה מלאכותית

### רקע

"ניתן להבין סוכני בינה מלאכותית כמערכות התופסות את סביבתן ופועלות בה במידה מסוימת של אוטונומיה, תוך שימוש בכלים לפי הצורך להשגת מטרות ספציפיות והתאמה לנתוני קלט והקשרים משתנים".<sup>1</sup> היכולות של סוכני בינה מלאכותית מתאפשרות במידה רבה הודות למערכות בינה מלאכותית יוצרת (Generative AI) שמאפשרות להם לנתח ולפרש מידע, לקבל החלטות ולפעול לצורך ביצוע משימות מורכבות. בהשוואה למערכות בינה מלאכותית יוצרת,<sup>2</sup> סוכני בינה מלאכותית אינם מוגבלים למענה לשאלתה של המשתמש, והמאפיינים שלהם מעצימים את הסיכונים לפרטיות, לאבטחת מידע, לשקיפות ולשליטה האנושית.

מסמך זה סוקר חלק מן הסיכונים לפרטיות הנובעים משימוש בסוכני בינה מלאכותית **על ידי משתמשי קצה יחידים למטרות אישיות בלבד**, ומציע המלצות להתנהלות הציבור שיאפשרו להקטין סיכון זה. דוגמאות לשימושים אישיים של סוכני בינה מלאכותית כוללות, בין היתר, ניהול זמן ומשימות, לימודים ולמידה, בריאות וכושר, ניהול כספים וצרכנות, שיפור הרגלים, תכנון טיולים, פנאי וניהול תקשורת.

ההמלצות במסמך זה אינן עוסקות בשימוש בסוכני בינה מלאכותית למטרת עיבוד מידע אישי במסגרת מאגרי מידע כהגדרתם בחוק הגנת הפרטיות, קרי לצרכי עבודה או למטרה עסקית או ארגונית, ואינן גורעות מן החובות והדרישות החוקיות החלות על בעלי השליטה במאגרי המידע והמחזיקים בהם לפי חוק הגנת הפרטיות, כמפורט בטיטת ההנחיה שפרסמה הרשות בנושא.<sup>3</sup>

<sup>1</sup> ראו OECD (February 2026) [The agentic AI landscape and its conceptual foundations](#), (עמ' 15):

"AI agents can be understood as systems that perceive and act upon their environment with a degree of autonomy, using tools as needed to achieve specific goals and adapt to changing inputs and contexts."

<sup>2</sup> ראו מסמך המלצות להתנהלות הציבור במערכות בינה מלאכותית יוצרת שפרסמה הרשות להגנת הפרטיות: <https://www.gov.il/he/pages/ai147>

<sup>3</sup> עיבוד של מידע אישי באמצעות סוכני בינה מלאכותית הנעשה במסגרת ארגונית או עסקית כפוף לדרישות ולחובות הספציפיות המוטלות על בעל שליטה במאגר מידע ועל מחזיק במאגר מידע, כהגדרתם בחוק הגנת הפרטיות, התשמ"א-1981. חובות אלו פורטו בהרחבה בהנחיית הרשות להגנת הפרטיות בנושא "תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית" (אפריל 2025), שפורסמה כטיטת להערוך הציבור. טיטת ההנחיה [זמינה כאן](#).

## איך פועלים סוכני בינה מלאכותית?

סוכן בינה מלאכותית מיועד לפעול כדי להשיג מטרה עבור המשתמש בהתאם להוראותיו ובאמצעות כלים הזמינים לו. הגדרת המטרה עבור הסוכן כוללת לעיתים קרובות גם הגדרה לגבי מה הסוכן נדרש ורשאי "לדעת", כיצד הוא נדרש לפעול ובאיזה אופן עליו להפיק את התוצרים.

**דוגמה:** סוכן בינה מלאכותית המתוכנן לעקוב אחר הוצאות והכנסות משפחתיות, לנתח ולהציג היכן אפשר לחסוך, לתכנן ולהציג תקציב חודשי, ולהתריע על חריגות או הוצאות לא מתוכננות.

