

נספח ב' - אבטחת מידע, הגנת סייבר ופרטיות

1. כללי:

- 1.1. הוראות נספח זה חלות על ספקים המוגדרים כספקים המחזיקים אצלם מידע עסקי, ספקים בעלי גישה לוגית רחבה, ספקי טכנולוגיה, מפתחי מערכות, או ספקים המוגדרים כ"מחזיקי מידע" כהגדרתם בחוק.
- 1.2. הוראות נספח זה באות להוסיף על הוראות ההסכם ולא לגרוע מהן. מובהר כי דרישות אבטחת המידע והביטחון של הרשות המפורטות בנספח זה, הינן בנוסף לדרישות אבטחת המידע שהוגדרו על ידי מערך הדיגיטל הלאומי או החשב הכללי במשרד האוצר (ככל שההתקשרות הינה מכוח מכרז מרכזי שלהם), ואינן גורעות מהן.
- 1.3. עמידה בהוראות נספח זה, לרבות עמידה בציון הסף בשאלון שרשרת האספקה ו/או תקני אבטחת המידע, הינה תנאי סף להתקשרות והפרתן תחשב כהפרה יסודית של ההסכם.

2. טבלת תחולה (מודולרית):

התחייבויות הספק יחולו בהתאם לסימון המזמין בטבלה להלן:

פרק	נושא	רלוונטי	סימון תחולה (ע"י המזמין)
א'	תשתית אבטחה רוחבית ושמירת סודיות	☒	חל על כל הספקים
ב'	דרישות שרשרת אספקה וסייבר [פירוט דרישות מענה בגוף הפרק]	☒	ספקים בעלי קישוריות, פיתוח תוכנה, תשתיות, ענן, OT וכד'
ג'	הגנת הפרטיות (מחזיק מידע)	☒	ספקים המעבדים/מאחסנים מידע אישי רגיש/בעל רגישות מיוחדת עבור המזמין

3. הגדרות:

- 3.1. "מידע": מידע עסקי, מסחרי, טכנולוגי או ביטחוני, המצוי במאגרי המזמין או שהספק נחשף אליו במסגרת עבודתו. הגדרה זו כוללת גם "מידע אגבי": מידע שהגיע לידיעת הספק באקראי (שמיעת שיחות, צפייה במסכים/מסמכים, זהות מבקרים).
- 3.2. "מידע אישי": נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי, "אדם הניתן לזיהוי" - מי שניתן לזהותו במאמץ סביר, במישרין או עקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי.
- 3.3. "מידע בעל רגישות מיוחדת":
 - 3.3.1. מידע על צנעת חיי המשפחה של אדם, על צנעת אישיותו ועל נטייתו המינית.
 - 3.3.2. מידע המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי לפי חוק זכויות החולה.
 - 3.3.3. מידע גנטי, כהגדרתו בחוק מידע גנטי.
 - 3.3.4. מזהה ביומטרי המשמש או מיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב.
 - 3.3.5. מידע על מוצאו של אדם.
 - 3.3.6. מידע על עברו הפלילי של אדם.
 - 3.3.7. מידע על דעותיו הפוליטיות של אדם או אמונותיו הדתיות או השקפת עולמו.
- 3.4. "מחזיק" לעניין מאגר מידע: גורם חיצוני לבעל השליטה במאגר המידע המעבד מידע עבורו

מערכות מידע ואבטחת מידע

3.5. "עיבוד", "שימוש": כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו.

פרק א': תשתית אבטחה רוחבית ושמירת סודיות:

1. סודיות, מניעת חשיפה ומהימנות עובדים:

- 1.1. הספק מתחייב לשמור בסודיות גמורה כל מידע שנחשף בפני עובדיו, בין אם מתוך מערכות המידע ובין אם באופן אגבי (שיחות טלפון/מסדרון/מראה עיניים וכד').
- 1.2. **מניעת חשיפה ברשתות חברתיות:** הספק ועובדיו מתחייבים שלא לתעד, לצלם, להקליט או לפרסם כל פרט הנוגע למתרחש במתקני המזמין. איסור זה כולל הפצה בעל-פה או בכתב (לרבות רשתות חברתיות) של מידע אודות התנהלות פנים-ארגונית, שיחות מסדרון, מידע על נבחר ציבור או בכירים ששהו במקום או כל אירוע חריג אחר אליו נחשפו.
- 1.3. **התחייבות לאבטחת מידע וסודיות:** הספק מתחייב להחתים את כל עובדיו, קבלני המשנה וכל גורם מטעמו (להלן: "עובדי הספק") על נספח סודיות אישי (נספח א' לפרק זה) בטרם תחילת עבודתם. הטפסים החתומים יישמרו במשרדי הספק וישלחו לממונה אבטחת המידע כתנאי לתחילת העסקה.
- 1.4. **בדיקות רקע ומהימנות:** הספק מתחייב לבצע בדיקות מהימנות קפדניות לעובדיו בטרם שיבוצם לפרויקט, לרבות בדיקת העדר עבר פלילי (בהתאם למגבלות החוק) ובדיקת המלצות. המזמין שומר לעצמו את הזכות לדרוש ביצוע סיווג ביטחוני לרמות שונות (2-6) כתנאי לגישה למידע.
- 1.5. **הרחקת עובד:** המזמין רשאי לדרוש את הרחקתו של כל עובד ספק מהפרויקט, מסיבות של אבטחת מידע או חוסר התאמה, והספק יחליפו לאלתר בעובד מתאים אחר.

