

עדכון לקוחות:

רגולציית AI בישראל -

הרשות להגנת הפרטיות פרסמה טיוטת הנחיה
שאתם צריכים להכיר



8 במאי, 2025

לקוחות יקרים,

ביום 28.4.25 פרסמה הרשות להגנת הפרטיות טיוטת הנחיה תקדימית, המבהירה כיצד חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**החוק**") יחול על שימוש במערכות בינה מלאכותית (AI). מדובר במסמך רגולטורי משמעותי, שמטרתו לשרטט את גבולות ההגנה על פרטיות הציבור בעידן הבינה המלאכותית.

ההנחיה, שפורסמה בשלב ראשון כטיוטה להערות הציבור, מסבירה איך הרשות מתכוונת לפרש ולאכוף את דיני הגנת הפרטיות ביחס ל-AI ומדגישה שהחוק חל על בינה מלאכותית לכל אורך שלבי הפיתוח והיישום שלה – הן **בשלב האימון** והן **בשלב ההפעלה**, לרבות בעת שימוש בטכנולוגיות חיצוניות מבוססות בינה מלאכותית.

ההנחיה מתייחסת למגוון סוגיות מהותיות הנוגעות לשימוש במידע אישי במסגרת AI לרבות שאלת ההסכמה, דרישות שקיפות, אחריותיות, אבטחת מידע, ורישום מאגרי מידע, ומציבה רף רגולטורי חדש לארגונים המפתחים או מפעילים מערכות מסוג זה.

להלן יובאו עיקרי ההנחיה, ולנוחיותכם מצורפת [ההנחיה המלאה לעיון](#).

עיקרי ההנחיה

❖ תחולת החוק גם על מידע שנגזר ממערכות בינה מלאכותיות

כל מערכות בינה מלאכותית שמפיקות, מאחסנות או מנתחות מידע אישי, מערכות בינה מלאכותית שמפיקות, מנתחות או שומרות מידע אישי – גם כאשר המידע **לא נמסר ישירות**, אלא הופק מהסקת מסקנות או סיווגים – כפופות להוראות חוק הגנת הפרטיות.

המשמעות היא שחלים עליהן כללי שקיפות, הסכמה מדעת, הגבלת שימוש ואבטחת מידע.

❖ הסכמה מדעת ושקיפות מוגברת – גם כשמדובר במידע "פומבי"

ההנחיה קובעת כי **מידע אישי שפורסם באופן פומבי אינו בהכרח חופשי לשימוש**. כדי לעבד מידע כזה במסגרת AI יש צורך בהסכמה מדעת, לאחר יידוע פרטני וברור על אופן הפעולה של המערכת, סוגי המידע המעובד, הגורמים המעורבים והשימושים המתוכננים.

למשל: גם אם אדם פרסם מידע אישי מיוזמתו, לדוגמה, תמונה או פוסט ברשת חברתית, אין להסיק מכך שניתנה הסכמה לשימוש בו לצורך אימון אלגוריתם או כרייה אוטומטית של נתונים.

בנוסף, יש למסור לנושא המידע הסבר ברור בנוגע למטרות השימוש ואופן פעולתה של מערכת הבינה המלאכותית בעיבוד מידע אישי, לרבות פירוט בדבר סוגי מידע החשופים לעיבוד. כמו כן, יש ליידע את נושא המידע כאשר הוא מקיים אינטראקציה עם מערכת אוטומטית – "בוט" שאינו בן אנוש.

❖ **אחריותיות וניהול פרטיות בארגון**

הרשות מדגישה את החשיבות באימוץ עקרונות אחריותיות בשימוש בטכנולוגיות בינה מלאכותית, בשל הסיכון הגבוה לפגיעה בפרטיות והקושי לחזות את השלכות העיבוד מראש.

הרשות **מונה שורת צעדים שעל ארגונים ליישם**, שבהם מינוי ממונה על הגנת פרטיות (DPO), משהרשות סוברת כי הוא גם הגורם המתאים לטפל בשימוש במערכות בינה מלאכותית בארגון; ביצוע תסקיר השפעה על פרטיות (DPIA) בשימושים רגישים; גיבוש מדיניות פרטיות עדכנית; והסדרת השימוש בכלי GenAI כמו ChatGPT, לרבות פיקוח על שימוש חורג במידע אישי.

❖ **הגבלות על כריית מידע אישי (Scraping)**

ההנחיה קובעת כי כרייה אוטומטית של מידע אישי מאתרים פתוחים, לרבות רשתות חברתיות, **אינה מותרת מעצם הפומביות של המידע**. איסוף כזה, בהיעדר הסכמה או עילה חוקית, עלול להיחשב לעבירה על החוק.

יתרה מכך, בעלי שליטה במאגרי מידע המאפשרים שיתוף מידע אישי באינטרנט (רשתות חברתיות, אתרי היכרויות) נדרשים לנקוט באמצעים נאותים כדי למנוע כריית מידע אסורה מאתריהם. **כרייה אסורה של מידע אישי ממאגר מידע מהווה "אירוע אבטחה חמור"** בהגדרתו בתקנות הגנת הפרטיות (אבטחת מידע), ועל כן חלה חובה מיידית לדווח עליו לרשות.

❖ **מימוש זכויות נושאי מידע**

הזכויות חלות גם על מידע שמעובד באמצעות מערכת בינה מלאכותית, ועל כן ייתכן שיידרש מהארגונים לתקן אלגוריתמים וליישם מנגנונים שיבטיחו את דיוק המידע.

ההנחיה מתפרסמת בשלב ראשון כטיוטה להערות הציבור, והציבור מוזמן להעביר את התייחסותו והערותיו לטיוטת ההנחיה, זאת עד **ליום 5.6.25 בשעה 12:00**, באמצעות כתובת הדוא"ל ppa@justice.gov.il.

הסקירה שלעיל מהווה סיכום תמציתי. המידע המופיע בה נועד למטרות מידע בלבד, ואינו מהווה יעוץ משפטי מחייב.

אנו עומדים לרשותכם בכל שאלה, הבהרה ועניין הנוגעים לעניין זה, ובכלל.

שלכם – מחלקת הגנת הפרטיות ואבטחת מידע,

וקסלר ברגמן ושות', עורכי דין.