בין המרכיבים של סוכני בינה מלאכותית שמאפשרים להם להבין, לתכנן, לפעול ולהשתפר לאורך זמן, אפשר לציין כמה אלמנטים בולטים:

1. **"מוח":** זהו רכיב ליבה של הסוכן המבוסס בדרך כלל על מודל שפה גדול (LLM - Large language model) ואחראי על הבנת הוראות, ניתוח מידע, קבלת החלטות ותכנון פעולות. ה"מוח" מפרש הוראות משתמש ובונה רצף פעולות להשגת מטרה.

**דוגמה:** סוכן עוזר אישי המקבל בקשה כמו "תכנן לי סוף שבוע בתל אביב" מפרש את הנדרש לביצוע באמצעות ה"מוח" ומבין שעליו לתכנן לוח זמנים, להתחבר לאתרי מידע הכוללים פרסומים על אירועים ולהשוות אותם לפעילויות ביומן של המשתמש.

2. **"זיכרון":** הזיכרון מאפשר לסוכן לשמור מידע לאורך זמן (למשל העדפות והקשר של הפעולות), ולשפר ביצועים באמצעות התאמת הפעולות במצבים חדשים לאינטראקציות קודמות.

**דוגמה:** סוכן עוזר אישי הנדרש לתכנן סוף שבוע בתל אביב עשוי שלא להציע אפשרויות למלונות אם יש באפשרותו להבין מאינטראקציות קודמות שהמשתמש גר בתל אביב. לחלופין, הסוכן עשוי שלא להציע מופעים או אתרים שהכרטיסים אליהם מופיעים במייל של המשתמש בשנה האחרונה.

3. **"ידיים":** כלים וממשקים למערכות חיצוניות, למשל לקבלת מידע לניתוח או לביצוע פעולות. "הידיים" מאפשרות לסוכן לגשת למשאבים דיגיטליים, להפעיל שירותים ולפעול באינטגרציה עם יישומים.

**דוגמה:** סוכן עוזר אישי הנדרש לתכנן סוף שבוע בתל אביב עשוי להזמין מקום באתר של מסעדה ולשריין מועד בהתאם ביומן של המשתמש.

אלמנטים אלו של סוכני בינה מלאכותית יוצרים כמה מהמאפיינים המרכזיים בהגדרות של סוכני בינה מלאכותית, וביניהם השפעה על הסביבה (Influence on Environment), אוטונומיה (Autonomy), אדפטיביות (Adaptiveness) והסקה (Inference).<sup>4</sup> לעומת מערכות בינה מלאכותית יוצרת שגם בהן לרוב כלולים אלמנטים של "מוח" ו"זיכרון", המאפיינים של סוכני בינה מלאכותית שמאפשרים להם לפרש מטלות, לבצע משימות מורכבות ולקבל החלטות ללא מעורבות המשתמש,

<sup>4</sup> ראו [The agentic AI landscape and its conceptual foundations](#), OECD (February 2026), (עמ' 14-16).

תוך ריכוז, עיבוד והסקה של מידע אישי בהיקף נרחב, מעצימים את הסיכונים למידע האישי ולפרטיותו של המשתמש.<sup>5</sup>

### סוכני בינה מלאכותית ואתגרים להגנת הפרטיות

השימוש בסוכני בינה מלאכותית מאפשר ביצוע משימות מורכבות בהתאמה אישית על בסיס הוראות כלליות בשפה טבעית. כדי לבצע זאת בהצלחה ולתת ערך משמעותי למשתמש, הסוכנים נדרשים לנתח מידע רב, ולפעול ברמה מסוימת של אוטונומיה. כפועל יוצא מכך, סוכני בינה מלאכותית יוצרים אתגרים מהותיים להגנה על מידע אישי במספר תחומים מרכזיים:

1. ריכוז ידע ותובנות אצל הסוכן<sup>6</sup>: סוכני בינה מלאכותית פועלים לעתים קרובות תוך חיבורים למערכות מידע של המשתמשים, כגון יומנים, מיילים או פירוט תשלומים שוטף. הסוכן עשוי לקבל גישה למידע אישי בהיקף נרחב מאוד העולה על הנדרש לביצוע המשימה הספציפית, וזאת כתוצאה מהגדרות חיבור רחבות מדי, הרשאות גישה עודפות או היעדר סינון מוקדם של המידע הנגיש אליו.