2. ביטחון פיזי, בקרת כניסה והתנהלות במתקן:

- 2.1. **בקרת כניסה למתקן:** הספק מאשר כי ידוע לו שהכניסה למתקני המזמין מבוקרת באמצעות אמצעי בקרת הכניסה הקיימים במתקן. עובדי הספק יכנסו למתקן בהתאם להרשאות שניתנו להם ולהנחיות המזמין בלבד.
- 2.2. **ליווי ותנועה:** תנועת עובדי הספק במתקן תיעשה בהתאם להנחיות המזמין ובאזורים הנדרשים - בליווי נציג המזמין. חל איסור על כניסה לאזורים שאינם נדרשים לצורך ביצוע העבודה או שלא ניתנה לגביהם הרשאה מפורשת.
- 2.3. **שמירה על אמצעי בקרת הכניסה:** חל איסור להעביר, לשותף או לחשוף קוד כניסה, מפתח או כל אמצעי גישה אחר שנמסר לעובדי הספק. כמו כן, אין לאפשר כניסה של אדם אחר באמצעות הרשאה שניתנה לעובד הספק.
- 2.4. **דיווח על אובדן או חשיפה:** במקרה של אובדן אמצעי גישה או חשיפתו לגורם שאינו מורשה, ידווח הספק לנציג המזמין באופן מיידי עם גילוי האירוע.

3. אבטחת גישה לוגית, ציוד קצה ועבודה מרחוק בסביבת המזמין:

- הוראות סעיף זה יחולו בכל מקרה בו מוענקת לספק ו/או למי מטעמו גישה לוגית מסיבה כלשהיא למערכות המחשוב, ליישומים או לנכסי המידע של המזמין (בין אם מרחוק ובין אם מחצרי המזמין). יובהר כי עמידה בדרישות סעיף זה הנה מצטברת ואינה גורעת מכל התחייבות אחרת של הספק בהסכם זה, ובפרט מחובותיו בכל הנוגע להגנה על מידע עסקי/אישי רגיש המועבר להחזקתו או לעיבודו כמפורט בפרקים הבאים.
- 3.1. **כפיפות לנהלי הרשות:** עם קבלת הרשאות גישה לסביבת המזמין, יחולו על עובד הספק מלוא נהלי אבטחת המידע של המזמין, ועליו לפנות באופן יזום למנהל מטעם המזמין לקבלתם ולהטמעתם. בנוסף, העובד ישתלב במערך המודעות הארגוני (בהתאם לרמת החשיפה והנחיות ממונה אבטחת

- המידע), לרבות ביצוע לומדות, מעבר הדרכות והשתתפות בסימולציות Phishing הנערכות על ידי המזמין, כתנאי להמשך הגישה.
- 3.2 **תקינות ציוד קצה** : במידה והגישה לסביבת המזמין תתבצע באמצעות ציוד מחשב של הספק (מחשב נייד/נייח חיצוני), הספק מתחייב כי הציוד יעמוד בדרישות האבטחה של המזמין. המזמין רשאי לבצע בדיקת תקינות ("Sanity Check") לציוד כתנאי לחיבור.
- 3.3 **עבודה בסביבה מבודדת ומניעת זליגת מידע (DLP)** : העבודה בסביבת המזמין תתבצע אך ורק בתוך "סביבת העבודה" שהוגדרה (החלון המרוחק, הדפדפן המאובטח או ממשק הענן). חל איסור מוחלט לבצע העתקה של קבצים, נתונים או מידע מתוך סביבת המזמין אל המחשב המקומי של הספק. איסור זה כולל שימוש בפונקציות "גזור-הדבק" (Clipboard) החוצה, צילומי מסך לשמירה מקומית, הורדת קבצים מהענן למחשב האישי, או יצוא קבצים לתיבות דואר פרטיות.
- 3.4 **איסור שימוש בכלי בינה מלאכותית (AI)** : חל איסור מוחלט להזין ו/או להעלות מידע עסקי ארגוני, קוד מקור או מידע אישי ו/או מידע בעל רגישות מיוחדת לכלי AI פתוחים. שימוש בכלי AI יותר אך ורק באישור מראש ובכתב מממונה אבטחת המידע (לרבות במעמד ההתקשרות ציון כלי AI אשר עומדים ב-GDPR).
- 3.5 **ניהול משתמשים** : הגישה לחצרות המזמין תינתן באמצעות שם משתמש אישי בלבד. חל איסור מוחלט על שימוש בסיסמאות משותפות או העברת פרטי הזדהות.
- 3.6 **הסכמה לניטור** : הספק מצהיר כי הוא ועובדיו מודעים לכך שכל הפעולות המבוצעות בתשתיות המזמין (לרבות תעבורת רשת, דואר אלקטרוני, קבצים, גישה למאגרים ופעילות בענן) מתועדות ומנוטרות באופן שוטף ע"י מערכות האבטחה.
- 3.7 **חובת דיווח מיידית** : הספק מתחייב להודיע למזמין באופן מידי וללא דיחוי (ולכל המאוחר תוך 24 שעות) על כל מקרה של סיום העסקת עובד בעל הרשאות גישה לסביבת המזמין, או על כל הפסקת עבודה זמנית ממושכת (כגון : חל"ת, חופשת לידה, מילואים ממושכים, השעיה או חופשה העולה על 30 יום), וזאת לצורך הקפאה או חסימה של הרשאות הגישה לאלתר.
- 3.8 **חובת דיווח על שינוי תפקיד** : כמו כן, ידווח הספק מיידית על כל שינוי בתפקיד העובד הגורע את הצורך בגישה למערכות המזמין או לחלקן.
- 3.9 **חובת דיווח מיוחדת בגין עבירות משמעת וטוהר מידות** : על אף האמור בסעיף לעיל, במקרה בו סיום ההעסקה (או השעיית העובד) נובע מנסיבות של חשד לעבירת משמעת, אי-סדרים, עבירה פלילית, מעילה באמון, גניבה, הונאה או עבירת מחשב, מתחייב הספק לדווח על כך באופן ישיר, מידי ודיסקרטי לגורם המזמין או לממונה אבטחת המידע (בנוסף לדיווח התפעולי). הדיווח יכלול את פרטי החשד או האירוע, וזאת על מנת לאפשר למזמין לבצע בחינה של פעולות העובד במערכות, ניטור לאחור (Forensics), שלילת דליפת מידע ובקרת נזקים.

