

מדיניות הגנת הפרטיות והסכם עיבוד מידע (DPA) בפלטפורמה הדיגיטלית לניתוח מסמכים רפואיים (SaaS AI)

תאריך עדכון אחרון: אוגוסט 2026

בעלת התוכנה, חברת **טל אינוביישן בע"מ, ח.פ. 517364709** (להלן: "**החברה**" או "**אנו**") מייחסת חשיבות עליונה להגנה על הפרטיות, סודיות המידע ואבטחת הנתונים האישיים והרגישים המעובדים במסגרת הפלטפורמה הדיגיטלית לניתוח מסמכים רפואיים מבוססת בינה מלאכותית (להלן: "**הפלטפורמה**" או "**התוכנה**").

1. כללי

1.1. מדיניות פרטיות זו (להלן: "**המדיניות**") מפרטת את אופן איסוף המידע, עיבודו, שמירתו ואבטחתו בפלטפורמה, ומסדירה את מערכת היחסים המשפטית והטכנולוגית שבין החברה לבין המשתמשים בפלטפורמה (להלן: "**הלקוח**" או "**המשתמש**").

1.2. המדיניות מנוסחת בלשון זכר מטעמי נוחות בלבד, אך היא פונה ומיועדת לכלל המגדרים כאחד.

1.3. המדיניות מנוסחת בהתאמה להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן – "**חוק הגנת הפרטיות**"), תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן – "**תקנות אבטחת מידע**"), וכן בזיקה לעקרונות הכלליים של תקנות הגנת הנתונים הכלליות והנחיות הרשות להגנת הפרטיות בישראל.

1.4. יוקדם ויודגש כי התוכנה והשירותים מוצעים לקהל מקצועי של עורכי דין ומשרדיהם ואינה מותאמת לקהלים אחרים.

1.5. במסגרת פעילות הפלטפורמה ככלי עזר טכנולוגי החברה מדגישה כי האחריות על השימוש בתוכנה ובשירותיה הם כדלקמן:

1.5.1. הלקוח כ"בעל השליטה" (Data Controller):

1.5.1.1. הלקוח, עורך הדין, המעלה את מסמכיו הרפואיים והאישיים של לקוח הקצה (להלן: "**הניזוק**" או "**נושא המידע**") הוא בעל השליטה החוקי הבלעדי במאגר המידע.

1.5.1.2. עורך הדין קובע את מטרות העיבוד, סוגי המסמכים המועלים, הרשאות הגישה בתוך המשרד, וזמני מחיקת המידע מהמערכת והתוכנה.

1.5.2. החברה כ"מעבד המידע" (Data Processor):

1.5.2.1. החברה פועלת כמעבדת מידע בלבד עבור משרד עורכי הדין.

1.5.2.2. החברה מעבדת את המידע הרפואי והרגיש אך ורק בהתאם להנחיותיו הטכניות הישירות של הלקוח, כפי שהן מתבטאות בפעולותיו האקטיביות בפלטפורמה.

1.5.2.3. החברה אינה עושה כל שימוש עצמאי, מסחרי או פרסומי במידע של הניזוקים.

2. חובות אתיות מיוחדות של עורכי הדין (החלטת לשכת עורכי הדין את/60/24)

2.1. השימוש בפלטפורמה מיועד לעורכי דין הנדרשים לעמוד בדרישות האתיקה המקצועית החלות עליהם.

2.2. החברה מפנה את המשתמשים לגילוי הדעת המקדים של ועדת האתיקה הארצית של לשכת עורכי הדין בישראל בעניין שימוש בבינה מלאכותית (החלטה את/60/24) ובפרט אחריותם כדלקמן:

2.2.1. חובת השגת הסכמה מדעת בכתב מהניזוק:

2.2.1.1. באחריותו המקצועית, המשפטית והבלעדית של הלקוח (משרד עורכי הדין) לוודא כי השיג

מראש, בכתב ובאופן מפורש, את הסכמתו של הניזוק (או אפוטרופוסו החוקי, במקרה של

קטין או חסר ישע) להעלאת מסמכיו הרפואיים, הפיננסיים והאישיים הרגישים לצורך אחסון ועיבוד בענן ושימוש בכלי בינה מלאכותית (AI) כדוגמת הפלטפורמה.

