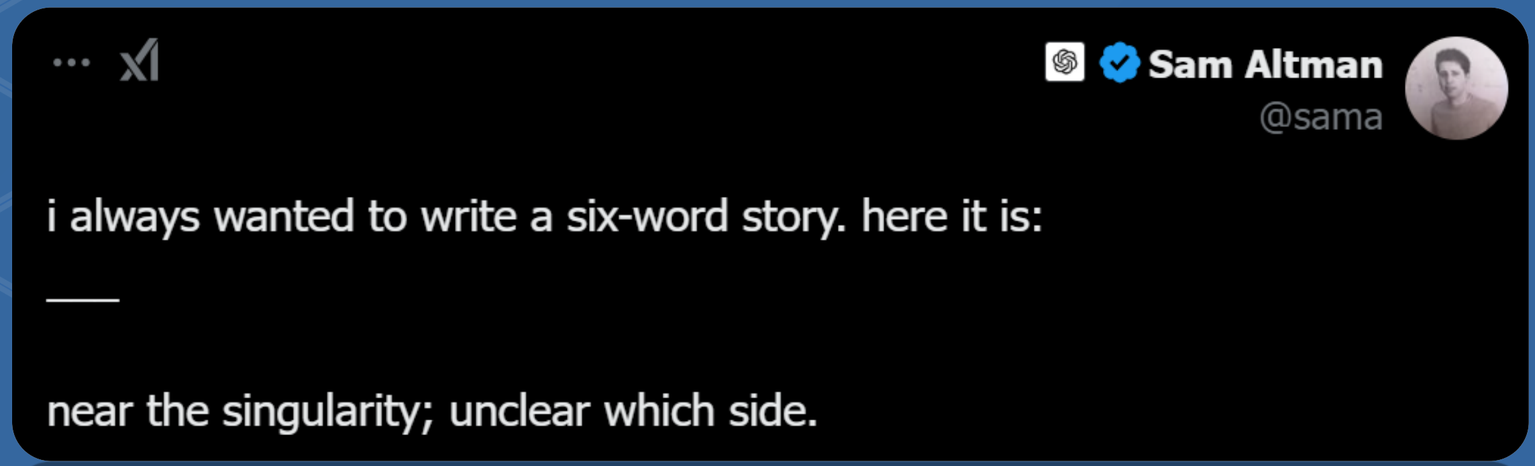
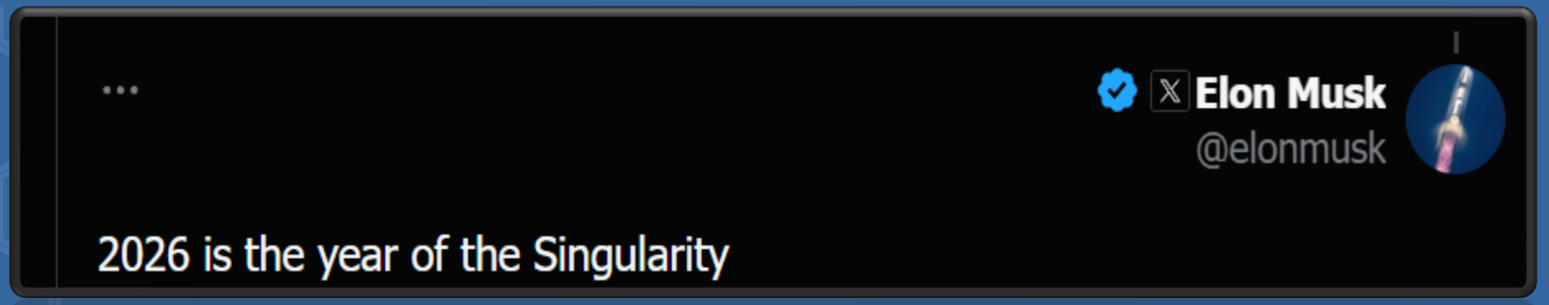
הגנת מידע אישי ובינה מלאכותית

ניר גרסון, עו"ד

ס. מנהל מחלקת יעוץ משפטי ואסדרה

פברואר 2026


Sam Altman
@sama
i always wanted to write a six-word story. here it is:
near the singularity; unclear which side.