4. זכות הביקורת והפיקוח (Audit Rights):

- 4.1 המזמין שומר לעצמו את הזכות לבצע ביקורת (Audit) על נכונות הצהרות הספק, על אופן שמירת המידע ועל עמידתו בכל דרישות נספח זה (לרבות דרישות פרקים ב' ו-ג', ככל שסומנו כרלוונטיים).
- 4.2 הביקורת תוכל להתבצע באמצעות דרישת מסמכים, שאלונים, ראיות לוגיות (Logs/Screenshots), או באמצעות ביקורת פיזית בחצרי הספק, בתיאום סביר מראש.

4.3. על הספק לשתף פעולה באופן מלא עם הביקורת ולהעמיד לרשות המזמין או מי מטעמו את כל המידע והגישה הנדרשים לצורך אימות עמידתו בדרישות האבטחה.

5. שינויים מהותיים וחובת דיווח:

- 5.1. הספק מתחייב לשמור על רמת האבטחה והתאימות (Compliance) לאורך כל תקופת ההתקשרות.
- 5.2. הספק יודיע לממונה אבטחת המידע של המזמין באופן מיידי ובכתב על כל שינוי מהותי העלול להשפיע על רמת אבטחת המידע, לרבות:
- 5.2.1. שינוי בארכיטקטורת המערכת או במיקום שמירת הנתונים (Data Residency).
- 5.2.2. אירוע סייבר משמעותי שפגע בתשתיות הספק (גם אם לא דלף מידע של המזמין באופן ישיר, אך קיים חשש לזליגה רוחבית).

6. קבלני משנה (Sub-contractors):

- 6.1. חל איסור על הספק להעביר מידע של המזמין, לאפשר גישה למערכות המזמין, או להעביר את ביצוע השירותים הקריטיים לידי צד שלישי (קבלן משנה), ללא קבלת אישור המזמין מראש ובכתב.
- 6.2. ניתן האישור כאמור, אחריותו של הספק כלפי המזמין תהיה מלאה ומוחלטת גם בגין מעשיו או מחדליו של קבלן המשנה. הספק מתחייב להחתים את קבלן המשנה על הסכם הכולל את מלוא דרישות אבטחת המידע המפורטות בנספח זה ("Back-to-Back").

7. סיום התקשרות והשמדת מידע:

- 7.1. עם סיום ההתקשרות מכל סיבה שהיא, או על פי דרישת המזמין בכל עת, **מתחייב הספק:**
- 7.1.1. להשיב למזמין כל מידע, נכס, ציוד או הרשאה שנמסרו לו.
- 7.1.2. לבצע מחיקה מוחלטת (Sanitization) של כל המידע והנתונים של המזמין מכלל מערכותיו, שרתיו וגיבוייו, באופן שלא ניתן יהיה לשחזרם.
- 7.2. כתנאי לסיום ההתקשרות וגמר חשבון, הספק ימציא למזמין "הצהרת מחיקת מידע" חתומה על ידי מורשה חתימה, המאשרת כי לא נותר בידיו (או בידי קבלני המשנה שלו) כל שריד למידע של המזמין.

8. הפרה וסעדים:

- 8.1. מוסכם כי עמידה בהוראות נספח זה (על כל פרקיו הרלוונטיים) הינה תנאי יסודי בהתקשרות.
- 8.2. אי-עמידה בדרישות האבטחה, אי-תיקון ליקויים בלוח הזמנים שהוגדר, מסירת מידע כוזב בשאלונים או הפרת חובת הסודיות, ייחשבו כהפרה יסודית של ההסכם ויקנו למזמין את הזכות לבטל את ההתקשרות לאלתר, וזאת מבלי לגרוע מכל סעד אחר העומד לו על פי דין או על פי ההסכם הראשי.

חתימת הספק:

אני הח"מ מצהיר כי קראתי את נספח אבטחת המידע, הבנתי את תוכנו, ואני מתחייב לפעול על פיו ולהנחות את עובדיי בהתאם לדרישות נספח זה.

שם הספק: _____ ח.פ: _____ שם החותם: _____

חתימה וחותמת: _____ תאריך: _____

נספח א': כתב התחייבות עובד/קבלן משנה - בעת גישה למערכות, מידע ומתקנים

בחצרות המזמין

אני הח"מ: _____ ת"ז: _____

עובד בחברת: _____ (להלן "הספק") מועמד לעסוק בתפקיד: _____

מבקש לקבל הרשאת כניסה למתקני הארגון ו/או גישה למערכות המידע שלו (להלן: "הרשות"), ומתחייב בזאת באופן בלתי חוזר כדלקמן:

- 1. הגדרות והבנת מהות המידע:** הובהר לי כי במסגרת עבודתי אני עשוי להיחשף למידע רגיש ביותר, לרבות "מידע אישי" ו/או "מידע בעל רגישות מיוחדת" כהגדרתו בחוק הגנת הפרטיות ועליו לציית להוראות ותקנות הגנת הפרטיות לרבות שמירת סודיות מוחלטת. כמו כן, ידוע לי כי חובת הסודיות חלה גם על "מידע אגבי" - דברים שראיתי או שמעתי במקרה (שיחות מסדרון, מסכים של אחרים, זהות מבקרים במשרד וכד').
- 2. שמירת סודיות ופרטיות:** אני מתחייב לשמור בסודיות מוחלטת כל מידע שאליו איחשף. לא אעתיק, לא אצלם, לא אדפיס ולא אעביר מידע זה לשום גורם (לרבות בני משפחה, חברים או עמיתים לעבודה שאינם מוסמכים). אני מתחייב לגשת אך ורק למידע שחיוני לביצוע המשימה שלי. חל איסור מוחלט לבצע שאילתות או לחפש מידע על מכרים, שכנים, בני משפחה או אישיות ציבורית מתוך סקרנות.
- 3. אבטחת מידע וסייבר:** במידה ונדרשתי במסגרת עבודתי לעבוד בסביבת הארגון, אני מתחייב לעבוד אך ורק בתוך סביבת העבודה שהוקצתה לי (VDI, Citrix), מחשב משרדי או ענן מנוהל. חל איסור מוחלט לשמור קבצים של הרשות על המחשב האישי שלי (או על הלפטופ של הספק). חל איסור מוחלט לשלוח חומרים מהעבודה לתיבת המייל הפרטית שלי (Gmail/Walla וכו') או לשירותי ענן חיצוניים (Google Drive/Dropbox פרטיים). לא אבצע צילומי מסך (Screenshots) ולא אשתמש אעתיק או אשתמש במניפולציות דומות כדי להוציא מידע החוצה. במידה ואני מתחבר מרחוק, אני מצהיר כי המחשב שלי מוגן (מערכת הפעלה חוקית ומעודכנת, אנטי-וירוס פעיל), ואין בו תוכנות פיראטיות או תוכנות שיתוף קבצים. הסיסמה שנמסרה לי היא אישית. לא אעביר אותה לאף אדם (גם לא למנהליי) ולא אאפשר לאף אדם לעבוד על היוזר שלי. אני מתחייב שלא להשתמש בכלי בינה מלאכותית לצורך ביצוע עבודתי. ידוע לי כי חל איסור מוחלט להזין, להעתיק או לטעון לכלי AI כלשהו קוד תוכנה, מסמכים פנימיים, נתונים אישיים או לבצע שאילתות מזהות על מידע ארגוני. אני מצהיר כי ידוע לי שאני כפוף לנהלי אבטחת המידע הארגוניים, ועלי לפנות לממונה עליי לקבלתם. כמו כן, אני מתחייב לשתף פעולה עם מערך המודעות של הרשות, לרבות: ביצוע לומדות, מעבר מבחני ידע, והשתתפות בתרגילי פישג ככל שיידרש ממני.
- 4. ביטחון פיזי ונוהלי התנהגות במתקן:** אני מתחייב להישמע להוראות הביטחון הארגוניות. אני מתחייב שלא לפתוח דלתות עבור אנשים אחרים ולא לאפשר לאף אדם להיכנס אחריי, גם אם הם נראים כעובדים מוכרים, אלא אם קיבלתי אישור מפורש. לא איכנס לאזורים שלא הוגדרו לי, ובמידת הצורך אמתין לליווי או לאישור הגורם המזמין.

5. **מניעת חשיפה** : חל איסור מוחלט לצלם, להקליט או לתעד כל דבר בתוך מתקני הרשות (בטלפון נייד או בכל אמצעי אחר). אני מתחייב שלא לפרסם שום פרט על המתרחש ברשות חברתיות או שיתוף חוויות על דברים שראיתי או שמעתי במסגרת שהותי (ויכוחים, אירועים, אישים שביקרו).
6. **הסכמה לניטור** : אני מצהיר כי הובא לידיעתי שכל הפעולות שאבצע במערכות המחשוב שהוקצו לי ע"י הרשות (כולל גלישה באינטרנט, תכתובות מייל, גישה לקבצים) ובמתקני הרשות, מנוטרות, נרשמות ונשמרות לצרכי אבטחת מידע. אני נותן בזאת את הסכמתי המלאה לביצוע ניטור זה ומוותר על כל טענה לפגיעה בפרטיות בהקשר זה.
7. **חובת דיווח וסיום עבודה** : אני מתחייב לדווח מיידית לגורם המזמין על : אובדן תג/סיסמה, חשד לאירוע אבטחה, או אם הבחנתי באדם חשוד. עם סיום עבודתי או יציאה לחופשה ממושכת, אדווח על כך ואחזיר כל אמצעי גישה שנמסר לי.
8. **סנקציות והצהרה משפטית** : ידוע לי כי הפרת התחייבות זו עלולה להוות עבירה על חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו, ועל חוק העונשין, ועלולה לחשוף אותי לתביעות אזרחיות, הליכים פליליים והרחקה לצמיתות ממתן שירותים לרשות.

ולראיה באתי על החתום:

שם פרטי ומשפחה: _____ חתימה: _____ תאריך: _____

פרק ב': דרישות הגנה בסייבר:

פרק זה חל על ספקים המספקים פתרונות טכנולוגיים, תוכנה, ענן, או בעלי קישוריות לרשת המזמין

1. עמידה במתודולוגיית מערך הסייבר הלאומי:

1.1. שאלון הספק: הספק נדרש למלא את "שאלון שרשרת אספקה 1.4" של מערך הסייבר הלאומי.

המענה יתייחס למודולים הרלוונטיים לאופי השירות כדלהלן:

☐ דרישות רוחביות ☐ מערכת עננית ☐ פיתוח תוכנה

☐ גישה מרחוק ☐ אחסון אתרים ☐ אבטחת OT ☐ אבטחת AI

1.2. רמת סיכון: המענה על הבקורות יהיה לפי רמת הסיכון:

☐ רמה 1 - דרישות ליבה.

☒ רמה 2 - ספקים בעלי זיקה למידע/מערכות.

☐ רמה 3 - ספקים קריטיים עם פוטנציאל נזק גבוה.

1.3. אופן ההוכחה הנדרש:

☐ הסמכה חיצונית: תעודת הסמכה ע"י גוף מוסמך לשרשרת אספקה 1.4 של מס"ל.

☐ בודק ספקים מוסמך: הצגת אישור חתום ע"י בודק ספקים מוסמך מטעם מס"ל.

☒ הצהרה עצמית: חתימת מורשה חתימה של הספק על עמידה במתודה + צירוף שאלון:

- על הספק להציג ראיות תומכות לשאלון על פי דרישתו של המזמין (צילומי מסך מהגדרות המערכת, נהלי אבטחת מידע בתוקף, פלטי מערכות ניטור וכד').

- המזמין שומר לעצמו את הזכות לדרוש ביצוע בדיקת אימות (Validation) בהתאם לצורך.

