

הרשות להגנת הפרטיות: טיוטת הנחיה בנוגע לתחולת חוק הגנת הפרטיות על מערכות בינה מלאכותית

מזכר לקוחות - מאי 2025

לקוחות יקרים,

ביום 28 באפריל 2025 פרסמה הרשות להגנת הפרטיות טיוטת הנחיה אשר מטרתה להבהיר את תחולת חוק הגנת הפרטיות, התשמ"א-1981 על מערכות בינה מלאכותית (Artificial Intelligence).

טיוטת ההנחיה מבקשת לגבש סטנדרטים משפטיים בתחום מתפתח זה ולהציב ציפיות ברורות לפעילותם של ארגונים המפתחים, מאמנים או עושים שימוש במודלים מבוססי בינה מלאכותית המעבדים מידע אישי.

ראינו לנכון לסקור טיוטת הנחיה זו בתמצית הן משום שהאופן בו הרשות מגדירה בטייטה את יישום הוראות החוק והתקנות שמכוחו בכל שלבי מחזור החיים של מערכות בינה מלאכותית, צפוי לדעתנו להשפיע באופן נרחב על המשק והציבור, והן משום שהציבור מוזמן להעביר התייחסויות לטייטה עד ליום ה-5 ביוני 2025.

אתם מוזמנים להסתייע בנו בהעברת הערות לטייטה ובבחינת היערכות ארגונכם בנושא זה בהתאם להוראות הדין הקיים והצפוי לדעתנו.

להלן נסקור את עיקרי הטייטה.

1. בינה מלאכותית ותחולה.

1.1. בטייטת הנחיית הרשות להגנת הפרטיות ("הרשות") - תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית שפורסמה ביום 28 באפריל 2025 ("הטייטה"), הרשות מגדירה מערכת בינה מלאכותית כ- "מערכת ממוכנת אשר מסיקה מהקלט המוזן לה כיצד להפיק תחזיות, תוכן, המלצות או החלטות שיכולות להשפיע על הפרט או פעילותו של בעל השליטה או המחזיק במאגר, הפועלת ברמות משתנות של עצמאות והסתגלות".



סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

ירושלים
ישעיהו ליבוביץ 30, בניין 2
ט. 02-5607607
פ. 02-5639948

1.2. חוק הגנת הפרטיות, התשמ"א-1981 ("החוק") מאסדר עיבוד מידע אישי על גווניו,¹ ולכן מאירה הרשות

(א) ששימוש בבינה מלאכותית עשוי לטמון בחובו פעולות עיבוד מידע אישי לאורך כל ההליך העסקי ולאורך כל חיי המערכת. ביחס לתוכן המוזן למערכת (קלט) – משלב לימוד/אימון המודל, השימוש בו, וביחס לתוכן הנוצר ע"י המערכת (פלט) – מערכות בינה מלאכותית מייצרות פלט שייתכן שיעלה כדי מידע אישי;²

(ב) התחולה היא ביחס לעיבוד מידע אישי בין אם נעשה בכוונה או בשגגה.

אמירות אלה מצביעות לדעתנו על הצורך לקיים הליכים מוקפדים שחלקם ניתן אף ליישם באמצעות עזרים טכנולוגיים, שיקבעו באילו תחומים נעשה שימוש במערכות בינה מלאכותית, אילו נתונים מונגשים למערכות אלה, מה פעולות העיבוד המותרות, ומה נעשה בתוצריהן (במיוחד ככל שהם עולים כדי מידע אישי).

2. בסיס חוקי לעיבוד מידע.

