

# נספח 4 להסכם - כתב התחייבות - דרישות הגנת פרטיות

## ואבטחת מידע

מבלי לגרוע מהאמור בהסכם זה, החברה מאשרת בזאת כלפי האגודה (כהגדרתה בהסכם), כי ידוע לה שבמהלך מתן שירותיה לאגודה, כמשמעותם בהסכם ("השירותים") נחשף בפניה ומגיע לידיעתה מידע אישי בעל רגישות גבוהה בנוגע לנוסעים (כהגדרתם בהסכם) של האגודה וכן מידע המהווה סוד מסחרי של האגודה ולפיכך גם מטעם זה הוא בעל רגישות גבוהה ("המידע"). המידע יכול להימסר לחברה על ידי האגודה, או מי מטעמה, או על ידי צד שלישי, או להיאסף על ידי החברה, או מי מטעמה, או להגיע לידיעת החברה בכל דרך אחרת.

ידוע לחברה כי קיימת חשיבות רבה, לרבות חוק הגנת הפרטיות, התשמ"א-1981, התקנות שהותקנו ו/או שיותקנו מכוחו לרבות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, וכן הנחיות הרשות להגנת הפרטיות, כפי שיהיו בתוקף מעת לעת ("חוק הגנת הפרטיות"), מכוח חוק עוולות מסחריות, התשנ"ט – 1999 ("חוק עוולות מסחריות"), לאבטח את המידע כראוי, לשמור עליו מפני שימוש בלתי חוקי או בלתי מורשה ולקיים לגביו סודיות מלאה ודיסקרטיות הנדרשת לשם כך.

מהטעם האמור מתחייבים יחסי אמון ברמה גבוהה בין החברה לבין האגודה. לכן, הפרת אילו מהתחייבויות החברה המפורטות בכתב התחייבות זה, המהווה עם חתימת החברה עליו חלק בלתי נפרד מההסכם, תהווה הפרה יסודית של ההסכם.

לפיכך, החברה מצהיר ומתחייב כלפי האגודה, כדלקמן -

### 1. התחייבות כללית

- 1.1. למלא ולפעול בקפדנות בהתאם לכל הוראות חוק הגנת הפרטיות, ביחס למידע אישי ומניעת שימוש שלא למטרה לשמה נשמר.
- 1.2. לאבטח את המידע ברמה ההולמת את רגישותו הגבוהה, בהתאם להוראות חוק הגנת הפרטיות ולשם הגנה על סודותיה המסחריים של האגודה בהתאם להוראות חוק עוולות מסחריות. על החברה להסתייע בבעל מקצוע מתאים, כדי ליישם התחייבות זו באופן הולם ומלא.
- 1.3. להשתמש במידע אך ורק לצורך אספקת השירותים, בהתאם למטרת ההתקשרות (כפי שהוגדרה בהסכם עם האגודה) ולא מעבר להיקף השימוש הדרוש לצורך אספקת השירותים.
- 1.4. לא לעשות כל שימוש במידע לכל צורך אחר ובכלל זה לצרכיה הפנימיים של החברה ו/או לצורך לקוחותיה.
- 1.5. לא להעביר את המידע או כל חלק ממנו לצד שלישי כלשהו, אלא בהנחיית האגודה או בעל המידע בכתב ומראש, או אם העברה כאמור נדרשת על פי דין.
- 1.6. אם במהלך אספקת השירותים תעסוק במישרין באיסוף מידע אישי הקשור בשירותיה עבור האגודה, הרי שתקיים ותקפיד הקפדה יתירה על קיום חובת ההודעה לנושאי המידע, הקבועה בחוק.
- 1.7. להימנע מאיסוף מידע או מגישה למידע בדרכים בלתי-חוקיות או תוך כדי שימוש במאגרי מידע בלתי-חוקיים.
- 1.8. ליצור הפרדה וחציצה מלאה, פיזית ולוגית, בין המידע והפעילות המבוצעת במסגרת שרותיה עבור האגודה, לבין פעילות אחרת שהיא מבצעת עבור צדדים שלישיים.
- 1.9. לדווח לאגודה מייד לאחר שנודע לה על כל מקרה של: (1) חשש לדליפת מידע ממערכות המידע שברשותה או שבעלותה; (2) שימוש בלתי מורשה במידע; או (3) שימוש בלתי חוקי במידע. כמו כן מתחייבת החברה להישמע להוראות האגודה, או מי מטעמה, ביחס לניהול האירוע במישורים הטכנולוגיים, המשפטיים, הרגולטורים והמנהלתיים וכן להמשיך לדווח לאגודה על כל דבר ועניין הקשור באירוע ובניהולו, בהתאם להנחיות ודרישות האגודה.
- 1.10. לדווח לאגודה מייד לאחר שנודע לחברה על כל תלונה שקיבלה מכל צד שלישי שהוא ועל כל פניה של רשות הגנת הפרטיות או מי מטעמה ("הרשות"), בקשר עם ניהול ועיבוד המידע