1.4. ביקורת ובקרה (Audit Rights):

1.4.1. המזמין שומר לעצמו את הזכות לבצע ביקורת אימות (Audit) על נכונות הצהרות הספק ורמת

עמידתו בדרישות המפורטות בשאלון. הביקורת תתבצע באופן עיתי, לכל הפחות אחת לשנה, או בכל מועד אחר בהתאם לשיקול דעתו הבלעדי של המזמין (למשל: בעת חשד לאירוע סייבר או שינוי מהותי בשירות).

1.4.2. על הספק לשתף פעולה באופן מלא עם הביקורת, לרבות העברת מסמכים, לוגים וגישה לגורמי המקצוע מטעמו, בתוך פרק זמן סביר שיוגדר ע"י המזמין.

1.5. סנקציות וסיום התקשרות:

1.5.1. יובהר כי עמידה בדרישות הסייבר המפורטות לעיל הינה תנאי יסודי בהתקשרות. אי-עמידה

ביעדי תוכנית תיקון הליקויים (GAP Analysis), ירידה בציון הנדרש ללא דיווח, או גילוי כי ניתנה הצהרת כוזב/מידע שגוי במסגרת השאלון, ייחשבו כהפרה יסודית של הסכם זה.

1.5.2. במקרים אלו, יהיה המזמין רשאי לנקוט בכל האמצעים העומדים לרשותו, לרבות סיום ההתקשרות לאלתר וללא כל פיצוי לספק.

2. עמידה בתקנים והסמכות:

2.1. על הספק להציג אסמכתאות בתוקף עבור התקנים שסומנו בטבלה זו.

נדרש?	התקן/מסגרת	האסמכתא הנדרשת	למה זה מיועד?
☒	ISO/IEC 27001: 2022	תעודת הסמכה ע"י גוף מוסמך + דו"ח הסמכה	תקן הבסיס הבינלאומי לניהול מערכת אבטחת מידע (ISMS) וניהול סיכונים סדור בארגון.
☐	SOC 2 Type II	דו"ח ביקורת חתום ע"י משרד ר"ח או מוסד מוסמך ומוכר.	אימות חיצוני לאפקטיביות התפעולית של בקורות האבטחה, הזמינות והסודיות לאורך זמן
☐	ISO 22301: 2019	תעודת הסמכה ע"י גוף מוסמך + דו"ח הסמכה	תקן המבטיח את מוכנות להתאוששות מאסון (DR) ושמירה על רציפות תפעולית (BCP) בעת משבר.
☐	PCI-DSS	תעודת תאימות (AOC) חתומה ע"י מעריך מוסמך *לא ניתן להסתפק בהצהרה Service Provider רמה 1.	תקן מחייב לאבטחת נתונים עבור ספקים המעבדים, מאחסנים או מעבירים פרטי כרטיסי אשראי.
☐	ISO/IEC 27017: 2015	תעודת הסמכה ע"י גוף מוסמך + דו"ח הסמכה	הרחבה ייעודית לתקן 27001 הכוללת בקורות אבטחה מתקדמות לסביבות ענן (SaaS/IaaS/PaaS).
☐	ISO/IEC 27701: 2019	תעודת הסמכה ע"י גוף מוסמך + דו"ח הסמכה	תקן לניהול הגנת הפרטיות (PIMS) ומידע אישי (PII), המבטיח עמידה בסטנדרטים בינלאומיים
☐	[ריק לבחירה משתנה CIS, NIST וכד']	דו"ח בדיקה של יועץ חיצוני בלתי תלוי / דו"ח הצהרה עצמית לצד חתימת מורשה	[תיאור מהות ההקשחה הנדרשת]

2.2. הלימה לתיחום השירות (Scope Validity):

2.2.1. מובהר בזאת כי האישורים וההסמכות שיוצגו ע"י הספק חייבים להיות תקפים ורלוונטיים

באופן ישיר לשירותים, למערכות, לאתרי האחסון ולתהליכי העבודה המוצעים במסגרת המכרז.

2.2.2. לא יתקבלו תעודות הסמכה כלליות של הארגון אשר תחום הכיסוי שלהן (Scope of

Certification) מחריג את המחלקה, המוצר או האתר הרלוונטיים למתן השירות למזמין.

2.2.3. באחריות הספק להוכיח כי השירות המוצע נכלל תחת הגדרת Scope בתעודה.

2.3. רציפות ההסמכה ודיווח עיתי:

2.3.1. הספק מתחייב לשמור על תוקף ההסמכות לכל אורך תקופת ההתקשרות.

2.3.2. העברה שנתית: הספק יעביר למזמין, באופן יזום אחת לשנה (או עם חידוש ההסמכה, לפי

המוקדם), את התעודות המעודכנות לצד דו"חות הביקורת.

2.4. הספק יודיע לממונה אבטחת המידע של המזמין, לא יאוחר מ2 ימי עסקים, במקרים הבאים:

2.4.1. שלילה או אי-חידוש של אחת מההסמכות הנדרשות.

2.4.2. גילוי אי התאמות מהותיות (Major Non-Conformities) במסגרת מבדקי האימות התקופתיים.

2.4.3. שינוי מהותי בScope של ההסמכה אשר גורע את השירותים הניתנים למזמין.

פרק ג': הגנת הפרטיות ועיבוד מידע (מיקור חוץ):

הוראות פרק זה מתייחסות לחובות הספק כ"מחזיק" וכ"גורם חיצוני" בהתאם לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "התקנות").

1. צמידות המטרה והגבלת השימוש (Purpose Limitation):

- 1.1 **הצהרת עיבוד:** הספק מצהיר כי יעבד ו/או יעשה שימוש במידע אך ורק למטרת מתן השירותים כפי שהוגדרו בהסכם זה, ולא לכל מטרה אחרת (לרבות שימוש מסחרי, טיוב נתונים עצמי או העברה לצד ג' לרבות מערכות בינה מלאכותית AI).
- 1.2 **בעלות המידע:** מובהר כי המידע הוא קניינו הבלעדי של המזמין. מעמדו של הספק הינו של "מחזיק" בלבד, ואין לו כל זכות קניינית במידע או בתוצריו.