2.2.1.2. בהתאם להמלצות ועדת האתיקה של לשכת עורכי הדין, הסכמה זו דורשת התייחסות לסוג המסמכים הספציפי ולאמצעי ההגנה הננקטים ביחס אליהם, ועל הלקוח לעגן אותה בהסכם שכר הטרחה או בנספח הסכמה ייעודי.

2.3. אחריות המשתמשים למסמכים ולעיבודם:

- 2.3.1. הלקוח נושא באחריות המלאה והבלעדית לתוכן המסמכים והקבצים שהוא בוחר להעלות לסביבת העבודה שלו בפלטפורמה.
- 2.3.2. החברה אינה מפקחת, אינה בוחנת ואינה מסננת את המסמכים המועלים, ואינה נושאת באחריות כלשהי לחוקיותם, דיוקם או אמיתותם של הנתונים הכלולים בהם.
- 2.3.3. הלקוח מתחייב לוודא כי העלאת המסמכים אינה מפרה זכויות של צדדים שלישיים, הוראות חיסיון חקוקות או צווי איסור פרסום שיפוטיים.

2.4. חובת אימות התוצרים ובקרת איכות אנושית:

- 2.4.1. תוצרי הפלטפורמה (צירי זמן, טבלאות נכות, פתולוגיות וכו') מופקים באמצעות כלי בינה מלאכותית ומשמשים ככלי עזר מסייע בלבד למשתמש.
- 2.4.2. בהתאם לחובותיו המקצועיות של עורך הדין, עליו לבחון באופן קפדני ואנושי את כל תוצרי המערכת, לאמת את דיוקם ולהצליבם מול מסמכי המקור טרם הצגתם, הגשתם או הסתמכות עליהם בכל פורום משפטי או רפואי.

2.5. חיסיון עורך-דין-לקוח:

- 2.5.1. התוכנה מתוכננת לשמש כסביבת עבודה מאובטחת המשמרת ומגנה על חיסיון עורך-דין-לקוח (לפי סעיף 90 לחוק לשכת עורכי הדין, התשמ"א-1961).
- 2.5.2. החברה מתחייבת שלא לעשות כל שימוש במידע החסוי המועלה לפלטפורמה, למעט עיבודו הטכנולוגי הזמני והחולף לצורך אספקת השירותים ללקוח עצמו.

3. פירוט המידע שנשמר בידי החברה וצורכי איסופו

המידע המעובד והנשמר במערכות החברה נחלק לשתי קטגוריות ראשיות על פי אופן איסופו: מידע שנאסף באופן אוטומטי בעת השימוש בפלטפורמה, ומידע שנאסף כתוצאה מפעולות אקטיביות ויזומות של המשתמשים.

3.1. מידע הנאסף באופן אוטומטי (מטא-נתונים ויומני מערכת)

בעת הגלישה, החיבור והשימוש בפלטפורמה, מערכות הניטור והאבטחה של החברה אוספות ומתעדות נתונים טכניים מסוימים באופן אוטומטי:

3.1.1. פירוט המידע שנאסף:

- 3.1.1.1. כתובות IP של המשתמשים.
- 3.1.1.2. מזהי מכשיר קצה, סוג מערכת ההפעלה וסוג דפדפן האינטרנט.
- 3.1.1.3. מועדי כניסה ויציאה מהמערכת, משך פעילות ואירועי מערכת.

3.1.1.4. יומני פעילות פנימיים המתעדים פעולות בתיקים כגון: העלאת מסמך, מחיקת מסמך, הפעלת מנגנון סריקת המסמכים, יצירת אנליזה, עריכת נתונים, צפייה במסמך ויצוא קבצים.

3.1.1.5. נתוני גלישה ושימוש כלליים באמצעות קבצי עוגיות (Cookies) חיוניות.

3.1.2. צורכי איסוף המידע:

3.1.2.1. עמידה בדרישות אבטחת מידע סטטוטוריות: תיעוד יומני הפעילות ושמירתם למשך 24 חודשים לפחות מהווה חובה חוקית קשיחה לעמידה בדרישות "רמת אבטחה גבוהה" לפי תקנות אבטחת המידע הישראליות, לצורך ניטור, בקרה, מניעה ותחקור של אירועי אבטחה וגישה בלתי מורשית למידע.

