הגנת הפרטיות (אבטחת מידע)

תנאים אלו הם בנוסף לכל מסמך התקשרות אחר בין הלקוח לבין החברה, ולתנאים הכלליים החלים על אותו שירות שהזמין הלקוח. כל אלו ביחד יהוו את הסכם ההתקשרות של הלקוח עם החברה.

1. כללי

1. החברה מספקת שירותי ענן ללקוחותיה במכתונת של **IAAS** (תשתית כשירות) ו/או **SAAS** (תוכנה כשירות) (להלן ביחד או לחוד: "**שירותי הענן**").

2. שירותי הענן ניתנים באמצעות מערכות התשתית של החברה (Data Center) המצויים ברח' **הסיבים 49, פתח תקווה** (להלן: "**מערכות התשתית של החברה**").

3. 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"**).

4. במסגרת השימוש בשירותי הענן ייתכן ויחזיק הלקוח על גבי הסביבה שהועברה לרשותו ולניהולו מאגר/ים של מידע ו/או מידע רגיש (להלן: "**מאגר המידע**") כהגדרתם בחוק הגנת הפרטיות, התשמ"א-1981.

5. מטרת מסמך זה, לסייע ללקוח בקיום הוראות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "התקנות" או "תקנות הגנת הפרטיות") באמצעות מודל תפעולי של אחריות משותפת לאבטחת המידע של הלקוח (ראה: רמו"ט- שאלות ותשובות בנושא מיקור חוץ)

2. אחריות תפעולית

ראשית יש להבהיר כי שירותי הענן אינם כרוכים במתן גישה לחברה למאגר המידע של הלקוח וכי:

א. **החברה אינה מעבד מידע של הלקוח** – הלקוח הינו אחראי בלעדי לעיבוד המידע המצוי בסביבת הלקוח.

ב. **גישה אל מערכות המאגר** - לחברה ו/או למי מטעמה אין כל גישה ישירה או עקיפה אל מאגרי המידע של הלקוח.

ג. **סוגי העיבוד** - החברה אינה רשאית לעשות במידע ו/או מאגרי המידע כל שימוש, לרבות גילוי העברה או מסירה ולפיכך כלל אינו מחזיק במאגרי המידע של הלקוח.

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

1. משך אופן ומועד הפסקת ההתקשרות הינו בהתאם להסכם שבין הצדדים.

2. במהלך ההתקשרות הלקוח אחראי למידע למאגרי המידע, למידע ולניהולם לרבות מחיקת המידע. מחיקת המידע על ידי החברה יכולה להתבצע אך ורק על ידי מחיקת סביבת העבודה של הלקוח.

3. הלקוח רשאי לדרוש מהחברה למחוק את סביבת הלקוח והחברה מתחייב לפעול על פי דרישת הלקוח עם קבלת הדרישה.

4. מבלי לגרוע מהאמור, במקרה של סיום או הפסקת ההתקשרות בין הצדדים מכל סיבה שהיא, תמחק החברה את סביבת הלקוח על כל המידע המצוי בו לרבות שרתים, כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת, בהתאם לנהלי החברה ובהתאם לסיכום עם הלקוח. המחיקה תבוצע באופן שאינו מאפשר לשחזר או לאחזר את המידע שנמחק בכל אופן שהוא. על הלקוח בטרם סיום ההתקשרות, לדאוג להעביר ו/או לגבות ו/או למחוק את המידע מהמערכות.

ה. יישום החובות בתחום אבטחת המידע

החברה הינה בעלת תקן ISO27001 ומתחייב להחזיקו בתוקף לכל אורך תקופת מתן השירותים. בהנחיית רשם מאגרי המידע מס׳ 03/2018 בנוגע לתחולת תקנות הגנת הפרטיות על ארגונים המוסמכים לתקן ISO27001, ניתן פטור חלקי מעמידה בכל התקנות ונקבע כי ארגונים שקיבלו הסמכה לתקן ומקיימים בפועל את הוראותיו לרבות את כל הבקרות הרלבנטיות יראו אותם כמקיימים את אותן הוראות בתקנות (הנחיית רשם מאגרי המידע מס׳ 03/2018).

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

מערכות התשתית של החברה מצויים במתקן חברה, מקום מוגן אשר אינו מאפשר כניסה אליו בלא הרשאה, לרבות קיומם של אמצעים לבקרה ולתיעוד של הכניסה והיציאה בהם מצויות המערכות המפורטות וכן של הכנסה והוצאה של ציוד אל המתקן וממנו:

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

כניסה למתקן באישור ובליווי אחד מעובדי חברה בלבד.

