

הגנת הפרטיות במערכות בינה מלאכותית – הנחיית הרשות להגנת הפרטיות

עדכוני לקוחות

לאחרונה פרסמה הרשות להגנת הפרטיות ("הרשות") [טיטות הנחיה](#) בנושא תחולת הוראות חוק הגנת הפרטיות ("החוק") על מערכות בינה מלאכותית ("ההנחיה"). ההנחיה מציגה את פרשנות הרשות להוראות החוק בהקשר של פיתוח ושימוש במערכות בינה מלאכותית, ומפרטת את האופן בו הרשות מתכוונת להפעיל את סמכויותיה בתחום זה, במיוחד לאחר כניסתו לתוקף של [תיקון 13 לחוק הגנת הפרטיות](#) ("תיקון 13") באוגוסט 2025.

בעדכון זה נסקור את הנקודות העיקריות בטיטות ההנחיה שרלוונטיות לחברות ועסקים, ונציע צעדים פרקטיים להיערכות.

הסכמה מדעת ודרישת הידוע

ההנחיה מציינת כי שימוש במידע אישי אודות אדם במערכות בינה מלאכותית טעון קבלת הסכמה מדעת מאותו אדם. לעמדת הרשות, כתנאי לקבלת הסכמה בת תוקף יש להציג בפני האדם ממנו נאסף המידע את הפרטים הבאים:

- המטרות שלשמן מבוקש המידע;
- למי יימסר המידע ומטרות המסירה;
- האם חלה על אותו אדם חובה חוקית למסור את המידע;
- סוגי המידע בהם עשוי להיעשות שימוש והמקור שלהם;
- תיאור של הסיכונים העשויים לנבוע מכל אחת ממטרות עיבוד המידע;
- אופן פעולת מערכת הבינה המלאכותית שתשמש לעיבוד המידע; ו-
- העובדה שהמידע נאסף באמצעות מערכת אוטומטית מבוססת בינה מלאכותית (בוט), ככל שעשויה להיות לכך השפעה מהותית על מתן ההסכמה.

אחריותיות (accountability)

לעמדת הרשות קיימת חשיבות מיוחדת ליישום פרקטיקות של אחריותיות בפיתוח ושימוש במערכות בינה מלאכותית. בין היתר, הרשות מציינת את האמצעים הבאים להגברת האחריותיות בתחום זה:

- **מינוי ממונה הגנת פרטיות (DPO)** – במסגרת תיקון 13, ארגונים רבים מחויבים [במינוי ממונה הגנת פרטיות](#), שישמש, בין היתר, סמכות מקצועית ומוקד ידע בתחום הגנת הפרטיות בארגון. לעמדת הרשות, ממונה הגנת הפרטיות עשוי להיות הגורם המתאים והמיומן ביותר לטיפול בסוגיות הנובעות משימוש במערכות בינה מלאכותית בארגון. כמו כן, הרשות מציינת כי חברות שמאמנות מודלים של בינה מלאכותית כפופות "בסבירות גבוהה" לדרישה למינוי ממונה הגנת פרטיות, בהתאם לחוק (כפי שתוקן בתיקון 13).
- **תסקיר השפעה על פרטיות (DPIA)** – תסקיר השפעה על פרטיות הוא תהליך מתודולוגי המנתח באופן מקיף ושיטתי את השפעת עיבוד המידע על הפרטיות של מי שהמידע על אודותיו נאסף או מוחזק, מזהה את

מכלול הסיכונים לפרטיות, בוחן חלופות ומציע דרכים לצמצם את אותם סיכונים. עמדת הרשות היא שעריכת תסקיר השפעה על הפרטיות, בטרם שימוש במערכות בינה מלאכותית לעיבוד מידע אישי, היא הדרך המיטבית המומלצת לוודא ולהוכיח כי השימוש במערכות אלו עומד בדרישות הגנת הפרטיות.

• **מדיניות לשימוש בכלים של בינה מלאכותית יוצרת (generative AI)** – בהתאם להנחיה, יש לאמץ מדיניות לצמצום הסיכונים לחשיפת מידע אישי הנובעים מהסתייעות בשירותים של בינה מלאכותית יוצרת, כגון ChatGPT, Gemini, Claude ו-CoPilot. על המדיניות להתייחס, בין השאר, לנושאים הבאים: מי בארגון רשאי להשתמש בכלים של בינה מלאכותית יוצרת; מי רשאי להתיר את השימוש; מהם הכלים המותרים לשימוש; אילו סוגי מידע מותר להזין לשירותים, צמצום משך השמירה של שאליות (prompts); הגבלת היכולת לעשות שימוש במידע המוזן לאימון האלגוריתם; והדרכת עובדים בעניין סיכוני האבטחה הייחודיים לשימוש במערכות אלו.

כריית מידע מהאינטרנט (scraping)

ההנחיה קובעת כי כריית מידע אישי מרשת האינטרנט (scraping) לצורך אימון מודלים של בינה מלאכותית, ללא הסכמה מדעת של נושאי המידע, מהווה פגיעה אסורה בפרטיות. לעמדת הרשות, גם כאשר אדם מפרסם מידע אודות עצמו (או אודות אחרים) ברשת חברתית, ככלל לא ניתן יהיה להסיק מכך הסכמה מדעת לעיבוד המידע אודותיו לאימון מערכות בינה מלאכותית.