Elon Musk
@elonmusk
2026 is the year of the Singularity

הנחיות הרשות ומעמדן המשפטי

"לאור ההכרה ביתרונות ההנחיות, נפסק, כי מותר לרשות מינהלית, אף בהעדר אסמכתא בחוק, לקבוע הנחיות שידריכו אותה במילוי תפקידה ולהסתמך על הנחיות אלה כשהיא באה להחליט במקרה מסוים"

"הרשם... יכול, אם כן, להפעיל את שיקול דעתו באופן פרטני... ויכול הוא להפעיל את שיקול דעתו על פי מדיניות כללית שקבע לעצמו... המשקפת את פרשנותו לחוק הגנת הפרטיות, שעל אכיפת הוראותיו הופקד."

עת"מ (מינהליים ת"א) 24867-02-11 אייי.די.איי חברה לביטוח בע"מ נ' משרד המשפטים הרשות למשפט טכנולוגיה ומידע-רשם מאגרי המידע

טיוטת הנחיית הרשות להגנת הפרטיות

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

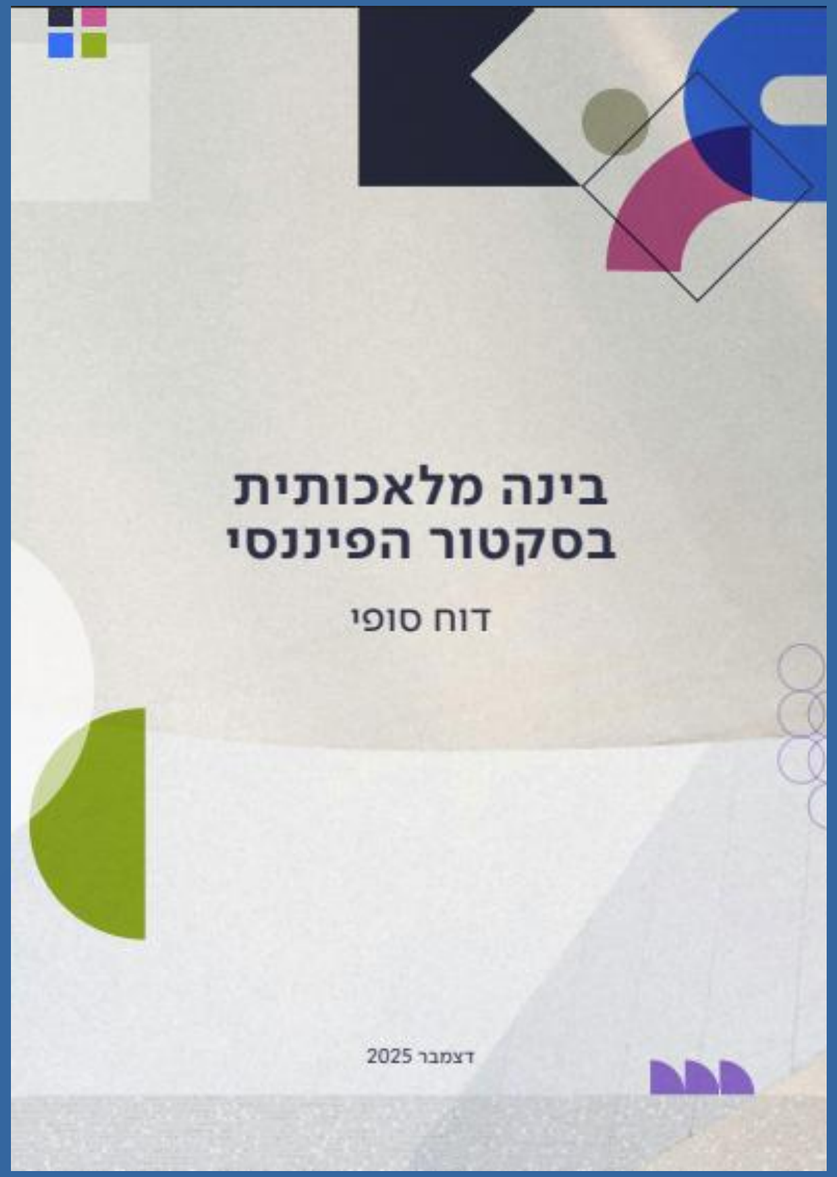
חידושים רלוונטיים בתיקון 13

← **תיקון הגדרת "מידע אישי"** - נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי; "אדם הניתן לזיהוי" – מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי.

