הגנת הפרטיות - אבטחת מידע

נספח זה של הגנת הפרטיות אבטחת מידע (להלן: "**הנספח**") מהווה חלק בלתי נפרד מהסכם התקשרות לשירותי ענן ו/או התנאים הכלליים וכל הסכם ו/או הזמנה של שירותי ענן (להלן ביחד "**ההסכם**") שבין טריפל סי מחשוב ענן בע"מ (להלן: "**החברה**") לבין מזמין השירותים (להלן: "**הלקוח**").
הסכם זה חל כאשר במהלך מתן שירותי הענן הלקוח יחזיק או יאחסן מאגר מידע (להלן: "**מאגר המידע**") כהגדרתם בחוק הגנת הפרטיות, התשמ"א-1981 על גבי מערכות התשתית של החברה.

1. מערכות וסביבת שירותי הענן

1.1. שירות הענן הוא שירות מקוון המסופק על ידי החברה באמצעות מערכות התשתית, רכיבים ומערכות חומרה כגון שרתים, ציוד רשת ומערכות תוכנה מארחות המשמשות את החברה לאספקת השירותים (להלן: "**מערכות התשתית של החברה**").

1.2. שירותי הענן אינם כוללים תוכנות, יישומים ושירותים צדי ג' ממערכות אשר אינם בבעלות ו/או שליטת החברה, הניתנים בתנאי שירות והגנת פרטיות נפרדים.

1.3. מערכות התשתית של החברה נמצאים במתקני החברה (Data Center) המצויים פתח תקווה ובטירת הכרמל (להלן: "**מתקן החברה**").

1.4. עם רכישת שרותי הענן על ידי הלקוח מוסרת החברה לידי הלקוח סביבה לשמושו וניהולו האישיים בהתאם לדרישות והמפרטים השונים שנתנו לה על ידי הלקוח (להלן: "**סביבה או "סביבת הלקוח"**).

1.5. סביבת הלקוח מאפשרת קביעת משאבים שונים, תכונות, פונקציונליות ו/או פקדים שהלקוח רשאי להשתמש בהם לפי בחירתו ו/או לפי קביעתו, כולל ממשק ניהול, הצפנה, רישום וניטור, ניהול זהות וגישה, סריקת אבטחה וחומות אש בהתאם לסוג השירות.

2. אבטחת המידע

2.1 בשימוש הלקוח בשירותי הענן של החברה מצהיר הלקוח כי הוא מודע ומסכים לכך כי:

א. סוג המידע שהחברה רשאית לעבד ומטרות שימוש –

לחברה אין ידיעה בדבר המידע אשר שלהלקוח מאחסן על גבי מערכת התשתית של החברה לרבות מאגרי המידע וסיווגם אלא אם הודיע אחרת הלקוח לחברה בכתב.

לשם מתן השירותים המפורטים בהסכם ו/או על מנת לעמוד בהתחייבויותיה החוזיות, החברה תהא רשאית לעבד כל מידע, כהגדרתו בחוק הגנת הפרטיות, הנמצא על גבי תשתיות החברה.

ב. מערכות המאגר שהחברה רשאית לגשת אליהן –

לחברה ו/או למי מטעמה יש גישה אל מערכות התשתית של החברה אשר הינן חלק ממערכות המאגר של הלקוח. במקרים מסוימים, כגון תמיכה, תחזוקה או פתרון בעיות, על פי הסכמה של הלקוח או לבקשתו, תינתן לחברה גישה לסביבת הלקוח, לצורך ביצוע פעולות עבורו בהתאם להסכם בין הצדדים.

ג. **סוגי העיבוד שהחברה רשאית לעשות –**

כל אותן פעולות עיבוד אשר דרושות לשם מתן השירותים, לרבות מחשוב, אחסון, גיבוי, שחזור, העתקה, תחזוקה וכיו"ב.

ד. **משך ההתקשרות, הפסקת השירותים ומחיקת מערכות המאגר –**

משך, אופן ומועד הפסקת ההתקשרות הינו בהתאם להסכם שבין הצדדים. במהלך ההתקשרות הלקוח אחראי למידע, למאגרי המידע ולניהולם לרבות מחיקת המידע.