**דוגמה:** סוכן למיון דואר אלקטרוני מקבל גישה לתיבת המייל האישית לצורך מיון המיילים לתיקיות (כגון עבודה, לימודים ופנאי). בעוד שהמשתמש מעוניין אך ורק במיון תכתובת נכנסת מהשנתיים האחרונות שבהן הוא התחיל ללמוד לתואר שני – הסוכן מנתח את כל תכולת תיבת המייל ב-15 השנים שחלפו מפתחתה, כולל דואר יוצא וטיוטות המשמשות לגיבוי. הסוכן ממין את כלל המידע מהתכתבויות קודמות ומשתמש במידע זה למיון של הודעות עתידיות.

הדוגמה ממחישה את הסיכון הטמון בכך שלעיתים המשתמש עלול להתקשות להעריך את היקף ואופי המידע שהסוכן יכול לגשת אליו, כמו גם את סוג הדפוסים והמסקנות שניתן להסיק על בסיסו ובהצלבה עם מקורות מידע אחרים. אמנם גישה רחבה למידע מגוון עשויה לתרום לביצוע הפעולות של הסוכן ולהפוך אותן למהירות, מדויקות ויעילות יותר, אך הסוכן עשוי לרכז ידע רחב וליצור פרופיל אישיותי מקיף, בין היתר על הרגלים יומיומיים, קשרים חברתיים, העדפות צריכה, מצב בריאותי או התנהלות פיננסית, שלא היה קיים בעבר במקום אחד. זהו סיכון משמעותי בייחוד כשהמשתמש אינו מבין את ההיקף הנרחב של חשיפת המידע שלו, באופן הנדרש כדי לגבש הסכמה מדעת.

2. פעולה של הסוכן על בסיס מידע אישי רחב: בשונה ממודלי שפה גדולים, סוכני בינה מלאכותית מאופיינים ביכולת לפעול בהתאם למידע אישי שנשמר או מוסק על ידם. ההיקף הרחב של המידע שנגיש לסוכן הבינה המלאכותית ומוסק על ידו לאורך זמן מקשה על המשתמש להעריך

<sup>5</sup> ראו פרסום של רשות הגנת המידע הבריטית (ICO) בנושא סוכני בינה מלאכותית, [ICO tech futures: Agentic AI](#), (January 2026).

<sup>6</sup> בהקשר זה יש לציין כי הסוכן עצמו ובפרט מודל השפה ("המוח") המשמש אותו, לרוב מפותחים בחברה מסחרית שעשויה לקבל גישה לידע ולתובנות שהפיק הסוכן.

באופן מלא וממצה את סוג ואופי הנתונים שעשויים להשפיע על פעולות הסוכן. במצב כזה מתחדד הסיכון לפרטיות בדמות שימוש של הסוכן במידע אישי ובמסקנות שהוא הפיק מחוץ להקשר ושלא בהתאם לציפייה של המשתמש, או בחשיפה שלהם לצדדים שלישיים באמצעות פעולה, ניסוח או המלצה.

**דוגמה:** סוכן אישי לניהול בריאות וכושר מקבל גישה ליומן, לנתוני פעילות גופנית ולרשימת קניות, כדי לנהל תפריט שבועי ותזכורות לאימונים. לאורך זמן, הסוכן מסיק מן המידע כי ייתכן שהמשתמש מתמודד עם רגישות רפואית מסוימת. בהמשך, כאשר המשתמש מבקש מהסוכן להזמין מקום במסעדה עבור מפגש חברתי, הסוכן מציין במסגרת ההזמנה כי נדרשת התאמה תזונתית מיוחדת, מבלי שהמשתמש התכוון לחשוף מידע זה בפני אחרים.

הדוגמה ממחישה את הסיכון בפעולה של הסוכן על בסיס מידע אישי, מסקנות והמלצות שלא הוזנו במפורש אך עשויים להצטבר לכדי פרופיל אישיותי מקיף ושלם ולכלול העדפות, הרגלים, מאפייני התנהגות ותפקוד מקצועי. מידע זה עלול להיות רגיש ביותר, לא בהכרח מדויק ולא בהכרח ידוע לנושא המידע, ולשמש בסיס להחלטות ופעולות של הסוכן או מערכות אחרות.

3. יכולת החלטה עצמית של סוכן על מידע אישי: סוכני בינה מלאכותית אינם רק צרכני מידע, אלא גם בעלי יכולת פעולה אקטיבית ואוטונומית: עריכה, עדכון, מחיקה והעברה של מידע אישי במערכות אליהן הם מחוברים. הפעולה האוטונומית של הסוכן עלולה שלא לעלות בקנה אחד עם הרצון של המשתמש ולפגוע במידע האישי שלו.