2.1. הרשות מבהירה כי בכל אחד משלבי מחזור החיים של מערכת הבינה המלאכותית – לרבות איסוף, אחסון, אימון ושימוש בפועל – יש לוודא קיומו של בסיס משפטי כדין לעיבוד מידע אישי. זאת כאשר, במקרים מסוימים הסכמה מכללא בלבד, עלולה להיתפס כהיעדר הסכמה וכהיעדר בסיס משפטי מתאים לדעת הרשות.³

2.2. כך למשל רשויות המדינה צריכות לוודא שקיימת להן הסכמה בחוק לקיים את הפגיעה בפרטיות ולוודא שהן עומדות בדרישות המידתיות. כך גם מעסיקים הנדרשים אף הם לעמוד בדרישות המידתיות בעת פגיעה בפרטיות.

¹ לצורך מסמך זה נתייחס ל-"מידע אישי" כ-מידע אישי כהגדרתו בתיקון 13 לחוק הגנת הפרטיות ("תיקון 13"), "עניינו הפרטיים של אדם" ו-"מידע" כהגדרתו בחוק.

² כך גם לפי דוח הביניים של הצוות הבינמשרדי בנושא "בינה מלאכותית בסקטור הפיננסי" (נובמבר 2024) שם הדגיש הצוות כי "אין בעינינו ספק כי תוצרי מערכות הבינה המלאכותית – תחזיות, היסקים, הערכות, סיווגים שנעשים לגבי אדם ספציפי הם מידע אישי הזוכה להגנת דיני הגנת הפרטיות".

³ ראו גם את טיוטת הרשות בנושא הסכמה בדיני הגנת הפרטיות. מזכרנו זמין [באן](#).



3. הסכמה מדעת ושקיפות.

3.1. סעיף 1 לחוק קובע כי אין לפגוע בפרטיותו של אדם ללא הסכמתו, ובסעיף 3 מודגש שהסכמתו של אדם צריכה להיות "הסכמה מדעת".⁴ לפי הרשות, הסכמה כאמור צריכה להיות הסכמה המבוססת על מידע מלא, ברור ורלוונטי שנמסר מראש, ובאופן שמאפשר לנושא המידע להבין את משמעות השימוש הצפוי במידע אודותיו.

3.2. בנוסף, סעיף 11 לחוק קובע כי פנייה לאדם לצורך איסוף מידע אודותיו תלווה בהודעה הכוללת את: המטרה לשמה מבוקש המידע, זהות הגורמים להם יימסר המידע, מטרות המסירה, והאם קיימת חובה חוקית למסור את המידע.

3.3. לצד הדרישות הבסיסיות, הרשות גורסת שבמצבים בהם מעובד מידע אישי באמצעות מערכות בינה מלאכותית יש להדגיש בפני נושאי המידע מאפיינים ייחודיים לעולמות הבינה המלאכותית דוגמת:

(א) **שקיפות לגבי אופן פעולת המערכת.** יש לספק הסבר על אופן פעולת המערכת בעיבוד מידע אישי, ברמת פירוט שתאפשר גיבוש הסכמה מדעת ובשים לב למגבלות טכנולוגיות.

(ב) **גילוי לגבי אינטראקציה מול מערכת.** אם האינטראקציה עם נושא המידע מתבצעת מול "בוט" ולא בן אנוש, יש ליידע אותו על כך, ככל שעובדה זו עשויה להשפיע על מתן ההסכמה.

(ג) **פירוט סוגי המידע ומקורותיו.** יש לפרט אילו סוגי מידע ישמשו את המערכת ומהם מקורות המידע.

(ד) **פירוט לגבי כל מטרת שימוש.** יש להתייחס לכל אחת ממטרות השימוש במידע והסיכונים האפשריים הכרוכים בה, כולל שימוש לאימון האלגוריתם.

(ה) **הסכמה מפורשת למטרות מורכבות.** ככל שמטרות השימוש מורכבות יותר או חורגות מציפייתו הסבירה של נושא המידע, נדרשת הסכמה מפורשת יותר. כלומר, תוכן ההסבר הנוגע למטרות יידרש להיות מפורט ובהיר יותר, והאינדיקציה לרצונו של נושא המידע

⁴ ראו גם את מזכרנו בדבר עמדת הרשות בנושא חובת יידוע במסגרת איסוף ושימוש במידע אישי, [כאן](#).