3. ניהול כוח אדם

בטרם מתן גישה לעובד למערכות התשתית של חברה, 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 ותקנות, ואודות חובותיהם לפי נוהל האבטחה של חברה.

4. **ניהול הרשאות גישה**

א. הגישה למערכות התשתית של החברה, מוגבלת אך ורק לאותם עובדים הנדרשים לצורך מתן השירותים מטעם החברה בהתאם להגדרות תפקידם ובמידה הנדרשת לביצוע התפקיד בלבד.

ב. החברה מנהלת רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן: "**רשימת ההרשאות התקפות**").

5. **זיהוי ואימות**

א. החברה מוודא כי הגישה למערכות התשתית של החברה, נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות.

ב. החברה דואגת לביטול ההרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי 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 למערכות התשתית של החברה.

7. **התקנים ניידים**

עובדי החברה מנועים, אם באמצעות נהלים ואם באמצעות אכיפה טכנית, מלהכניס קבצים לרשת באופן לא מאובטח..

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

א. מערכות התשתית עליהן מופעלת סביבת הלקוח מאובטחות על פי הסטנדרטים המקובלים בשוק האבטחה. המערכות מעודכנות באופן שוטף ותדיר בתיקוני ועדכוני אבטחה המופצים על ידי היצרנים.

ב. ישנה הפרדה בין סביבות הלקוח לבין סביבות של לקוחות אחרים ו/או של החברה עצמה. ההפרדה לרבות הגישה מרחוק או היכולת להתחבר לסביבות הלקוח היא באמצעות אבחנה לוגית לשרתים על גביהם מצוי המידע של הלקוח.

9. **אבטחת תקשורת**

א. ככלל, התעבורה ברשת הציבורית אינה מוצפנת. העברת מידע מוצפן אפשרית, במידה והמזמין רכש שרות מתאים.

ב. הקישור של מערכות התשתית של החברה אל רשת האינטרנט מאובטח באמצעות firewall ואמצעים נוספים על מנת למנוע הוצאת מידע מתוכם.. עם זאת, באחריות הלקוח לוודא באם אבטחה זו מספקת הגנה מתאימה למידע הקיים על מערכות ו/או סביבת הלקוח.

1. <u>התחייבות לשמירת סודיות המידע</u>

1. החברה מתחייבת לשמור בסודיות מלאה כל מידע סודי שהועבר אליה ולא להשתמש במידע הסודי אלא בקשר עם ביצוע הסכם זה.

2. כל המועסקים על ידי החברה ו/או מטעמה, במתן השירותים, ישמרו על סודיות המידע הסודי כאמור לעיל. מבלי לגרוע מהאמור לעיל, כל המועסקים מטעם החברה, לרבות עובדים ו/או קבלני משנה, בטרם מתן השירותים ללקוח, חתומים על הצהרות לשמירת סודיות ואבטחת מידע.

2. <u>מתן שירות באמצעות גורם חיצוני</u>

החברה לא תספק שירותי ענן אלא באמצעות עובדים בעלי הרשאה ולא תתיר לגורם חיצוני לתת את שירותי הענן ללקוח ,ללא אישור הלקוח מראש ובכתב.

כל ספק משנה שעמו תתקשר החברה, יהיה חייב, כתנאי מוקדם להיותו ספק משנה בקשר עם השירותים, להתחייב כלפי החברה בהתחייבויות מקבילות להתחייבויות החברה כלפי הלקוח לקיים, לכל הפחות, באותה רמת הגנה ואבטחת מידע החלה על החברה.

3. <u>גיבוי ושחזור</u>

א. באחריות הלקוח לקבוע נוהל גיבוי ושחזור. יובהר כי שירותי גיבוי של מידע הלקוח אינם כלולים כחלק מחבילת השירות אלא במקרים בהם הדבר מפורט בהזמנת השירות. שירותים אלו ניתנים לרכישה בנפרד.

ב. באפשרות החברה לספק ללקוח, שירותי גיבוי לצורך עמידותו בתקנות הגנת הפרטיות:

1. גיבוי שגרתי Backup incremental או SnapShot.
2. גיבוי תקופתי Full Backup.
3. עותק גיבוי למקרה אסון (עותק שלישי או עותק DR).

4. <u>אחריות וחבות הלקוח</u>

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

הלקוח מצהיר בזאת כי סדרי אבטחת מאגרי המידע הנהוגים אצל החברה, כאמור לעיל, ידועים ומקובלים עליו, וכי אין באמור כדי לפטור את הלקוח מעמידה בתקנות.