**דוגמה:** סוכן שמטרתו לפנות שטח אחסון בתיבת הדוא"ל מזהה מיילים ישנים (צילומי תעודות, מרשמים רפואיים, חוזי שכירות) ומוחק אותם לצמיתות לאחר תקופה מוגדרת. המשתמש אינו יכול לשחזר מידע אישי חיוני הנדרש לצורך תביעת ביטוח.

הדוגמה ממחישה את הסיכון לכך שיכולות הפעולה של הסוכן, כאשר אינן מוגדרות ומפוקחות כראוי, עלולות לגרום לפגיעה באבטחת המידע ובשלמותו<sup>7</sup> ולאובדן מידע אישי.

אתגרים אלו מחייבים משנה זהירות בכל הנוגע למתן גישה של סוכני בינה מלאכותית למידע אישי, להגדרת הפעולות שמותר לסוכן לבצע ולפיקוח על פעולתו.

<sup>7</sup> ראו הגדרות המונחים "אבטחת מידע" ו"שלמות המידע" בסעיף 3 לחוק הגנת הפרטיות.

## המלצות לשימוש אחראי בסוכני בינה מלאכותית<sup>8</sup>

סוכני בינה מלאכותית מיועדים במקרים רבים לפעול כעוזר אישי, המבצע פעולות עבור המשתמש באופן יעיל, מהיר ולעיתים גם אוטומטי ואוטונומי. כאשר סוכן בינה מלאכותית מחליף פעולות שבעבר בוצעו על ידי המשתמש או עוזר אנושי, כמו קריאת מיילים, ניהול יומן, ביצוע רכישות או קיום תקשורת עם גורמים אחרים - הוא נדרש לתפקד כמעין "איש סוד דיגיטלי" שמצופה ממנו להבין את הקשר ביצוע הפעולה, להפעיל שיקול דעת, לעשות שימוש במידע אישי אליו קיבל גישה, ולפעול בהתאם לרצון המשתמש (כפי שהוא מבין אותו), אך ללא התערבותו.

מכאן נובע הסיכון למידע האישי ולפרטיות, שהרי סוכן בינה מלאכותית אינו בהכרח בעל אינטואיציה חברתית או הבנה ערכית התואמת את הכוונה של המשתמש או את הנורמות המקובלות החלות בסיטואציה בה הוא נדרש לפעול. לפיכך, ולאור מאפייניהם הייחודיים של סוכני בינה מלאכותית, מומלץ לאמץ עקרונות עבודה ייעודיים לצמצום הסיכונים לפרטיות ולמידע אישי.

להלן עקרונות מרכזיים לשימוש אחראי בסוכני בינה מלאכותית:

1. **צמצום הגישה למידע אישי:** הנטייה הרווחת בשימוש בסוכן בינה מלאכותית היא לאפשר לו לאתר מידע רלוונטי למילוי המשימה באופן אוטונומי, וכך לתת לסוכן גישה רחבה למקורות מידע אישי. הגדרה ספציפית של המידע האישי הזמין עבור הסוכן לביצוע משימותיו תסייע למשתמש לגדר את השימוש במידע האישי על אודותיו ובהתאם תאפשר לצמצם את הסיכון לפרטיות.

**דוגמה:** סוכן בינה מלאכותית נדרש להכין דוח שנתי למס הכנסה ולרכז לצורך כך חשבוניות שהתקבלו במייל. ניתן להנחות את הסוכן לבדוק רק את המיילים שהתקבלו בשנת 2025, תוך הימנעות מבדיקת מיילים שהגיעו מבני משפחה או מחברים. כמו כן, ניתן לפתוח תיבת מייל ייעודית לחשבוניות, המופרדת מתיבת המייל הפרטי, ולהנחות את הסוכן לבדוק רק אותה.

**דוגמה:** סוכן המסייע למשתמש לכתוב פוסטים מקצועיים נדרש להכין פרסום ללינקדין בהקשר לאירוע אקטואלי. לצורך כך לסוכן ניתנת גישה למידע על האירוע מאתרי חדשות לשם הבנת הנושא ולפרסומים קודמים של המחבר לשם חיקוי סגנון הכתיבה שלו. לעומת זאת, הסוכן אינו מקבל גישה למיילים שכוללים תכתובת בנוגע לאירוע ובהם גם פרטים אישיים של המעורבים בו.