3.1.2.2. הגנה על המידע הרפואי ומניעת זליגה: אימות ואבטחת החשבונות ומניעת התחזות.

3.1.2.3. אכיפת רישוי מסחרי ומניעת שימוש לרעה: זיהוי והצלבה של כתובות IP ומזהי מכשירים משמשים לצורך ניהול עמדות הגישה של הלקוח, אכיפת מגבלת המכשירים המותרים לכל עמדה, ומניעה של שיתוף סיסמאות ופרטי גישה עם גורמים בלתי מורשים מחוץ למשרד.

3.1.2.4. שיפור טכנולוגי וייעול המערכת: ניתוח ביצועים אנונימי וסטטיסטי של זמני תגובה, תקלות תוכנה ויציבות ממשק המשתמש.

3.2. מידע הנאסף כתוצאה מפעולות יזומות של המשתמשים

מידע זה כולל נתונים שהמשתמשים מזינים או מעלים באופן אקטיבי ומרצונם החופשי לצורך הקמת החשבון ושימוש בכלי האנליזה של הפלטפורמה:

3.2.1. פרטי משתמשים, מנהלה וחיוב (עורכי הדין וצוות המשרד)

3.2.2. פירוט המידע שנאסף:

3.2.2.1. שם מלא של עורך הדין / משתמשי הקצה במשרד.

3.2.2.2. שם משרד עורכי הדין או הישות המשפטית המפעילה את המנוי.

3.2.2.3. כתובת דואר אלקטרוני משרדית ומספרי טלפון נייד לאימות.

3.2.2.4. פרטי אמצעי תשלום וחיוב (המעובדים בצורה מוצפנת ומאובטחת דרך ספק סליקה חיצוני ללא שמירת פרטי כרטיס האשראי המלאים במערכות החברה).

3.2.3. צורכי איסוף המידע:

3.2.3.1. הקמת חשבון המשתמש וסביבת העבודה הייעודית של המשרד.

3.2.3.2. ניהול מחזור החיים של המנוי, ביצוע חיובים תקופתיים, הפקת חשבוניות מס וקבלות כחוק, וטיפול בבקשות שירות וביטולים.

3.2.3.3. אימות זהות אקטיבי ודו-שלבי בכל כניסה למערכת לשם הגנה על פרטיות המידע.

3.2.3.4. יצירת קשר, מתן תמיכה טכנית ומתן מענה לפניות משתמשי הקצה.

3.3. תוכן סביבת העבודה (לקוחות קצה / ניזוקים)

3.3.1. פירוט המידע שנאסף ונשמר:

- 3.3.1.1. נתוני זיהוי בסיסיים של הניזוקים כפי שמועלים על ידי עורך הדין (שם מלא, מספר תעודת זהות, תאריך לידה, מגדר, גיל).
- 3.3.1.2. מסמכים רפואיים, חוות דעת, סיכומי מחלה, רשומות רפואיות, תוצאות בדיקות, מסמכי השתכרות ופיצויים, וכל נתון רגיש אחר שהלקוח בוחר להעלות לסלוטים של התיקים השונים.
- 3.3.1.3. תוצרי האנליזה המופקים על ידי המערכת (צירי זמן דיגיטליים, טבלאות נכות מסכמות, הצעות לשאלות חקירה וכו').

3.3.2. צרכי איסוף המידע:

- 3.3.2.1. מתן השירות הטכנולוגי העיקרי של הפלטפורמה: עיבוד הקבצים (OCR), חילוץ פתולוגיות מובנה, תרגום מסמכים, ניתוח נתונים משפטי-רפואי אלגוריתמי והפקת דוחות עזר.
- 3.3.2.2. אחסון זמני ומאובטח בענן של התיק המשפטי-רפואי, המאפשר למשרד עורכי הדין לשלוף את הנתונים, לערוך אותם, לייצאם או למחוק אותם בשירות עצמי (Self-Service) בכל עת.
- 3.3.2.3. שמירת המידע בסביבה מבודדת ומוצפנת קצה-לקצה לצורך הגנה קפדנית על סודיות הלקוחות.