ולמודעותו למטרת העיבוד ולהשלכותיו תהיה מפורשת יותר (כגון בהסכמה נפרדת במתכונת של opt-in).

בהתאם, ארגונים יידרשו לבחון את מנגנוני היידוע וההסכמה הקיימים ברשותם, ולעדכןם כך שיתאימו למורכבות ולסיכונים הייחודיים שמזמנות מערכות בינה מלאכותית בהן הם מבקשים לעשות שימוש.

4. כריית מידע מהרשת (Scraping).

4.1. עמדת הרשות היא שכריית מידע אישי מרשת האינטרנט לצורך עיבודו במערכת בינה מלאכותית, לרבות למטרת אימון האלגוריתם, כרוכה בפגיעה אסורה בפרטיות, כאשר לא ניתנה לכך הסכמה מדעת של נושא המידע.

4.2. לפי הרשות, פרסום מידע על אדם לא בהכרח מלמד על הסכמה מדעת לעיבוד המידע לצורך אימון או שימוש במערכות מורכבות לגביהן קיים חוסר ודאות גדול בדבר התכליות להן ישמשו וההשלכות והסיכונים הכרוכים בהן. באופן דומה, לא ניתן יהיה להסיק מפרסום כאמור כי אדם הסכים שהמידע אודותיו ישמש לאימון או למערכת בינה מלאכותית היוצרת סיכון גבוה במיוחד לפרטיות.

4.3. כאן רצוי להדגיש לדעתנו שכריית מידע אישי בניגוד לתנאי שימוש וללא הסכמת נושא המידע, תיחשב כהפרה לכאורה של האיסור על עיבוד מידע ממאגר ללא הרשאת בעל השליטה במאגר, לפי סעיף 8(ג) לתיקון 13,⁵ ועלולה אף להיחשב עבירה פלילית לפי סעיף 23נה לתיקון 13.

גורמים המבקשים לאמן מערכות בינה מלאכותית באמצעות מידע הזמין באינטרנט (גם אם באופן "פומבי") יידרשו להביא עמדה זו בחשבון אם הטיוטה תהפוך לעמדת רשות. למעשה, כל מי שמפעיל אתר אינטרנט יידרש לדעתו להביא אמירה זו בחשבון במסגרת תנאי השימוש שלו בין אם כדי לאפשר שימוש במידע המוצג בו ובין אם לאו.

4.4. באמירה חריגה של הרשות בטיוטה, נקבע כי על בעלי שליטה במאגרי מידע המאפשרים פרסום ושיתוף פומבי של מידע אישי (כגון רשתות חברתיות, אתרי סחר והיכרויות) חלה חובה לנקוט באמצעים אפקטיביים למניעת כריית מידע אסורה מהפלטפורמות שבשליטתם בהתאם לתקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017 ("תקנות אבטחת מידע"), וכי כריית מידע

⁵ מזכרנו ביחס לתיקון 13 לחוק הגנת הפרטיות, זמין כאן.



אסורה עשויה להיחשב "אירוע אבטחה חמור" כהגדרתו בתקנות האמורות, ולהצמיח חובת דיווח מידית לרשות לפי תקנה 11(ד) לתקנות אבטחת מידע.

5. אחריותיות (accountability).

5.1. אחריותיות בתחום הגנת המידע האישי מהווה, בין היתר, עיקרון המחייב את הארגון לוודא עמידה בהוראות הדין וליישם מנגנוני בקרה שיאפשרו לו להוכיח את עמידתו בהן. עיקרון זה מקבל משנה חשיבות לדעת הרשות בעולמות הבינה המלאכותית, בשל הפוטנציאל הרב לסיכון לפרטיות, ובמיוחד בשל הקושי המובנה לזהות מבעוד מועד את הסיכונים העתידיים העלולים לבוע מעיבוד מידע אישי באמצעותן בשל האוטונומיה של מערכות אלה ואי-הוודאות הכרוכה בתפקודן.