מבלי לגרוע מהאמור, במקרה של סיום או הפסקת ההתקשרות בין הצדדים מכל סיבה שהיא, תמחק החברה את סביבת הלקוח על כל המידע המצוי על גבי מערכות התשתית של החברה, בהתאם לנהלי החברה ובהתאם לסיכום עם הלקוח. על הלקוח בטרם סיום ההתקשרות, לדאוג להעביר ו/או לגבות ו/או למחוק את המידע.

על אף האמור לעיל, ככל שיש הוראה בדין המחייבת שמירה של מידע על ידי החברה, או שהחברה נדרשת לשמור מידע לצורכי התגוננות מתביעות, תשמור החברה את המידע המינימלי הנדרש ותאפשר גישה למידע אך ורק למטרה הנ"ל ולמורשי גישה הנדרשים לכך בלבד. כל עוד נותר המידע שמור בארכיב החברה, יחולו עליה כל הוראות נספח זה וכן הוראות בעניין סודיות המידע בהסכם.

ה. **יישום החובות בתחום אבטחת המידע –**

החברה הינה בעלת הסמכה לתקן ISO27001 ומתחייבת להחזיקו בתוקף לכל אורך תקופת מתן השירותים. בהנחיית רשם מאגרי המידע מס' 03/2018 בנוגע לתחולת תקנות הגנת הפרטיות על ארגונים המוסמכים לתקן ISO27001, נקבע כי "ארגונים שקיבלו הסמכה לתקן יראו אותם כמקיימים את הוראות התקנות במלואן ביחס למאגרים עליהם ניתנה הסמכה בתקן" (ראה הנחיית רשם מאגרי המידע מס' 03/2018).

החברה יישמה צעדים טכניים והארגוניים בנושאים הבאים:

1. **ממונה אבטחת מידע**

לחברה מונה מנהל אבטחת מידע והוא ו/או נציג אחר שיסוכם בין הצדדים ישמש מול הלקוח כאיש הקשר בנושא אבטחת המידע. אין באמור לגרוע מחובתו של הלקוח למנות ממונה אבטחת מידע ככל שהדבר נדרש ממנו בהתאם לכל דין ו/או הנחיה ו/או תקן.

2. **אבטחה פיזית וסביבתית**

מתקן החברה, הינו מקום מוגן אשר אינו מאפשר כניסה אליו בלא הרשאה. החברה נוקטת אמצעים לבקרה ולתיעוד של הכניסה והיציאה בהם מצויות המערכות וכן של הכנסה והוצאה של ציוד אל המתקן וממנו:

א. הכניסה מצולמת במצלמות אבטחה, מאובטחת 24/7, נעולה ונשלטת המאפשרת גישה דרך נקודת כניסה מבוקרת ומורשית בלבד.

ב. כניסה למתקן באישור ובליווי אחד מעובדי החברה בלבד.

3. **ניהול כוח אדם**

בטרם מתן גישה לעובד למערכות התשתית, החברה נוקטת אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי אינו מתאים לקבלת גישה למערכות התשתית של החברה (להלן: "**בעל הרשאה**"); אמצעים כאמור ננקטים בשים לב לרגישות התפקיד ולהיקף הרשאות הגישה המיועד לו.

החברה מתדרכת באופן תדיר את עובדיה בנושא החובות לפי החוק והתקנות ואודות חובותיהם לפי נוהל האבטחה של החברה.

4. **ניהול הרשאות גישה**

הגישה למערכות התשתית של החברה, מוגבלת אך ורק לאותם עובדים הנדרשים לצורך מתן השירותים מטעם החברה בהתאם להגדרות תפקידם ובמידה הנדרשת לביצוע התפקיד בלבד. החברה מנהלת רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן: "**רשימת ההרשאות התקפות**").

5. **זיהוי ואימות**

החברה מוודא כי הגישה למערכות התשתית של החברה, נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות. החברה דואגת לביטול ההרשאות של בעל הרשאה שסיים את תפקידו ולשינוי סיסמאות למערכות השונות, אשר בעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

6. **בקרה ותיעוד גישה**

החברה מנהלת מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה אל מערכות התשתית.

7. **התקנים ניידים**

עובדי החברה מוגבלים, אם באמצעות אכיפה טכנית ואם באמצעות נהלים, מחיבור התקנים ניידים למערכות התשתית.