4. מעבדי משנה מורשים, אבטחת בינה מלאכותית והסכמי DPA

- 4.1. לצורך הפעלת התשתית הטכנולוגית, החברה נעזרת במעבדי משנה.
- 4.2. כל העברת מידע למעבדי המשנה מוסדרת במסגרת הסכמי עיבוד מידע (Data - DPAs Processing Agreements) המבטיחים עמידה שלהם בתנאים נאותים של אבטחה והגנת פרטיות:
- 4.2.1. תשתית בסיס הנתונים ואחסון הענן (Supabase / AWS):
- 4.2.1.1. כלל מסמכי המקור הרפואיים, שכבות הטקסט והאנליזות המופקות מאוחסנים על גבי שרתי ענן מאובטחים.
- 4.2.1.2. המידע מוצפן באופן מלא הן במעבר המידע והן בהצגתו ושמירתו.
- 4.2.2. עיבוד השפה והבינה המלאכותית (OpenAI API Enterprise):
- 4.2.2.1. חילוץ המידע, תרגום מסמכים, יצירת צירי זמן וניתוח הנתונים מבוצעים באמצעות ממשק בינה מלאכותית של חברת OpenAI.
- 4.2.2.2. המידע הרפואי, האישי והרגיש המועבר לעיבוד שפתי אינו משמש, אינו נשמר ואינו מאומן לצורך שיפור או למידה של מודלי השפה הציבוריים של OpenAI. העיבוד מבוצע בצורה חולפת, וכל שכבת מידע המועברת לצורך הניתוח נמחקת משרתי העיבוד של OpenAI מיד עם השלמת המשימה.

5. אמצעי אבטחת מידע פיזיים ולוגיים

- החברה מיישמת רמת אבטחה קפדנית העונה על דרישות "רמת האבטחה הגבוהה" על פי תקנות אבטחת המידע הישראליות:
- 5.1. תקשורת מוצפנת: כל תקשורת בין המשתמש לפלטפורמה ובין הפלטפורמה למעבדי המשנה מבוצעת אך ורק דרך תקשורת מאובטחת ומוצפנת.

- 5.2. **אימות דו-שלבי:** כניסה לסביבת העבודה מותנית בהזנת שם משתמש, סיסמה מורכבת ומעבר הליך אימות דו-שלבי חובה מבוסס אפליקציית אימות (Authenticator App) או קוד חד-פעמי (OTP).
- 5.3. **מנגנון ניתוק אוטומטי:** המערכת מבצעת ניתוק לוגי כפוי וסגירת חיבור של משתמש לאחר 15 דקות ללא פעילות אקטיבית בממשק.
- 5.4. **ניהול הרשאות:** מנהל משרד עורכי הדין ("משתמש האב") שולט באופן מלא על הרשאות הגישה של עובדי המשרד ("משתמשי קצה") לתיקים השונים, ויכול לחסום גישה באופן מיידי.
- 5.5. **יומני אבטחה ובקרה:** רישום ותיעוד מלא של כל חיבור, ניסיון כניסה ופעולה בתיקים, לצורך איתור ותחקור חריגות.

6. מנגנון מחיקה לצמיתות ושמירת מידע

- 6.1. **מחיקת תוכן סביבת העבודה ביוזמת הלקוח:**
- 6.1.1. המערכת פועלת במודל "שירות עצמי". כאשר הלקוח מוחק קובץ, תיק או נשוא מידע מסביבת העבודה שלו, פקודת המחיקה מיושמת באופן מיידי וסופי במערכות הייצור ובבסיסי הנתונים הפעילים של החברה ובמערכות מעבדי המשנה.
- 6.1.2. מידע שנמחק בדרך זו נמחק פיזית לצמיתות ולא ניתן לשחזור.
- 6.2. **שמירה מנהלתית וסטטוטורית:**
- 6.2.1. פרטי חשבון המנהלה, פרטי ההתקשרות של עורכי הדין והיסטוריית החיובים יישמרו במערכות החברה כל עוד המנוי פעיל, ולמשך תקופה של עד 7 שנים מסגירת המנוי – וזאת לצורכי דיווח חשבונאי, עמידה בחוקי מס, התגוננות משפטית, ופתרון מחלוקות.
- 6.2.2. יומני אבטחה ובקרה יישמרו למשך 24 חודשים ממועד רישום הפעולה לצורך עמידה בתקנות אבטחת מידע, ולאחר מכן יימחקו או יעברו אנונימיזציה מלאה.