5.2. הרשות מדגישה מספר פרקטיקות מרכזיות שיש להקפיד עליהן כדי לעמוד בעיקרון האחריותיות:

(א) **מינוי ממונה על הגנת הפרטיות (DPO).** תיקון 13 לחוק כבר קובע חובה מפורשת למינוי DPO בגופים ציבוריים ובחלק מהגופים במגזר הפרטי (למשל כאשר פעילותיהם כוללת עיבוד נרחב של מידע בעל רגישות מיוחדת). לדעת הרשות, אימון מודלים באמצעות עיבוד מידע אישי מגדיל את הסבירות להתקיימות התנאים המקימים חובת מינוי ממונה הגנת פרטיות⁶.

בטיטה הרשות מציגה עמדה לפיה, במקרים רבים, ממונה הגנת הפרטיות עשוי להיות גם הגורם המתאים והמיומן ביותר ליטול על עצמו את המשימה לתכלול גם את הטיפול בסוגיות הנובעות משימוש במערכות בינה מלאכותית בארגון, לפחות כל עוד לא מונה בארגון בעל תפקיד ייעודי.

(ב) **ביצוע תסקיר השפעה על פרטיות (Privacy Impact Assessment).** התסקיר הוא כלי מתודולוגי חשוב שמטרתו להעריך מראש את הסיכונים לפרטיות בעיבוד המידע, לזהות חלופות עם פגיעה פחותה, ולהציע אמצעים למזעור נזק. הרשות ממליצה לערוך תסקיר כאמצעי ניהולי חיוני בכל מקרה של שימוש בבינה מלאכותית, ובפרט כאשר מדובר במערכות מורכבות, או במצבים בהם עולות שאלות של מידתיות, הסכמה או קבלת החלטות אוטומטיות.

⁶ מזכרנו ביחס להמלצות הרשות בנוגע לממונה הגנת פרטיות בארגונים זמין [בא.י](#).



הרשות בדעה שעבור רשויות ציבוריות ובעלי מאגרים אחרים הכפופים לדרישת המידתיות (כגון בעת עיבוד מידע אישי במסגרת יחסי עבודה או ככל שיש רצון להסתמך על הגנות סעיף 18 לחוק), תסקיר הוא הכלי המיטבי והמומלץ לוודא ולהוכיח כי קיים קשר רציונלי בין הפגיעה בפרטיות בשימוש בבינה מלאכותית לבין השגת המטרה, כי לא קיימת חלופה שפגיעתה בפרטיות פחותה, וכי התועלת הצפויה מן השימוש במערכת עולה על הפגיעה הצפויה בפרטיותם של נושאי המידע. כן גורסת הרשות שתסקיר יאפשר תיעוד מיטבי במסמך הגדרות המאגר ביחס לסיכונים הנובעים ממערכות בינה מלאכותית ביחס למאגר.

(ג) **חיזוק ממשל תאגידי בתחום הפרטיות.** לצד מנגנוני הפעלה יומיומיים, הרשות רואה בהנהלת החברה ובדירקטוריון שחקנים קריטיים בניהול הפרטיות. הרשות מזכירה בהקשר זה את הנחיה 1/2024 לפיה על חברות שהמידע האישי נמצא בליבת פעילותן או היוצרות סיכון גבוה לפרטיות – לוודא קיומה של מדיניות סדורה, מנגנוני פיקוח פנימיים, חלוקת אחריות ברורה ודיווח תקופתי להנהלה.⁷

(ד) **פעולה לפי עקרונות עיצוב לפרטיות וכברירת מחדל (privacy by design and by default).** במסגרת הטיוטה וכן מסמכים האחרים, לפי הרשות על ממונה הגנת הפרטיות להיות מעורב בעיצוב מערכות המידע של הארגון ובתהליכים הקשורים בהן, על מנת לוודא, ככל הניתן מראש, כי מערכות המידע בנויות באופן שיפחית את הסיכון לפגיעה בפרטיותם של נושאי המידע.⁸

6. עיון ותיקון מידע אישי.