**דוגמה:** סוכן שמטרתו לקבוע פגישות עבור המשתמש מקבל גישה לחשבון המייל והיומן. ניתן להנחות את הסוכן לבדוק אך ורק את הזמינות ביומן (פנוי/תפוס בלבד), ולא לגשת לכותרת ולתוכן הפגישות.

<sup>8</sup> ההמלצות ממוקדות לתחומים שבשליטת המשתמש בסוכני בינה מלאכותית לצרכים אישיים ואינן מתייחסות לאמצעים נדרשים ומומלצים באימון, פיתוח ובדיקה של מערכות אלו.

הדוגמאות ממחישות את הצורך לדעת (need to know) כבסיס לכך שהסוכן יקבל גישה אך ורק למידע ההכרחי לביצוע המשימה שהוגדרה לו, ולפרק הזמן הנדרש לכך. בתוך כך ניתן להגדיר הרשאות ספציפיות לפי סוג מידע, מקור מידע והקשר השימוש בו, ולהימנע מחיבורים למאגרי מידע שלמים, בעיקר כאשר ניתן לספק לסוכן תת-קבוצה רלוונטית של נתונים. צמצום הגישה למידע מפחית את היקף המידע האישי אליו נחשף הסוכן, מצמצם את הסיכון לשימוש במידע בניגוד למטרה ולציפיות של המשתמש או לשם הסקה לא רצויה, ומקטין את היקף הפגיעה במקרה של דליפת מידע.

בתוך כך, מומלץ להימנע מאימון של הסוכן על המידע האישי, מאחר והתוכן שמעובד על ידי הסוכן עשוי להישמר ולהפוך בעתיד לחלק מהמנגנונים במערכת. מומלץ להעדיף פתרונות המאפשרים עיבוד זמני בלבד, ללא שמירת היסטוריה וללא שימוש במידע האישי לצורכי אימון. במידת האפשר מומלץ להימנע משמירה של המידע האישי בזיכרון הסוכן. במקום להעתיק מסמכים, אנשי קשר, הודעות או קבצים, עדיף שהסוכן יקבל גישה זמנית ומבוקרת למידע, ואם נוצרו קבצים זמניים לצורך פעולה מסוימת – יש לקבוע הגדרות כך שיימחקו כשאננם נדרשים עוד.

**דוגמה:** סוכן אישי המסכם פגישות, אך אינו שומר עותק של ההקלטות או התמלילים לאחר יצירת הסיכום.

**דוגמה:** סוכן לניהול משימות שמקבל גישה זמנית ליומן המשתמש, בלי להעתיק את המידע ומבלי לבצע עליו אימון של המודל.

2. **צמצום חשיפת מידע אישי וניהול ממשקים חיצוניים:** סוכן בינה מלאכותית אישי יכול לרכז ולעבד מידע רגיש ממקורות רבים (כגון מיילים, יומן וקבצים), כמו גם לפעול באינטראקציה עם מערכות חיצוניות ולהפיק פלט בתגובה לשאילתות. יש לוודא כי הממשקים החיצוניים של הסוכן אינם מביאים למסירת מידע למי שלא אושר על ידי המשתמש ובהיקף רחב מהנדרש.

**דוגמה:** בסוכן בינה מלאכותית המשמש לקביעת פגישות ניתן להפעיל כלל/הנחייה שלא למסור שמות של משתתפים בפגישות לגורמים חיצוניים.

**דוגמה:** בסוכן בינה מלאכותית המשמש לניהול נסיעות ניתן להנחות את הסוכן שלא לשתף עם בתי מלון או חברות תחבורה מידע על מטרת הנסיעה, פגישות מתוכננות או זהות המשתתפים האחרים ביומן המשתמש, אלא אם המשתמש אישר זאת במפורש.