2. חובות רגולטוריות שוטפות (Compliance):

הספק מתחייב לקיים את כל החובות החלות עליו כ"מחזיק" וכ"גורם חיצוני" לפי כל דין, ובפרט לפי הוראות חוק הגנת הפרטיות, התשמ"א-1981, תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "התקנות") וכן בהתאם להנחיות הרשות להגנת הפרטיות וגילויי הדעת המפורסמים על ידה מעת לעת. יובהר כי פירוט הדרישות בסעיפים המשנה להלן נועד לצרכי הדגשה ופירוט עיקרי הדברים בלבד, ואין בו כדי לגרוע מכל חובה אחרת או נוספת החלה על הספק מכוח הדין, התקנות או הנחיות הרשות להגנת הפרטיות, גם אם אינה מנויה במפורש להלן:

- 2.1 **התאמה לרמת האבטחה:** מובהר בזאת כי הספק נדרש ליישם את הוראות אבטחת המידע בהתאמה לרמת אבטחה גבוהה החלה על מאגרי המידע של המזמין נשוא ההתקשרות, כפי שמוגדר בתקנות, וכי במקרה של סתירה או אי-בהירות, תחול חובת ההחמרה.
- 2.2 **מינוי ממונה אבטחת מידע (תקנה 3):** הספק ימנה אחראי לאבטחת המידע וסייבר מטעמו, אשר יבטיח בקרה שוטפת על העמידה בדרישות החוק והתקנות.
- 2.3 **נוהל אבטחת מידע (תקנה 4):** הספק יחזיק ויעדכן באופן שוטף נהל אבטחת מידע ארגוני, הכולל הוראות ברורות לעניין הגנה פיזית ולוגית, ניהול הרשאות, ניהול אירועי אבטחה, והנחיות לשימוש בהתקנים ניידים.
- 2.4 **מיפוי מערכות, סקרים ומבדקי חדירות (תקנה 5):** הספק מתחייב להחזיק ולעדכן באופן שוטף מסמך המתאר את מבנה מאגר המידע ורשימת מצאי מעודכנת הכוללת את פירוט תשתיות החומרה, מערכות התוכנה, רכיבי התקשורת ואבטחת המידע, הממשקים (Interfaces) ותרשים רשת עדכני המתאר את הטופולוגיה ומיקומם הפיזי של הרכיבים; בנוסף, בהתאם לרמת האבטחה החלה על המאגר, הספק יבצע אחת ל-18 חודשים לפחות סקר סיכונים (Risk Assessment) ומבדק חדירות (Penetration Test) לבחינת עמידות המערכות בפני סיכונים פנימיים וחיצוניים, ידון בתוצאותיהם, יפעל לתיקון הליקויים שנתגלו ויתעד את הפעולות שנקטו.
- 2.5 **אבטחה פיזית וסביבתית (תקנה 6):** הספק ישמור את מאגרי המידע, התשתיות והמערכות במקום מוגן המונע חדירה וכניסה ללא הרשאה, ינהל בקרת כניסה ויציאה מתועדת לאתרים אלו, וינקוט אמצעים להגנה מפני נזקים פיזיים וסביבתיים.
- 2.6 **ניהול כוח אדם והדרכות (תקנה 7):**
 - 2.6.1 הספק יבצע הליכי מיון ושיבוץ לעובדים לפני מתן גישה למידע.

- 2.6.2. הספק יבצע הדרכות אבטחת מידע ופרטיות לעובדים הרלוונטיים, אחת לשנה (או אחת לשנתיים במאגרים ברמה גבוהה), ויתעד את ביצוען.
- 2.7. **ניהול הרשאות גישה (תקנה 8):** הספק ינהל את הרשאות הגישה למידע בהתאם לעקרון "הצורך לדעת" (Need to Know), יבצע בחינה תקופתית של ההרשאות, ויבטל לאלתר הרשאות של עובדים שסיימו תפקידם או שאין להם עוד צורך בגישה.
- 2.8. **זיהוי ואימות (תקנה 9):** הספק יטמיע מנגנוני הזדהות חזקים ע"פ רמת האבטחה הנדרשת בתקנות, יקבע מדיניות סיסמאות (מורכבות, תדירות החלפה), ימנע שימוש בסיסמאות ברירת מחדל ויפעיל מנגנון נעילה אוטומטי לאחר מספר ניסיונות כניסה שגויים או לאחר פרק זמן של אי פעילות.
- 2.9. **תיעוד אירועים ולוגים (תקנה 10):** הספק מתחייב לנהל רישום לוגים (Audit Logs) אוטומטי עבור כל הגישות למערכות ולמידע, ולשמור אותם לתקופה של 24 חודשים לפחות (בהתאם לתקנה 17) לצורך בקרה ותחקור.
- 2.10. **ניטור ובקרת אירועי אבטחה (תקנה 11):** הספק יפעיל מנגנונים לגילוי אירועי אבטחת מידע, יתעד כל אירוע אבטחה (לרבות חשד לאירוע), ויקיים דיונים תקופתיים להפקת לקחים ועדכון בהתאם.
- 2.11. **אבטחת תקשורת והתקנים ניידים (תקנות 12, 13, 14):**
- 2.11.1. הספק יצפין מידע רגיש המועבר ברשתות תקשורת ציבוריות.
- 2.11.2. הספק יתקין אמצעי הגנה מפני קוד זדוני (Malware) בתחנות הקצה ובשרתים.
- 2.11.3. הספק יגביל חיבור התקנים ניידים למערכות, ובמידה והשימוש בהם הכרחי – יבטיח את הצפנת המידע עליהם.
- 2.12. **גיבוי ושחזור:** הספק יבצע גיבויים סדירים של המידע, ישמור אותם באתר נפרד (Off-site) או באופן מוגן, ויבצע בדיקות תקופתיות לוודא יכולת השחזור של המידע (Restore).