8. **ניהול מאובטח ומעודכן של מערכות התשתית**

מערכות התשתית מנוהלות ומופעלות באופן תקין, לפי המקובל בהפעלת מערכות כאלה. המערכות לרבות חומר המחשב הנדרש לפעולתן מעודכנים באופן שוטף.
מערכות התשתית מופרדות, בהיקף ובמידה הסבירים האפשריים, ממערכות מחשוב אחרות המשמשות את החברה.

9. **אבטחת תקשורת**

מתקני החברה מחוברים באמצעות קישורים פרטיים מהירים כדי לספק העברת נתונים מאובטחת ומהירה בינהם. חיבור זה נועד למנוע קריאה, העתקה, שינוי או הסרה של מידע ללא אישור במהלך העברה או או בזמן שהם מוקלטים על גבי אמצעי אחסון נתונים.

הקישור של מערכות התשתית של החברה אל רשת האינטרנט מאובטח באמצעות אמצעי הגנה מתאימים.

ככלל, התעבורה ברשת הציבורית אינה מוצפנת. החברה מעבירה נתונים באמצעות פרוטוקולים סטנדרטיים באינטרנט. העברת מידע מוצפן אפשרית, במידה והמזמין רכש שרות מתאים.

ו. **<u>התחייבות לשמירת סודיות המידע</u>** –

החברה מתחייבת לשמור בסודיות מלאה על סודיות המידע, לא תיכנס או תשתמש בו אלא בקשר עם מתן השירותים ועל פי ההסכם בין הצדדים. כל המועסקים על ידי החברה ו/או מטעמה, במתן השירותים, ישמרו על סודיות המאגר כאמור לעיל. מבלי לגרוע מהאמור לעיל, על כל עובדי החברה חלות חובות הסכמיות לשמירת סודיות ואבטחת מידע.

ז. **<u>מתן שירות באמצעות גורם חיצוני</u>** –

על מנת לספק את שירותי הענן ו/או למלא אחר התחייבויותיה החוזיות עושה שימוש בתוכנות ו/או מערכות תוכנה, לרבות קבלת תמיכה של גורמי צד ג' (להלן: "**ספקי משנה**"). לספק המשנה תהיה ככל הניתן, גישה מוגבלת רק במידה הנדרשת לביצוע השירות בהתאם להסכם החל עם החברה.

ח. **<u>דיווחים</u>**

1. על פי דרישת הלקוח, החברה תדווח אודות אופן ביצוע חובותיה לפי התקנות ונספח זה.
2. **דיווח על אירוע אבטחת מידע** –

א. החברה תודיע ללקוח בהקדם האפשרי מרגע שנודע לה על אירוע שנעשה בו שימוש במידע בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע. החברה תעשה מאמצים סבירים כדי לסייע ללקוח לצמצם, במידת האפשר, את הסיכונים ולהקטין את הנזקים.

ב. כדי לסייע ללקוח בדיווחים על אירועי אבטחה שהלקוח נדרש לבצע במסגרת תקנות הגנת הפרטיות, החברה תכלול בהודעה מידע שהחברה מסוגלת באופן סביר לחשוף ללקוח, בהתחשב באופי השירותים, המידע העומד לרשותה וכל הגבלה על גילוי המידע, כגון סודיות.

ג. הלקוח מסכים כי תקרית אבטחה לא מוצלחת לא תהיה כפופה לסעיף זה. אירוע אבטחה לא מוצלח יחשב כאירוע שלא הייתה בו גישה בלתי מורשית למאגר המידע או לסביבת הלקוח, ויכול לכלול, ללא הגבלה, מתקפות ping ושידור אחרים על חומות אש או שרתי קצה (Edge Servers), סריקות פורטים, ניסיונות כניסה כושלים, התקפות של מניעת שירות, Packet Sniffer (או גישה לא מורשית אחרת לנתוני תעבורה שאינה גורמת לגישה מעבר ל-Headers) או תקריות דומות.

א. חובת החברה לדווח או להגיב על אירוע אבטחה לפי סעיף זה אינה ולא תפורש כהכרה של החברה על כל אשמה או אחריות של החברה ביחס לאירוע אבטחה.

