נספח הגנת פרטיות ואבטחת מידע

בין: **ט.מ.ל מערכות מידע בע"מ**, ח.פ. 510986193

מרח' בר כוכבא 23, בני ברק (להלן: "**הספק**")

-מצד אחד-

לבין: _____, ח.פ. _____

רח' _____ (להלן: "**המזמין**")

-מצד שני-

הואיל ובמסגרת השירותים הניתנים על ידי ט.מ.ל מערכות מידע בע"מ, ח.פ. 510986193 (להלן: "**הספק**"), כמפורט בהרחבה בהסכם ו/או הצעה עליה חתם הלקוח (להלן: "**המזמין**") מול הספק (להלן: "**השירותים**", "**ההסכם העיקרי**"), הספק יקבל או עשוי לקבל גישה למידע אישי שבמאגרי המידע שבשליטת המזמין (להלן: "**המידע האישי**");

והואיל ולשם כך הצדדים מעוניינים להעלות על הכתב את הסכמותיהם בהקשר לתנאים שיחולו לגבי אבטחת המידע על ידי הספק

לפיכך הוצהר, הוסכם והותנה בין הצדדים כדלקמן:

1. **<u>מבוא ונספחים</u>**

1.1. מובהר כי המבוא לנספח זה ונספחיו מהווים חלק בלתי נפרד ממנו ויפורשו ביחד עמו.

1.2. בכל מקרה של סתירה בין הוראות נספח זה לבין נספחיו ו/או לבין הוראות ההסכם העיקרי, תחול בכל הנוגע להגנת הפרטיות ואבטחת המידע הוראת נספח זה.

2. **<u>הגדרות</u>**

בנספח זה תוקנה למונחים שלהלן המשמעות שלצידם, זולת אם משתמע אחרת מהקשר הדברים. למונחים שלא הוגדרו בנספח זה תוקנה המשמעות שניתנה להם בחוק או בתקנות הרלבנטיות.

2.1. "**החוק**" - חוק הגנת הפרטיות, התשמ"א-1981.

2.2. "**תקנות אבטחת מידע**" - תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

2.3. "**דיני הפרטיות**" - החוק, תקנות אבטחת מידע, תקנות אחרות מכח החוק, והנחיות מחייבות של רשות הגנת הפרטיות.

2.4. "**ספק משנה**" - קבלן משנה המועסק על ידי הספק בקשר ישיר עם השירותים ו/או ההסכם העיקרי, אשר תהיה לו באופן כלשהו גישה למידע אישי.

2.5. "**אירוע אבטחה חמור**" - כהגדרתו בתקנות אבטחת מידע.

3. **<u>המידע האישי/מאגרי המידע</u>**

3.1. הספק יקבל גישה למידע אישי של המזמין או למאגר/י מידע של המזמין. פרטי המידע האישי שאליהם תהיה לספק גישה מפורטים ב**<u>נספח א'</u>**.

3.2. הספק מצהיר ומאשר כי ידוע לו שהבעלות במאגר המידע ובמידע האישי המצוי בו הינה של המזמין ועל כן הספק מתחייב כי לא יעשה כל שימוש במידע האישי אלא לצורך אספקת השירותים.

3.3. המזמין מתחייב לעמוד בכל החובות החלות עליו כבעל שליטה לפי דיני הפרטיות, ובכלל זאת: (א) המזמין מתחייב ליידע את נושאי המידע מטעמו ביחס לעיבוד המידע האישי אודותיהם על ידי הספק, וכן לקבל מהם את כל ההסכמות הנדרשות בקשר לכך; (ב) המזמין מתחייב כי הוא עומד בכל חובת רישום ו/או הודעה שחלה עליו בקשר עם מאגרי המידע שבשליטתו; (ג) המזמין לא ימסור לספק ולא יבקש ממנו לעבד מידע אישי שנאסף, נוצר, התקבל או נצבר בדרכים שאינן חוקיות, בניגוד להוראות החוק או לכל דין אחר.

3.4. מובהר כי אחריות הספק על פי נספח זה הינה כלפי המזמין בלבד ולא כלפי נושאי המידע מטעמו, לרבות לקוחותיו ו/או עובדיו, ואין בנספח זה כדי להקנות לצדדים שלישיים זכויות כלפי הספק.