3. דיווח שנתי והצהרת עמידה (Annual Accountability):

בהתאם לתקנה 15(א)(8) לתקנות, הספק יעביר לממונה הגנת הפרטיות וממונה אבטחת המידע של המזמין, אחת לשנה, דיווח בכתב המפרט את אופן עמידתו בחובות החוק. הדיווח יכלול התייחסות מפורשת לנושאים הבאים:

- 3.1. **אירועי אבטחה:** פירוט האם ב-12 החודשים האחרונים התרחש אירוע סייבר או דלף מידע אצל הספק.
- 3.2. **הליכים משפטיים:** הצהרה האם מתנהלים נגד הספק הליכי פיקוח/אכיפה מצד הרשות להגנת הפרטיות, או תביעות אזרחיות בנושאי פרטיות.
- 3.3. **ביקורות חיצוניות:** מועד ביצוע מבדק חדירות (PT) וסקר סיכונים אחרון שבוצע ע"י גורם בלתי תלוי.
- 3.4. **שינויי תשתית:** דיווח על שינויים מהותיים שבוצעו בארכיטקטורת המערכת או במיקום שמירת המידע (ענן/שרתים).

4. ניהול כוח אדם והסכמי סודיות:

- 4.1. **בדיקת נאותות:** הספק לא יעניק גישה למידע לעובד אלא לאחר שביצע הליך מיון ושיבוץ (Security Screening) המודא את התאמתו ואמינותו, בהתאם לרגישות המידע.
- 4.2. **הסכם סודיות (NDA):** הספק יחתים כל עובד או קבלן משנה מטעמו על כתב התחייבות לשמירת סודיות ואי-עשיית שימוש במידע, בנוסח התואם הוראות החוק ואת דרישות המזמין.

4.3. **סיום העסקה** : עם סיום העסקתו של עובד אצל הספק, יבטל הספק את הרשאות הגישה שלו למערכות המזמין באופן מיידי.

5. זכויות נושאי מידע (Data Subject Rights):

הספק מתחייב לסייע למזמין לקיים את חובותיו כלפי נושאי המידע לפי חוק :

- 5.1. **זכות העיון והתיקון** : הספק יאפשר למזמין (טכנית ותפעולית) לאתר, להעביר עותק, לתקן או למחוק מידע אישי של אדם הפונה למזמין, בתוך פרק זמן סביר.
- 5.2. **דיווח על פניות** : הספק יעביר למזמין ללא דיחוי כל פנייה שתתקבל אצלו ישירות מנושא מידע בנוגע למידע האישי שלו.

6. סיום התקשרות והשמדת מידע (Data Destruction):

6.1. **חובת המחיקה** : עם סיום ההתקשרות מכל סיבה שהיא, או לפי דרישת המזמין, הספק מתחייב :

- 6.1.1. להחזיר למזמין את כלל המידע שנצבר אצלו (לרבות גיבויים).
- 6.1.2. לבצע מחיקה והשמדה לצמיתות (Secure Erasure) של כל עותקי המידע ממערכותיו, שרתיו ואמצעי הגיבוי שברשותו.
- 6.2. **הצהרת השמדה** : כתנאי לגמר חשבון, הספק יעביר למזמין "אישור השמדת מידע" חתום ע"י מורשה חתימה ומנהל אבטחת המידע של הספק. האישור יכלול הצהרה מפורשת כי :
 - 6.2.1. ההשמדה בוצעה ביחס לכלל המידע (לרבות עותקים, טיוטות וגיבויים).
 - 6.2.2. ההשמדה בוצעה באופן בלתי הפיך.
 - 6.2.3. לא נותר בידי הספק שום מידע הקשור למזמין.

7. שמירה, ריבונות ומיקום המידע:

- 7.1. **Data Residency** : המידע יישמר ויעובד אך ורק על גבי שרתים הממוקמים פיזית בגבולות מדינת ישראל. העברת מידע לחו"ל (לרבות לענן ציבורי) תתאפשר רק באישור מראש ובכתב, ובכפוף לתקנות העברת מידע אל מחוץ לגבולות המדינה (הבטחת רמת הגנה נאותה / תואמת GDPR).
- 7.2. **הפרדת סביבות** : הספק מתחייב לבצע הפרדה לוגית מלאה (Tenancy Isolation) בין המידע של המזמין לבין מידע של לקוחות אחרים של הספק.

8. קבלני משנה (Sub-Processors):

- 8.1. הספק אינו רשאי להעביר את המידע לקבלן משנה או לאפשר לו גישה, אלא בכפוף לקבלת אישור מראש ובכתב מהמזמין.
- 8.2. אישר המזמין התקשרות עם קבלן משנה, יחתים הספק את קבלן המשנה על הסכם הכולל את מלוא התחייבויות אבטחת המידע שבנספח זה ("Back-to-Back").

9. דיווח על אירועי אבטחה (רגולציה):

- 9.1. במקרה של גילוי אירוע אבטחה, חשש לדליפת מידע או פגיעה בשלמותו, הספק ידווח למזמין באופן מיידי וללא דיחוי (ולכל המאוחר תוך 24 שעות).
- 9.2. הדיווח יכלול את כל הפרטים הנדרשים לפי תקנות הגנת הפרטיות. הספק יסייע למזמין בתחקור האירוע ובדיווח לרשות להגנת הפרטיות במידת הצורך.