7. זכויות המשתמשים ונושאי המידע (הניזוקים)

- 7.1. **זכות העיון והתיקון (סעיפים 13 ו-14 לחוק הגנת הפרטיות):**
- כל משתמש ונושא מידע (ניזוק) זכאי לעיין במידע שנשמר עליו במאגר המידע של החברה, ולדרוש את תיקונו או מחיקתו אם נמצא כי המידע אינו מדויק, שלם, ברור או מעודכן.
- 7.2. **אופן מימוש הזכות:**
- 7.2.1. הואיל והחברה משמשת כמעבדת מידע בלבד עבור משרד עורכי הדין (שהוא בעל השליטה), פניות ישירות של ניזוקים לקבלת זכות העיון או המחיקה יינתנו ויפתרו אך ורק באמצעות פנייה ישירה למשרד עורכי הדין המייצג אותם.
- 7.2.2. ככל שיתקבל פנייה כזו אצל החברה, החברה תפנה את הניזוק למשרד עורכי הדין הרלוונטי ותסייע טכנולוגית למשרד עורכי הדין לממש את זכותו של הניזוק בהתאם להוראות הדין.
- 7.2.3. פניות של עורכי הדין עצמם לגבי נתוני החשבון המנהלתיים שלהם, יבוצעו באמצעות פנייה ישירה לשירות הלקוחות של החברה.

8. ממונה הגנת הפרטיות (DPO - Data Protection Officer)

- 8.1. החברה אינה נדרשת במינוי ממונה הגנת פרטיות ואבטחת מידע (DPO) בשלב זה ובשל היקף פעילותה. החברה מינתה אחראית תחום הגנת הפרטיות ואבטחת המידע לשם פיקוח על עמידת החברה בהוראות חוק הגנת הפרטיות, תקנות אבטחת מידע והסכמי ה-DPA מול ספקי המשנה.
- 8.2. תפקידי האחראי על הגנת הפרטיות של החברה כוללים:
- 8.2.1. ניהול ובקרה של סקרי סיכונים תקופתיים והערכות השפעה על הפרטיות (DPIAs / PIAs) לפחות פעם בשנה, או בעת ביצוע שינוי טכנולוגי מהותי בפלטפורמה.
- 8.2.2. פיקוח על בדיקות אבטחה יזומות (בדיקות חדירה וסריקות פגיעויות תקופתיות).
- 8.2.3. ניטור איתור וזיהוי של אירועי סייבר וניהול תוכניות תגובה במקרה של חשש לזליגת מידע, לרבות דיווח לרשות להגנת הפרטיות בתוך 72 שעות במקרים המוגדרים בדין.
- 8.2.4. מתן מענה וטיפול בפניות של לקוחות ושל הרשות להגנת הפרטיות בכל הנוגע לסוגיות הגנת מידע ואירועי אבטחה.
- 8.2.5. לכל שאלה, פנייה או בירור בנושא הגנת הפרטיות ואבטחת המידע, ניתן לפנות לאחראי הגנת הפרטיות של החברה בכתובת הדואר האלקטרוני הייעודית: **[הוסף דוא"ל ייעודי לאבטחת מידע / פרטיות]**.

9. שינויים ועדכונים במדיניות הפרטיות

- 9.1. החברה שומרת לעצמה את הזכות לבצע שינויים, עדכונים והתאמות במדיניות פרטיות זו בכל עת, בין היתר עקב שינויים טכנולוגיים, שינוי במעבדי המשנה או שינויים בהנחיות לשכת עורכי הדין והרשות להגנת הפרטיות.
- 9.2. הודעה על עדכון מהותי במדיניות הפרטיות תפורסם באופן בולט בלוח הבקרה של הפלטפורמה או תישלח בדואר אלקטרוני למשתמשי האב לפחות 14 ימים לפני כניסת העדכון לתוקף. המשך השימוש בפלטפורמה לאחר כניסת השינויים לתוקף מהווה הסכמה אקטיבית ומחייבת לנוסח המדיניות המעודכן.