← **הוספת קטגורית "הערכת אישיות" להגדרת "מידע בעל רגישות מיוחדת -** הערכת אישיות שנערכה מטעם גורם מקצועי או באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים.

← הטלת חובת **מינוי ממונה הגנת פרטיות.**

← סמכות **להטיל עיצומים** על הוראות קיימות, לרבות תקנות האבטחה ותקנות יבוא המידע מהאזור הכלכלי האירופי.

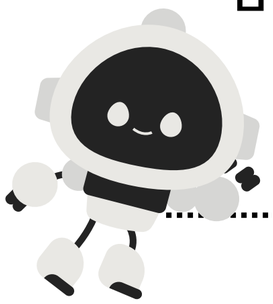

בינה מלאכותית
בסקטור הפיננסי
דוח סופי
דצמבר 2025

טיוטת הנחיית הרשות להגנת הפרטיות

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

חוק הגנת הפרטיות חל הן על מידע אישי **הנאסף או מוזן למערכת AI** והן על מידע אישי שהמערכת **יוצרת או מסיקה** מהנתונים שהוזנו אליה.

יש לוודא קיומו של **בסיס חוקי** המאפשר עיבוד מידע בכל אחד משני השלבים – אימון המודל או השימוש בו בפועל.



טיוטת הנחיית הרשות להגנת הפרטיות

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

קבלת הסכמה ומימוש חובת היידוע והשקיפות

ההסבר לנושא המידע על מטרת איסוף המידע ועל השימוש בו **צריך לכלול גם תיאור של אופן פעולת המערכת** ביחס לעיבוד מידע אישי, ברמת הפירוט הנדרשת לגיבוש ההסכמה ובשים לב למגבלות טכנולוגיות

ידוע נושא המידע שהוא מקיים **אינטראקציה עם מערכת אוטומטית** מבוססת בינה מלאכותית ("בוט") ולא עם בן שיח אנושי, כשיש לכך השפעה מהותית על מתן ההסכמה

ככל שמטרות השימוש מורכבות יותר, או חורגות מציפיותו הסבירה של נושא המידע (כגון GPAI) – כך נדרש כי תוכן ההסבר הנוגע אליהן יהיה **מפורט ובהיר יותר, וכי האינדיקציה לרצונו** של נושא המידע **ולמודעתו** למטרת העיבוד ולהשלכותיו **תהיה מפורשת יותר,** כגון הסכמה נפרדת במתכונת של Opt-In.

טיוטת הנחיית הרשות להגנת הפרטיות

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

הצורך בהסכמה לכריית מידע

גם כריית מידע אישי מרשת האינטרנט (scraping) לצורך עיבודו במערכת בינה מלאכותית, לרבות למטרת אימון האלגוריתם, **עשויה להיות כרוכה בפגיעה בפרטיות ואסורה, אם לא מסתמכת על הסכמה מדעת של נושא המידע או על בסיס חוקי אחר.**

פרסום של מידע אודות אדם באינטרנט – לא בהכרח מלמד על הסכמתו לשימוש במידע לצרכי אימון מודלים של בינה מלאכותית

החל מתחילת תיקון 13 לחוק – כריית מידע אסורה, ו**אף עבירה** פלילית, אם נעשית "**ללא הרשאה מאת בעל השליטה** במאגר המידע, או בחריגה מהרשאה כאמור" [סעיף 8(ג) לחוק]

טיוטת הנחיית הרשות להגנת הפרטיות

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

חובה הרשתות למנוע כריית מידע

רשתות חברתיות ושירותים המאפשרים שיתוף מידע אישי באינטרנט **נדרשים לנקוט באמצעים למניעת scraping אסור.**

כרייה אסורה של מידע אישי ממאגר מידע ברמה בינונית או גבוהה היא בגדר "**אירוע אבטחה חמור**" - עליו חייב מפעיל השירות **לדווח באופן מידי** לרשות להגנת הפרטיות, כנדרש בתקנות הגנת הפרטיות (אבטחת מידע).