4. **<u>מורשי גישה וספקי משנה</u>**

4.1. הגישה למידע האישי תוגבל לאותם אנשים מטעם הספק אשר הגישה למידע נדרשת להם לצורך אספקת השירותים על בסיס הצורך לדעת בלבד. באחריות הספק לבחון את רשימת מורשי הגישה וההרשאות למידע האישי של המזמין על בסיס תקופתי ולבטל הרשאות עודפות.

4.2. הספק מתחייב לתדרך כל עובד שהינו מורשה ובעל גישה למידע האישי של המזמין באשר למטרות השימוש במידע האישי וחובותיו בנושא אבטחת המידע.

4.3. עובדי הספק שתהיה להם גישה למידע האישי יחתמו על כתב התחייבות לשמירת סודיות כלפי הספק.

4.4. הספק עשוי להעסיק ספקי משנה לצורך מתן השירותים. על פי דרישה, יעביר הספק למזמין את רשימת ספקי המשנה הרלבנטיים.

4.5. הספק יתקשר בהסכם עם כל ספק משנה, בו יתחייב ספק המשנה לקיים חובות דומות בעיקרן לאלו החלות על הספק על פי נספח זה, בשים לב לפעולות העיבוד וסוג המידע האישי הכרוכים בשירותי ספק המשנה.

5. **<u>אבטחת מידע</u>**

5.1. הספק יקיים את אמצעי אבטחת המידע בהתאם למפורט ב**<u>נספח ב'</u>** לנספח זה ביחס למוצרים המאוחסנים בענן מטעם הספק, וכן יקיים את האמצעים הרלבנטיים מתוך הנספח ביחס למקרים שבהם הספק יבצע, בתיאום עם המזמין, חיבור מרחוק למערכת שמותקנת בצורה מקומית אצל המזמין לצרכי תחזוקה. מובהר כי במקרים בהם המערכת מותקנת באופן מקומי אצל המזמין ("On-Prem") אבטחת המידע השוטפת ביחס למערכת הינה באחריות המזמין בלבד.

5.2. הספק מתחייב כי תהיה הפרדה לוגית בין הפעילות שתתבצע עבור המזמין לבין הפעילות המבוצעת עבור לקוחות אחרים, לרבות לעניין הגישה מרחוק או היכולת להתחבר למאגר המידע של המזמין.

5.3. הספק ימנה ממונה אבטחת מידע מטעמו ככל שהוא נדרש לכך על פי דין.

6. **<u>זכויות נושאי מידע</u>**

6.1. ביחס למידע שמאוחסן בענן של הספק בלבד, הספק יסייע למזמין, לבקשתו, באופן סביר בטיפול בפניות של נושאי המידע לקבל גישה או לעדכן מידע אישי המצוי אצל הספק, בכל מקרה בו, מסיבה כלשהי, אין למזמין אפשרות גישה למידע האישי. כל העלויות הקשורות במתן זכות העיון, זכות התיקון או מחיקת המידע, ככל שיהיו, יחולו על המזמין.

6.2. קיבל הספק פנייה ישירה מנושא מידע, בכל הנוגע למידע לגביו הנמצא במאגר המידע של המזמין, יפנה הספק את נושא המידע אל המזמין. המזמין מתחייב לטפל בפנייה בהתאם למועדים הקבועים בדין.

7. **<u>אירוע אבטחה חמור</u>**

7.1. הספק יודיע למזמין בהקדם האפשרי מהמועד בו נודע לו על כל אירוע אבטחה חמור שארע אצלו או באחריותו בקשר עם המידע האישי של המזמין.

7.2. הדיווח יכלול את המידע הקיים אצל הספק באותה עת לעניין האירוע אשר נדרש למזמין במידת הצורך לצורך דיווח על האירוע לגורמים הנדרשים.

7.3. ככל שעל פי ייעוץ משפטי שקיבל הספק, חלה עליו חובת דיווח או יידוע של כל גורם שהוא שאינו המזמין בדבר אירוע אבטחת מידע, ככל שהדבר אפשרי לפי כל דין, ימסור על כך הספק הודעה למזמין, ויפעל בתיאום ושיתוף פעולה עם המזמין.

8. **<u>מחיקת מידע</u>**

8.1. המזמין אחראי לקבוע איזה מידע נדרש למחוק במהלך תקופת ההתקשרות ולהנחות את הספק בהתאם.