נספח א': כתב התחייבות ספק לשמירת סודיות ואבטחת מידע:

הואיל והספק מעניק שירותים לארגון הכרוכים בגישה ו/או חשיפה למידע אישי של הארגון; והואיל והספק מתחייב להבטיח כי עובדיו ומי מטעמו ישמרו על סודיות המידע של הארגון בהתאם להוראות הסכם זה; לפיכך הוסכם והותנה בין הצדדים כדלקמן:

1. הספק מתחייב להחתים את כל עובדיו ומי מטעמו הנותנים שירותים לארגון על כתב התחייבות לשמירת סודיות ואבטחת מידע בנוסח המצורף כנספח ב' לפרק זה, וזאת כתנאי מוקדם למתן השירותים לארגון.
2. הספק מצהיר כי הובהר לו על-ידי הגורמים המוסמכים בארגון כי חלה על עובדיו ומי מטעמו החובה לשמור בסוד מוחלט כל מידע אליו ייחשפו במישרין או בעקיפין בעת מתן השירותים לארגון.
3. הספק מתחייב להביא לידיעת עובדיו ומי מטעמו כי המידע המצוי במאגרי המידע של הארגון ו/או מאגרים אחרים אשר שותפו עימם במסגרת עבודתם, הינו חסוי ומשמש לצרכי עבודה בלבד ואין לעשות בו שימוש לצרכים אישיים.
4. הספק מתחייב כי עובדיו ומי מטעמו לא יעיינו או ישלפו כל מידע ממאגרי הארגון ו/או ממאגרים אחרים אשר שותפו עימם, למטרות שאינן קשורות לעבודתם עבור הארגון, לרבות טיפול או מעורבות כלשהי בעניינם של קרובי משפחתם ומכריהם. כמו כן, לא יפרסמו ולא יוציאו מחזקתם מידע עסקי של הארגון, בין אם במישרין ובין אם בעקיפין, לכל צד שהוא, לרבות בני משפחה ועובדי מערכות הביטחון שאינם מורשים מתוקף תפקידים.
5. הספק מתחייב לוודא כי עובדיו ומי מטעמו יפעלו בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981, תקנות הגנת הפרטיות (אבטחת מידע) 2017, והוראות כל דין הנוגע לעניין.
6. הספק מתחייב כי עובדיו ומי מטעמו, לאחר סיום עבודתם עבור הארגון, מכל סיבה שהיא, לא ישאירו ברשותם כל מסמך ו/או חומר שנמסרו להם או הגיעו לרשותם בעקבות ו/או כתוצאה מעבודתם עבור הארגון, ויחזירו מיד כל מסמך, מכשיר, חפץ או חומר כאמור עם סיום עבודתם ו/או ישמידו בתיאום מראש עם הארגון כל מידע שנאסף ו/או נשאר ברשותם ושלא הועבר לרשות הארגון.
7. הספק מצהיר בזאת שידוע לו, כי אי מילוי התחייבויות עובדיו ומי מטעמו כאמור בהסכם זה מהווה עבירה על פרק ז', סימן ה, לחוק העונשין, התשל"ז-1977 וכי יהיו צפויים לעונשים הקבועים בחוק בגין אי מילוי ההתחייבויות.
8. הספק מתחייב לפקח ולוודא את עמידת עובדיו ומי מטעמו בהוראות הסכם זה ובהתחייבויותיהם לשמירת סודיות ואבטחת מידע כאמור.
9. הסכם זה אינו גורע מכל חובה החלה על הספק ועובדיו לפי כל דין או הסכם אחר בנוגע לשמירת סודיות ואבטחת מידע.

חתימת הספק:

אני הח"מ מצהיר כי קראתי את פרק ג' ונספח זה, הבנתי את תוכנו, ואני מתחייב לפעול על פיו ולהנחות את עובדיי בהתאם לדרישות פרק ונספח זה.

שם הספק: _____ ח.פ: _____ שם החותם: _____

חתימה וחותמת: _____ תאריך: _____

נספח ב': כתב התחייבות עובד הספק לשמירת סודיות ואבטחת מידע

אני הח"מ: _____ ת"ז: _____

עובד בחברת: _____ (להלן "הספק") מועמד לעסוק בתפקיד: _____

מתחייב בזאת כלפיי הארגון כדלקמן:

- הנני מצהיר כי הובהר לי על-ידי הגורמים המוסמכים בארגון כי חלה עליי החובה לשמור בסוד מוחלט כל מידע אליו איחשף במישרין או בעקיפין בעת עבודתי.
- הובא לידיעתי כי המידע המצוי במאגרי המידע של הארגון ו/או מאגרים אחרים אשר שותפו עימי במסגרת עבודתי, הינו חסוי ומשמש לצרכי עבודה בלבד ואין לעשות בו שימוש לצרכים אישיים.
- מבלי לפגוע בכלליות האמור בסעיף 1, הנני מתחייב שלא לעיין או לשלוח כל מידע ממאגרי הארגון ו/או ממאגרים אחרים אשר שותפו עימי, למטרות שאינן קשורות לעבודתי, לרבות טיפול או מעורבות כלשהי בעניינם של קרובי משפחתי ומכריי. כמו כן, לא אפרסם ולא אוציא מחזקתי מידע עסקי של הארגון, בין אם במישרין ובין אם בעקיפין, לכל צד שהוא, לרבות בני משפחה ועובדי מערכות הביטחון שאינם מורשים מתוקף תפקידים.
- הספק מתחייב לוודא כי עובדיו ומי מטעמו יפעלו בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981, תקנות הגנת הפרטיות (אבטחת מידע) 2017, והוראות כל דין הנוגע לעניין.
- אני מתחייב כי לאחר סיום עבודתי עבור הארגון, מכל סיבה שהיא, לא אשאיר ברשותי כל מסמך ו/או חומר שנמסרו לי או הגיעו לרשותי בעקבות ו/או כתוצאה מעבודתי עבור הארגון, ואחזיר מיד כל מסמך, מכשיר, חפץ או חומר כאמור עם סיום עבודתי ו/או אשמיד בתיאום מראש עם הארגון כל מידע שנאסף ו/או נשאר ברשותי ושלא הועבר לרשות הארגון.
- אני מצהיר בזאת שידוע לי, כי אי מילוי התחייבויותי הנ"ל מהווה עבירה על פרק ז', סימן ה, לחוק העונשין, התשל"ז-1977 וכי אהיה צפוי לעונשים הקבועים בחוק בגין אי מילוי ההתחייבויות.

ולראיה באתי על החתום:

שם פרטי ומשפחה: _____ חתימה: _____ תאריך: _____