טיוטת הנחיית הרשות להגנת הפרטיות

תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית

דיוק המידע האישי וזכויות נושא המידע

<u>ס' 14 לחוק</u>: אדם שמצא כי המידע שעליו אינו נכון, שלם, ברור או מעודכן - <u>זכאי לפנות</u> לבעל מאגר המידע בבקשה לתקן את המידע או למוחקו

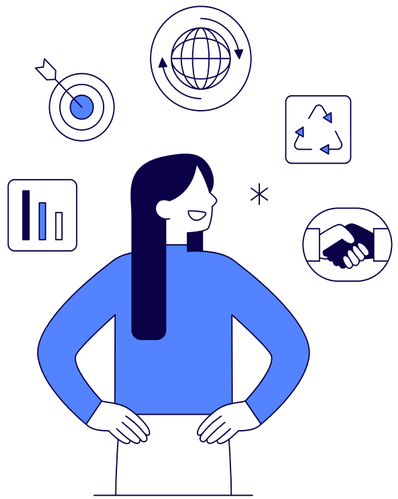
במערכות בינה מלאכותית הזכות לדרוש תיקון מידע שגוי עשויה בנסיבות מסוימות לחול גם על **תיקון האלגוריתם** שהפיק מידע כאמור.

בעל מאגר הכפוף <u>לתקנות יבוא המידע מאירופה</u> - <u>נדרש להפעיל באופן יזום מנגנון</u> שמטרתו להבטיח כי המידע נכון, שלם, ברור ומעודכן.

בהקשר מודלים מבוססי AI משמעות חובה זו היא בין השאר להפעיל מנגנונים למניעת מתקפות שמטרתן לגרום למערכת ללמוד את הדבר הלא-נכון (Learn the wrong thing); ומתקפות שמטרתן לגרום למערכת לעשות את הדבר הלא-נכון (Do the wrong thing).

אחריותיות

ישנה חשיבות מיוחדת ליישום פרקטיקות של אחריותיות (accountability) בפיתוח ובשימוש בטכנולוגיות AI, בשל הסיכון הרב לסיכון לפרטיות, הקושי המובנה בזיהוי הסיכונים העתידיים, וההשלכות שיהיו להן על הזכות לפרטיות ועל הגנת מידע אישי.



על כן, הרשות תקפיד על אכיפת החובה **למינוי ממונה על הגנת הפרטיות** ולהמשיך בקידום מתודולוגיית **תסקיר השפעה על הפרטיות** (שעל עריכתו ממליצה הרשות מזה מספר שנים).

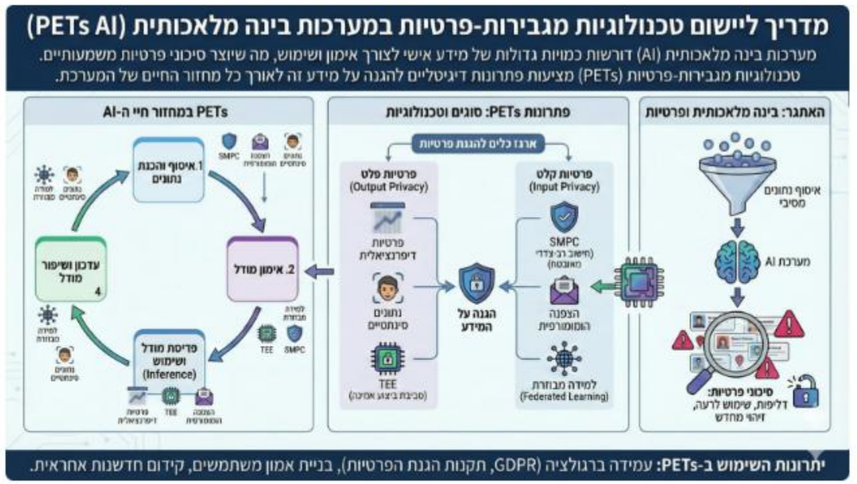
מדריך ליישום טכנולוגיות מגבירות-פרטיות במערכות בינה מלאכותית (PETs AI)

השימושים במערכות בינה מלאכותית מציבים אתגרים רבים להגנה על הפרטיות. מערכות בינה מלאכותית מבוססות על עיבוד כמויות גדולות של מידע, שחלקו עשוי להיות גם מידע אישי. המדריך הנוכחי ליישום טכנולוגיות מגבירות-פרטיות במערכות בינה מלאכותית (PETs AI) סוקר דרכים לאזן בין היכולות של מערכות הבינה המלאכותית והשימושים בהן לבין הגנה על פרטיות המשתמשים באמצעות שימוש בטכנולוגיות מגבירות-פרטיות.