8.2. עם סיום ההתקשרות יוודא הספק כי אין ברשותו מידע אישי של המזמין, וככל שקיים כזה ידאג למחיקתו.

8.3. על אף האמור לעיל, ככל שקיימת הוראה בדין המחייבת שמירת מידע אישי של המזמין אצל הספק גם לאחר סיום ההתקשרות, לרבות המשך שמירה של מידע על השתכרות ופנסיה של עובדים למשך התקופה הנדרשת בדין לאחר תום ההתקשרות, וכן ביחס לשמירת גיבוים, ימשיך הספק לקיים את התחייבויותיו לגבי אבטחת המידע כל עוד המידע האישי מצוי אצלו. עם תום התקופה המתחייבת על פי דין, או עם תום תקופת הגיבוי, לפי העניין, אחראי הספק למחוק את המידע האישי שנותר בחזקתו.

9. **<u>דיווח ובקרה</u>**

9.1. הספק ימסור למזמין, על פי דרישת המזמין ולא יותר מפעם בשנה, דיווח לגבי אופן ניהול ואבטחת המידע האישי של המזמין המוחזק על ידו בהתאם לנספח זה.

9.2. ככל שהמידע שמסר הספק בהתאם לסעיף 9.1 לעיל לא יהיה מספק על מנת לקיים את חובות הדיווח והפיקוח של המזמין על פי דיני הגנת הפרטיות, יהא המזמין רשאי, לא יותר מאחת ל-12 חודשים, לבקש מהספק מידע הקיים אצלו אשר נדרש בקשר עם עמידה בהוראות נספח זה.

10. **<u>שונות</u>**

10.1. במקרה שהוראה כלשהי בנספח תיחשב כחסרת-תוקף, בלתי-חוקית או בלתי-ניתנת-לאכיפה בדרך אחרת על ידי בית משפט מוסמך, יתר הוראות הנספח יישארו בתוקף מלא, אך הוראה כאמור תיחשב כאילו שונתה ככל הנחוץ כדי להפוך את ההוראה הבלתי חוקית או בלתי אכיפה, לחוקית או אכיפה, תוך שמירה מרבית ככל הניתן על הכוונה וההסכמות המקוריות של הצדדים כמפורט בנספח זה.

ולראיה באו הצדדים על החתום :

ט.מ.ל מערכות מידע בע"מ	**המזמין**
תאריך : 22.12.25	**תאריך :**
שם ותפקיד: ראון אקלר - DPO	**שם ותפקיד:**

נספח א'

טופס פרטים בקשר עם עיבוד מידע אישי על ידי הספק

1. **סוגי המידע האישי אשר יעובדו על ידי הספק כמחזיק במסגרת השירותים** [כתלות בשירותים שרכש המזמין בהתאם להסכם העיקרי]

☐ **מידע על עובדים של המזמין:**

- שם מלא ופרטי העובד (כולל ת"ז)
- פרטי התקשרות (טלפון וכתובת מייל)
- שם משתמש + סיסמה
- נתוני שכר, קופות, הפרשות וזכויות סוציאליות
- פרטי חשבון בנק

☐ **מידע על לקוחות של המזמין:**

- שם מלא ופרטי הלקוח (לרבות מספר ת"ז ועוסק מורשה)
- פרטי התקשרות (טלפון, פקס כתובת מייל, כתובת)
- שם משתמש + סיסמה
- פרטי חשבון בנק, ארבע ספרות אחרונות של כרטיס אשראי
- פירוט מוצרים שנקנו, סכומים ששולמו, תאריכים וכו'

המידע האישי שיעובד ישמר על גבי ענן של חברת AWS בארה"ב/אירופה מטעם הספק.

2. **מטרות השימוש המותרות במידע האישי**

מתן השירותים למזמין בהתאם להסכם העיקרי.