ב. הודעה על אירועי אבטחה, תימסר לאחד או יותר ממנהלי הלקוח בכל דרך שהחברה בוחרת, כולל באמצעות דוא"ל. באחריות הבלעדית של הלקוח להבטיח כי הוא שומר על פרטי קשר מדויקים עם החברה בכל עת.

3. ביקורות

החברה משתמשת במבקרים חיצוניים כדי לאמת את הלימות אמצעי האבטחה של מערכות התשתית מהם היא מספקת את השירותים, לרבות ביצוע סקר סיכונים. ביקורת זו: (א) מבוצעת לפחות בשנה; (ב) על פי תקן ISO27001; (ג) על ידי גורמי אבטחה עצמאיים של צד שלישי; ו- (ד) בסיומה מופק דו"ח ביקורת לחברה (סודי).

החברה דנה בתוצאות דו"ח הביקורת ובהתאם בוחנת את הצורך בעדכון נוהל האבטחה ופועלת לתיקון הליקויים שהתגלו במסגרת הדו"ח, ככל שהתגלו.

4. יישום אבטחת המידע על ידי הלקוח

4.1 הלקוח מצהיר ומסכים בהתבסס על השימוש הנוכחי והמיועד שלו בשירותי הענן, כי השירותים, אמצעי האבטחה, בקרות אבטחה נוספות וההתחייבויות החברה בנספח זה: (א) עונים על צרכי הלקוח, כולל בכל התחייבויות אבטחה המידע בהתאם לתקנות הגנות הפרטיות ו/או כל דין אחר החל על המידע, ו- (ב) מספקים רמת אבטחה המתאימה לסיכון למאגרי המידע.

4.2 הלקוח מצהיר כי הוא מודע לכך כי כבעל המאגר הוא אחראי לאבטחת המידע ולעמידה בתקנות הגנת הפרטיות וכי אין באמור בנספח זה כדי לגרוע מאחריות הלקוח כבעלים, מנהל ו/או מחזיק של מאגר מידע גם במידה והוא עושה שימוש בשירותי ענן.

4.3 סביבת הלקוח, מאפשרת מספר בקרות, תכונות אבטחה ופונקציות שונות (Features), בהן הלקוח עשוי להשתמש כדי לאחזר, לתקן, למחוק או להגביל את הגישה למידע. הלקוח אחראי לתפעל ולהשתמש בבקרות אלה כאמצעים טכניים וארגוניים כדי לסייע לו בקשר להתחייבויותיו עם תקנות הגנת הפרטיות.

4.4 אין באמור כדי לגרוע מחובת הלקוח ליישם אמצעים טכניים וארגוניים אחרים הדרושים בהתאם לרמת האבטחה של מאגרי המידע. חלק מאמצעים אלו יכול הלקוח לרכוש מהחברה או ישירות מספק צד ג', כדוגמת:

א. הצפנה כדי להבטיח רמת אבטחה מתאימה.

ב. ניהול הרשאות גישה, אמצעים לאימות החשבון למערכות שהלקוח משתמש בהם לגישה לשירותי הענן ו/או סביבת הלקוח.

ג. אמצעים לאבטחת סודיות מתמשכת, שלמות, זמינות ועמידות המערכות והשירותים המופעלים על ידי הלקוח.

ד. אמצעים המאפשרים ללקוח גיבוי וארכיב כראוי על מנת להחזיר את הזמינות והגישה למידע בזמן אירוע.

ה. תהליכים לבדיקה, והערכה אפקטיביות של הצעדים הטכניים והארגוניים המיושמים על ידי הלקוח באופן קבוע.

4.5 בהתאם לכך הלקוח מצהיר כי הובהר וידוע לו כי:

4.5.1 במסגרת שירותי הענן החברה מספקת רישוי תוכנה במודל חודשי למגוון רחב של חבילות תוכנה. לעיתים מספקת החברה גם עותק של רישוי התוכנה מותקן על סביבת הלקוח לפי דרישה. עם מסירת ו/או התקנת התוכנה והרישוי, חלה על הלקוח חובה לדאוג לעדכוני אבטחת מידע בחבילת התוכנה לפי הצורך וזמינות העדכונים אצל יצרן התוכנה. רישוי תוכנה זה מסופק ללקוח כרישוי בלבד, על הלקוח לבדוק מול יצרן התוכנה ו/או בהסכם ההתקשרות (Eula) תאימות התוכנה לרמת האבטחה הנדרשת ממאגרי המידע הקיימים אצל הלקוח והתאמתה לתקנות הגנת הפרטיות. הלקוח אחראי באופן בלעדי לכל מוצר שהוא מתקין או משתמש בשירות מקוון או רוכש או מנהל באמצעות שירותי הענן של החברה.