6.1. בהתאם לסעיפים 13–14 לחוק, לאדם נתונה הזכות לעיין במידע אודותיו וככל שמצא כי המידע לגביו אינו נכון, שלם, ברור או מעודכן, יכול האדם לפנות לבעל השליטה במאגר המידע בבקשה לתקן את המידע או למחקו.

דעתנו היא שזכות העיון תהפוך להיות חלק משמעותי מאוד בבקרה על תוכן המערכת שיווצר בשל שימוש בבינה מלאכותית וארגונים יידרשו לאמץ מנגנונים וטכנולוגיות שיאפשרו זכות עיון זו. עמדת

⁷ ראו מזכרנו בדבר הנחיית הרשות להגנת הפרטיות מס': 1/2024 תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע) - [באן](#).

⁸ ראו מזכרנו בדבר מינוי ממונה על הגנת הפרטיות בחברות ובארגונים - [באן](#).



הרשות בטיטה היא שהזכות לבקש תיקון מידע עשויה בנסיבות מסוימות ובהתאם להקשר להתייחס גם לתיקון האלגוריתם שהפיק את המידע – במקרים שבהם אלגוריתם חוזר ומייצר תוצאה שגויה לגבי אדם, ואין דרך אחרת למנוע זאת.

6.2. כאשר מדובר במידע אישי שמקורו באזור הכלכלי האירופי או במידע שמידע כאמור משולב בו, חלה חובה יזומה על הארגון להבטיח את תקינותו ועדכניותו של המידע.⁹ חובה זו כוללת גם הטמעה של מנגנונים למניעת עיוותים באימון או בהסקת מסקנות על ידי המערכת, באמצעות בקורות איכות, הסברתיות אלגוריתמית ושמירה על רלוונטיות המידע.

הרשות מציינת שבכוונתה לשים דגש על האכיפה של סעיפים 13 ו-14 לחוק ושל תקנה 5 לתקנות מידע מהאזור הכלכלי האירופי ביחס למערכות בינה מלאכותית.

7. **אבטחת מידע.** השימוש במערכות בינה מלאכותית מעורר סיכונים אבטחת מידע ייחודיים המחייבים התייחסות רגולטורית, תפעולית וטכנולוגית מוגברת בהתאם לסעיף 17 לחוק ובתקנות אבטחת המידע.

7.1. שימוש בסמכות לבחינת רמת אבטחה. הרשות מציינת שהיא עשויה לעשות שימוש בסמכותה בתקנה 20(א) (1) לתקנות אבטחת מידע ולבחון החלה יזומה של רמת אבטחה גבוהה במאגרים בהם נעשה שימוש במודלים בעלי פוטנציאל סיכון גבוה. כך שייתכן שמאגרים שיעשו שימוש במערכות בינה מלאכותית מסוימות יידרשו לרמת אבטחה גבוהה יותר בשל עצם השימוש במערכת מבוססת בינה מלאכותית בעלת פוטנציאל סיכון גבוה, שיעלה את רמת האבטחה לה יהיה כפוף המאגר לפי תקנות אבטחת מידע.

7.2. סיכונים ייחודיים. מערכות בינה מלאכותית חשופות לסיכונים ייחודיים, דוגמת מתקפות הסקה (המאפשרות לחלץ מידע אישי לפי מבנה שאילתות / תוכן משתמש שמוגש להן), הרעלת מידע ועוד. תקנות אבטחת המידע מחייבות התייחסות ישירה לסיכונים אלה במסגרת מסמך הגדרות המאגר, סקרי סיכונים, מבדקי חדירות והטמעה של אמצעי אבטחה הולמים. כן נדרש ניטור מערכות בינה מלאכותית אלה ודיווח על אירועי אבטחה לרשות.

⁹ תקנה 5(א) לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי) התשפ"ג-2023.