3. **מערכות מאגרי המידע**

הספק יעבד מידע אישי באמצעות המערכות המפורטות להלן (בהתאם למערכת בה המזמין עושה שימוש):

מערכות און פרם	מערכות בענן
☐ שיקלולית [מידע על עובדים ולקוחות]	☐ פנסיה (שיקלולית) [מידע על עובדים]
☐ עדכנית [מידע על עובדים]	☐ שיקלולית אפ [מידע על עובדים]
☐ חיסולית [מידע על עובדים ולקוחות]	☐ שיקלולית אפ+ [מידע על עובדים]
☐ עצמאית [מידע על עובדים ולקוחות]	☐ Acountbook [מידע על עובדים ולקוחות]
☐ הצהרונית [מידע על עובדים ולקוחות]	
☐ אשפית [מידע על לקוחות]	
☐ DMS [מידע על עובדים ולקוחות]	

הספק רשאי לעבד את המידע האישי של המזמין בהתאם להוראות ההסכם העיקרי ונספח זה, לרבות איסוף, שמירה, אחסון, והכל כנדרש לשם מילוי התחייבויות הספק תחת ההסכם העיקרי.

4. **משך שמירת המידע האישי על ידי הספק**

כמפורט בגוף הנספח ובהתאם להחלטת המזמין.

נספח ב'

מסמך אבטחת מידע

בנספח זה מפורטות דרישות אבטחת המידע בהן הספק נדרש לעמוד בקשר עם מאגר המידע של המזמין המאוחסנים בענן מטעם הספק, והמידע המצוי בו, אשר יעובד ע"י הספק במסגרת ההתקשרות בין הצדדים:

1. **טכנולוגיות אבטחת מידע** – לקיים אבטחת מידע נאותה לרשת הארגונית שתמנע חדירה מקרית או מכוונת למידע האישי של המזמין, ולהגן על מערכות המידע אצל הספק, לרבות תחנות העבודה, השרתים, מערכות הרשת, ציוד הקצה וציוד נייד, באמצעות טכנולוגיות אבטחת מידע מקובלות למניעת חדירות ושימוש בלתי מורשה במערכות המידע, לרבות מנגנוני ניטור, תיעוד והתראה על ניסיונות חדירה ושימוש בלתי מורשה (ולשמור את הלוגים המתעדים את הגישה למערכות למשך 24 חודשים).

   בפרט, יקפיד הספק על האמצעים הבאים:

   1.1. פיירול תיקני עם חבילת הגנת סייבר מאוקטבת ומוגדרת לפי המלצות יצרן כולל גרסת FIRMWARE עדכנית.

   1.2. אנטי וירוס מוכר עם הגנת EDR מוגדרת ופעילה.

   1.3. VPN בשילוב מערכת אימות כפול.

   1.4. מנגנון החלפת סיסמה באופן מבוקר ומנוהל GPO

2. **עדכוני אבטחה** – לעדכן את מערכות המידע של הספק באופן שוטף ובהתאם להנחיות היצרן, ככל שנדרש. הספק מתחייב להשתמש במערכות הפעלה מאוקטבות ועדכניות של חברת מייקרוסופט.

3. **הצפנת מידע בתקשורת** – לא לאפשר גישה לתשתיות מאגרי המידע מרשת האינטרנט, ולא להעביר את המידע האישי של המזמין על גבי רשת האינטרנט או רשת ציבורית אחרת, אלא אם מידע זה מוצפן בשיטת הצפנה מקובלת וסבירה והמפתח אינו נשלח ביחד עם המידע.

4. **התקנים ניידים** – לא לשמור את המידע של המזמין על גבי התקנים ניידים מבלי להצפין אותם באמצעי הצפנה סבירים ומקובלים ולהטמיע אמצעי הזדהות חכמים לגישה אל המידע המאוחסן בהם.

5. **אבטחה פיזית** – הספק מתחייב לנקוט באמצעי האבטחה הפיזיים כדלקמן:

   5.1. לאחסן את המידע במשרד מאובטח אשר הגישה הפיסית אליו מוגבלת למורשים בלבד.

   5.2. לדאוג לכך שבמשרדי הספק מותקנת מערכת הגנה טובה ותקינה כנגד פריצה.

   5.3. להגן על חדרי השרתים ומערכות המידע המרכזיות של הספק באמצעי אבטחה פיזיים ולנהל בקרה ותיעוד אוטומטיים של הגישה או של ניסיונות גישה לחדרים אלו, לרבות שם מבקש הגישה, תאריך ושעת ניסיון הגישה ולשמור את הלוגים על כך למשך 24 חודשים.

   5.4. לנעול את מסכי ותחנות עבודה בכל עת בה מורשי הספק עוזבים את תחנת העבודה.

   5.5. להקפיד על יישום מדיניות "שולחן נקי".