4.5.2 שירותי גיבוי אינם כלולים כחלק מחבילת השירות אלא במקרים בהם הדבר מפורט בהזמנת השירות. שירותים אלו ניתנים לרכישה בנפרד. אין באמור כדי לגרוע מחובתו של הלקוח לערוך בנוסף גיבוי של המידע, לרבות נתוני התקשרות עם צדדים שלישיים, וזאת בכל דרך שימצא לנכון, מחוץ למערכות התשתית של החברה. השירות ניתן כפי שהוא (As-is). באחריות הלקוח לקבוע נוהל גיבוי ושחזור (יומי/שבועי/חודשי/שנתי), לרבות ביצוע ניסוי שיחזור מידע. החברה אינה מתחייבת להצלחת השיחזור, לנכונות ותקינות המידע.

4.5.3 כחלק משירותיה, החברה מספקת שירותים מנוהלים לשרות תמיכה בשירותי הענן וציוד תקשורת, על פי הסכמה של הלקוח תינתן לחברה גישה לתוך סביבת הלקוח, לצורך ביצוע פעולות עבורו בהתאם להסכם בין הצדדים. השירותים ניתנים כשירותי מומחה לביצוע לפי הוראות והנחיות הלקוח. על הלקוח לוודא כי גישה זו, היא גישה זמנית (שם משתמש וסיסמא זמניים) וכי על ידי נקיטת אמצעים טכניים וארגוניים נמנעת הגישה מהחברה למאגרי המידע המצויים על סביבה זו ו/או מהמידע המצוי במאגרים אלו. אין במתן גישה כאמור משום הרחבת הוראות נספח זה.

4.6 מבלי לגרוע מהאמור, הלקוח אחראי (א) ליישם את האמצעים המתוארים בסעיף 4.3 , 4.4 ו- 4.5 לפי הצורך, (ב) להגדיר כראוי את השירותים, (ג) להשתמש בפקדים ובפונקציות הקיימות בקשר עם השירותים (כולל בקרות האבטחה) המאפשרים ללקוח להחזיר את הזמינות והגישה לנתונים במועד (למשל גיבויים וארכיון שוטף של מאגרי המידע) ו (ד) לנקוט צעדים שיראו ללקוח כנאותים לשמירה על אבטחה, הגנה ומחיקה של המידע, הכוללים שימוש בטכנולוגיית הצפנה כדי להגן עליהם מפני גישה בלתי מורשית ואמצעים לבקרה על הרשאות גישה.

5. כללי

5.1 למעט כפי שתוקן על ידי נספח זה במפורש, ההסכם והתנאים הכלליים החלים עליו יישארו במלואם בתוקף לרבות אחריות וחבות החברה. במידה קיימת סתירה בין ההסכם לנספח זה, תנאי נספח זה יגברו בכל הנוגע לאבטחת המידע והגנת הפרטיות.

5.2 נספח זה ממצה את ההסכמות בין הצדדים ביחס לעניינים המוסדרים בו ולא יהיה תוקף לכל הסכמה או מצגים, בין בעל פה ובין בכתב (ככל שישנם), אשר לא מצאו בו ביטוי במפורש.

5.3 נספח זה אינו מהווה הסכם לטובת צד שלישי ואין בו כדי להקנות זכויות כלשהן לצד שלישי. על נספח זה יחול הדין הישראלי בלבד.

5.4 אם הוראה כלשהי בנספח זה תימצא על ידי ערכאה מוסמך כבלתי ניתנת לאכיפה, כל יתר הוראות הנספח ימשיכו לחול ולחייב את הצדדים.

5.5 כל תיקון, שינוי או תוספת לנספח זה יהיו תקפים אך ורק אם ייעשו בכתב וייחתמו על ידי מורשי החתימה מטעם הצדדים.