7.3. עיקרון צמצום המידע. יש לבחון אחת לשנה אם נשמר מידע עודף או שאינו נדרש עוד למטרות המאגר (תקנה 2(ג)). עיקרון זה חשוב במיוחד במאגרים המאומנים באמצעות כמויות מידע אישי גדולות. הטיוטה מבירה כי יש לתת דגש מיוחד לעקרון זה כדי למזער את הסיכונים הייחודיים.

8. שימוש בעובדים ובספקים חיצוניים. השימוש ההולך וגובר במערכות בינה מלאכותית יוצרת מחייב גיבוש מדיניות ארגונית ויעודית. בין היתר: הגדרה ברורה של אילו שירותים מותרים לשימוש ובאילו תנאים; קביעת גבולות לחשיפת מידע אישי בשאלות; הקפדה על עמידה בהוראות תקנה 15 לתקנות אבטחת מידע ביחס להתקשרויות עם צדדים שלישיים; צמצום משך שמירת שאלות והגבלת השימוש בהן לאימון האלגוריתם; הדרכת עובדים בנוגע לסיכונים ואופן השימוש הבטוח.

9. רישום מאגרי מידע

9.1. החזקה או ניהול של מאגר מידע אישי מחייבים רישום בפנקס המאגרים בנסיבות מסוימות.

9.2. במסגרת בקשת רישום המאגר, יש להצהיר במפורש על מטרת השימוש במידע, ולוודא שהיא תואמת את שלב הפעילות – אימון או יישום. בנוסף, יש לוודא כי המידע שייאסף ויעובד הוא רק המידע המינימאלי הדרוש למימוש מטרה זו.

9.3. עקרונות אלה חלים גם על ניסוח מטרות המאגר במסגרת מסמך הגדרות המאגר. אותו יש לנהל ביחס לכל מאגר מידע ללא קשר לחובת הרישום של המאגר.

9.4. במסגרת מסמכי הגדרות המאגר, הרשות מצפה שינתן ביטוי מדויק לשימוש במערכות בינה מלאכותית בהיבטים שונים. בין אם הם מוגשים לה ובין אם לאו.

טיוטת ההנחיה פורסמה להערות הציבור והיא צפויה להוביל בהמשך לגיבוש הנחיה מחייבת. יישום עקרונות ההנחיה עשוי לחייב עדכון של מסמכי מדיניות ונהלים קיימים, נהלי עבודה מול ספקים, הסכמות משתמשים, והטמעת כלים לניהול מאגרי מידע ואבטחתם. אתם מוזמנים להסתייע בנו בבחינת כל אלה ובייעוץ כללי הקשור לנושאים שסקרנו במזכר זה.

נציין כי המידע האמור לעיל הוא מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי, ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים שנסקרו לעיל.



סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

באר שבע
גב ים, רחוב האנגריה 77
ט. 03-6071450
פ. 08-6155780

תל אביב
מגדל אלקטרה, ינאל אלון 98
ט. 03-6078607
פ. 03-6078666

ירושלים
ישעיהו ליבוביץ 30, בניין 2
ט. 02-5607607
פ. 02-5639948



עו"ד סער רוסמן, שותף
מחלקת הייטק, טכנולוגיה והון סיכון
ראש תחום סייבר ופרטיות
Saar@agmon-law.co.il



עו"ד אסנת סרוסי פירסטטר, שותפה
ראש מחלקת הייטק, טכנולוגיה והון
סיכון (משותפת)
Osnat@agmon-law.co.il



עו"ד מתן אברמוביץ
מחלקת הייטק, טכנולוגיה והון סיכון
Matana@agmon-law.co.il



עו"ד מרים שדה-פישר
מחלקת הייטק, טכנולוגיה והון סיכון
Miriamf@agmon-law.co.il



סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

ירושלים
ישעיהו ליבוביץ 30, בניין 2
ט. 02-5607607
פ. 02-5639948