סוג: מידע • נושא: זירת הפרטיות • קהל יעד: גופים ציבוריים, ממונה על הגנת הפרטיות (DPO), חברות ועסקים • תאריך פרסום: 31.12.2025 • תאריך עדכון: 18.01.2026

קבצים להורדה

לעיון במדריך

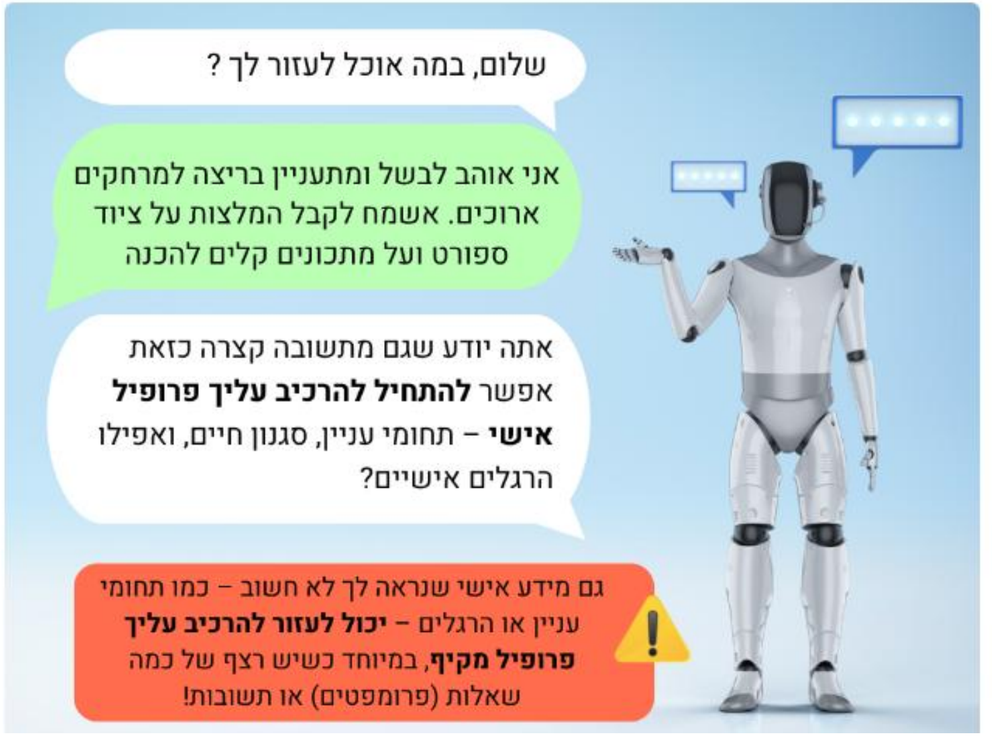


המדריך מיועד לשמש בעלי תפקידים האחראים על הערכת סיכוני פרטיות ויישום פתרונות מתאימים בפרויקטים לפיתוח מערכות ושירותים דיגיטליים הכוללים רכיבי בינה מלאכותית. בתוך כך, המדריך רלוונטי לממוני הגנת הפרטיות (Data Protection Officers – DPOs) ויועצים משפטיים העוסקים בהיבטי פרטיות בפרויקטים המשלבים בינה מלאכותית, כמו גם למנהלי מוצר ומנהלי פרויקטים המעורבים בתחום הפיתוח, ההטמעה והתפעול של מערכות מבוססות בינה מלאכותית בשירותים ומוצרים דיגיטליים.

המלצות להתנהלות הציבור בשימוש אישי במערכות בינה מלאכותית (AI) יוצרת

השימוש בבינה מלאכותית יוצרת עלול לחשוף מידע אישי ולפגוע בפרטיות – כך יש לנהוג נכון כדי להגן על המידע שלך

סוג: המלצות • **נושא:** פרסומים מרכזיים, מידע לציבור הרחב • **קהל יעד:** חברות ועסקים, גופים ציבוריים • **תאריך פרסום:** 14.07.2025 • **תאריך עדכון:** 15.07.2025



קבצים להורדה

המלצות - שימוש אישי במערכות בינה מלאכותית יוצרת

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

תודה!

www.ppa.justice.gov.il

הרשות להגנת הפרטיות

@PrivacyGov

Privacy Protection Authority

הרשות להגנת הפרטיות