בנוסף, לעמדת הרשות, מפעילים של פלטפורמות אינטרנטיות (כגון אפליקציות היכריות או רשתות חברתיות) נדרשים לנקוט אמצעים נאותים למנוע כריית מידע מהפלטפורמות שהם מנהלים, וכרייה ללא הסכמת מפעיל הפלטפורמה תהווה "אירוע אבטחה חמור" עליו יש לדווח לרשות להגנת הפרטיות.

זכויות נושאי מידע

החוק מעניק לכל אדם זכות לעיין במידע שמוחזק עליו בכל מאגר מידע, וזכות לתקן מידע שאינו נכון, שלם, ברור או מעודכן.

בהתאם להנחיה, לאור החשיבות המיוחדת של הדיוק והאמינות של המידע המעובד ומופק במערכות בינה מלאכותית, בכוונת הרשות לשים דגש על האכיפה של זכות העיין וזכות התיקון או המחיקה ביחס למערכות בינה מלאכותית. כמו כן, הרשות מבהירה בהנחיה כי במערכות בינה מלאכותית הזכות לבקש תיקון מידע שגוי עשויה לחייב גם תיקון של האלגוריתם שהפיק מידע כאמור.

צעדים פרקטיים ליישום ההנחיה

הנחיית הרשות משקפת מגמה של הגברת המעורבות של הרשות בהתוויית נורמות לאיסוף ועיבוד מידע במגזר הפרטי. לצד זאת, ההנחיה מצטרפת לחוקים והנחיות רגולטוריות במדינות נוספות לצמצום הסיכונים הנובעים משימוש במערכות בינה מלאכותית.

להלן צעדים עיקריים שניתן לנקוט ליישום ההנחיה:

1. **מיפוי השימושים בבינה מלאכותית בארגון:** זיהוי כל המערכות והתהליכים המשתמשים בבינה מלאכותית לעיבוד מידע אישי ובחינת מקורות המידע המשמשים לאימון מודלים.
2. **עדכון מסמכי פרטיות:** עדכון מדיניות הפרטיות והודעות פרטיות שנמסרות לנושאי מידע, כך שיכללו התייחסות

מפורשת לשימוש בבינה מלאכותית ולחובת הגילוי המוגברת שבאה לידי ביטוי בהנחיה. כמו כן, יש לבחון שילוב גילויים נוספים בקשר עם שימוש במערכות בינה מלאכותית בכלים שיש להם אינטראקציה ישירה עם נושא המידע (כגון צ'אטבוטים).

3. **ביצוע תסקיר השפעה על הפרטיות:** עריכת תסקיר לכל מערכת בינה מלאכותית המעבדת מידע אישי וזיהוי וטיפול בסיכונים לפרטיות העולים במסגרתו.

4. **גיבוש מדיניות לשימוש בשירותי בינה מלאכותית חיצוניים:** מדיניות זו תכלול, בין היתר, קביעת כללים ברורים לשימוש בשירותים כמו ChatGPT, הגדרת סוגי המידע שאסור להזין במערכות אלה והעברת הדרכת עובדים בנושא (ראו הפירוט לעיל בפרק אחריותיות). כמו כן, יש לבחון את תנאי השימוש ומדיניות הפרטיות של כלים אלה ואת השימושים שהשירות החיצוני עושה במידע המוזן (כגון, אימון מודלים).

5. **מינוי ממונה הגנת פרטיות (DPO):** חברות רבות מחויבות, במסגרת תיקון 13, במינוי ממונה הגנת פרטיות. אף בחברות שאינן כפופות לחובה זו, מינוי ממונה עשוי לתרום משמעותית לארגון בהטמעה של עקרונות ושיקולי פרטיות בתהליכי העבודה בארגון ובסיוע לארגון במימוש אחריותו וחובותיו לפי דיני הגנת הפרטיות, ומהווה פרקטיקה מומלצת מבחינת הרשות.

6. **scraping:** על חברות שפעילותן כוללת כריית מידע (scraping) לבחון את סוגי המידע הנאספים במסגרת זו ואת תנאי השימוש של הפלטפורמות מהן נאסף המידע, ולגבש מדיניות שתצמצם את הסיכונים המשפטיים בקשר עם פעילות זו.

לאור כניסתו הצפויה לתוקף של תיקון 13 לחוק הגנת הפרטיות באוגוסט 2025, וסמכויות האכיפה המורחבות שיוקנו לרשות להגנת הפרטיות במסגרתו, על חברות [לנודא בהקדם שהן מיישמות כראוי](#) את דרישות הגנת הפרטיות, גם בקשר עם השימוש במערכות בינה מלאכותית.

טיטוטת ההנחיה פתוחה להערות הציבור עד ליום 5 ביוני 2025.

אנו עומדים לרשותכם בכל שאלה.

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



אסף הראל
שותף