3. **צמצום הרשאות גישה:** במקרים רבים, הסוכן אינו נדרש לבצע פעולות אקטיביות כמו מחיקה, עדכון, שליחה או שינוי מידע כדי לספק ערך משמעותי למשתמש. סוכן שמנתח מסמכים, מסכם ישיבות, מציע תובנות או ממליץ על פעולות עתידיות יכול לפעול בצורה יעילה גם כאשר הוא

רק צופה במידע הקיים. מומלץ לתת לסוכן רק את הרשאות ההכרחיות לצורך ביצוע המשימה, כגון הרשאות צפיה או קריאה בלבד, ללא הרשאות שינוי או עריכה. ככל שלסוכן ניתנו הרשאות מצומצמות יותר, כך קטן הסיכון לנזק במקרה של טעות, תקלה, שימוש בלתי צפוי או אירוע אבטחת מידע.

**דוגמה:** סוכן המסכם פגישות בהתאם לזימונים ביומן האישי, אך אינו יכול לשנות מועדים, להזמין משתתפים או לבטל פגישות.

**דוגמה:** סוכן משפטי שמנתח מסמכים מקצועיים ומציג סיכונים או סעיפים חריגים, אך אינו מורשה לערוך את המסמך או לשלוח אותו לגורמים חיצוניים.

**דוגמה:** סוכן אישי לניהול דואר אלקטרוני שמציג הודעות חשובות ומציע תשובות אפשריות, אך אינו שולח מיילים בפועל ללא אישור מפורש של המשתמש.

4. **בקרה וניטור:** כאמור, סוכני בינה מלאכותית עלולים לאפשר פעולות במידע אישי שאינן עולות בקנה אחד עם הציפיות של המשתמש, ולעיתים אף בניגוד להן. כשם שנדרשת בקרה על עוזר אישי אנושי כדי לוודא שהוא פועל בהתאם לציפיות של הממונים עליו, כך נדרשת בקרה על סוכן בינה מלאכותית כדי להבטיח את ההגנה על המידע האישי שהוא רשאי לגשת אליו. להלן כמה מהלכים שניתן לנקוט לצורך כך:

**אישור אנושי:** ביצוע פעולות מסוימות רק לאחר בחינה של המשתמש ואישורו. לדוגמה, סוכן בינה מלאכותית יכול לנסח מיילים אך לשלוח אותם רק לאחר סקירה ואישור של המשתמש.

**תכנון לפני ביצוע:** הצגה למשתמש של רצף השלבים המתוכננים ומימוש התוכנית רק לאחר קבלת אישור. לדוגמה, סוכן בינה מלאכותית יכול לפרט את מקורות המידע שהוא מתכנן לגשת אליהם לצורך ביצוע משימה ולבצע את החיבור רק לאחר אישור המשתמש לכך.

**תיעוד:** רישום של כלל הפעולות במידע אישי שבוצעו על-ידי הסוכן (מתי, מה, למה), עם אפשרות להציגו למשתמש. לדוגמה, סוכן בינה מלאכותית יכול להציג את היסטוריית השינויים של הזימונים לפגישות ואת המידע ששימש לכל פעולה (כגון פניה אל המשתתפים, התנגשות עם תזמון אחר או אופטימיזציה שהסוכן הפעיל) באופן שהמשתמש יוכל לוודא שהסוכן פועל בהתאם לציפיותיו.

5. **גיבוי ושחזור:** עם הרשאות מתאימות, סוכני בינה מלאכותית יכולים לערוך, למחוק או לשנות מידע בקנה מידה רחב ובמהירות. גיבוי של המידע לפני מתן הרשאות לסוכן בינה מלאכותית יכולה לאפשר שחזור כאמצעי נוסף לניהול סיכונים.



**דוגמה:** לפני ביצוע פעולה של חלוקת קבצים לתיקיות ומחיקת קבצים כפולים ניתן לגבות את כל תוכן התיקיה למיקום חיצוני, כך שאם סוכן הבינה המלאכותית ביצע מחיקה שאינה תואמת את הנדרש, ניתן יהיה לשחזר משם את הקבצים הרלוונטיים. לחלופין, אפשר להגדיר העברה לסל מחזור שממנו ניתן יהיה לשחזר את המידע לאורך תקופה מסוימת, במקום מחיקה לצמיתות.

יישום משולב של צמצום הגישה למידע אישי, ניהול ממשקים חיצוניים, וקיום הליכים לבקרה וגיבוי מאפשרים למצות את היתרונות הטכנולוגיים של סוכני בינה מלאכותית, תוך צמצום הסיכונים לזכות לפרטיות וחיזוק השליטה של המשתמש ביחס לשימוש במידע אישי אודותיו.