על ידה, וכן להישמע להוראות האגודה (ככל שהדין איננו אוסר זאת) ולהמשיך לדווח לאגודה על כל דבר ועניין הקשור בטיפול בתלונה או בפניית הרשות, בהתאם להנחיות ודרישות האגודה.

1.11. להפנות לאגודה כל אדם המבקש לעיין במידע, בסמוך לאחר שקיבלה את הפניה לעיון, ולאפשר את העיון במידע ככל שנדרש הדבר, רק לאחר שקיבלה את הנחיות האגודה ובהתאם להן.

1.12. להשמיד כל עותק של המידע הנמצא ברשותה - בין בסיום ההתקשרות ובין במועד אחר בהתאם להנחיות הרשות או כל הנחיה מפורשת אחרת של האגודה ביחס לעצם השמדת המידע וביחס לפרוצדורת ההשמדה. החברה תוודא שלא נשאר בידיה עותק כלשהו של המידע, לרבות על גבי מדיה נתיקה, אתרי גיבוי ושחזור מאסון, זכרונות מטמון וכיו"ב. האגודה ממליצה לחברה להסתייע באיש מקצוע הולם שידריך את החברה ויסייע לה בהליך השמדת המידע. החברה תספק לאגודה מכתב ערוך וחתום על ידה אודות השמדת המידע ואי קיום עותקים מהמידע ברשות החברה. על אף האמור לעיל, ככל שנדרש על ידי החברה לגשת למידע לאחר סיום ההתקשרות לצורך התגוננות מפני תביעות הקשורות בעיבוד המידע על ידה, תעביר החברה את המידע לשמירה באמצעים המחמירים, העומדים בכל דרישות הרשות, ובכפוף לאישורה של האגודה.

## 2. שמירת סודיות

3. מבלי לגרוע מסעיף הסודיות בהסכם זה, מתחייבת החברה:

3.1. לשמור בסודיות מלאה כל מידע שיגיע לידיה כתוצאה ממתן השירותים, ולא לעשות כל שימוש במידע אלא לפי הוראות כתב התחייבות זה.

3.2. מידע שיגיע לידיה עקב קשריה עם האגודה על פי ההסכם, לרבות מידע שיוכן על ידה אשר מתייחס לתחום העיסוק של האגודה לרבות דוחו"ת ו/או נתונים ו/או רישומים ו/או כל מידע הקשור בספקים ו/או בלקוחות קיימים ו/או פוטנציאליים, כח אדם, תורמים ו/או ו/או כל מידע הקשור בפעילותה, הינו ויהיה סודי והינו ויהיה תמיד רכושה הבלעדי של האגודה והוא ניתן לידיעתה ולשימושה של החברה אך ורק בקשר לקשריה עם האגודה על פי ההסכם.

3.3. הימצאות מידע ברשותה של החברה אינו מעניק לה כל זכויות בו (למעט זכויות שימוש מוגבלות כאמור לעיל) והיא לא תהיה רשאית לעכב מידע וכל מסמך או קובץ הכולל מידע תחת ידיה מכל סיבה שהיא.

3.4. מבלי לגרוע מכל חובה המוטלת על החברה על פי כל דין או על-פי כתב התחייבות זה, מתחייבת בזה החברה כלפי האגודה כדלקמן:

1.4.1. לשמור בסוד את המידע ולא למסרו לאחרים.

1.4.2. למנוע ממי שאיננו מורשה במפורש לכך, גישה למידע.

1.4.3. לא לעשות שימוש במידע, למעט לצרכים שלגביהם הוא נמסר לידיעתה או לחזקתה, קרי לצורך מתן השירותים לאגודה על-פי ההסכם בלבד.

3.5. למען הסר ספק מובהר כי התחייבויותיה של החברה בכתב התחייבות זה חלות גם על מידע שנמסר לה טרם חתימתה על כתב התחייבות.

3.6. התחייבויות החברה על פי נספח זה תמשכנה לחול ללא הגבלת זמן.

3.7. כתב התחייבות זה הינו מעיקרי ההסכם. הפרתו על-ידי החברה תקנה לאגודה זכות בלעדית לביטול מידי של ההסכם וזאת מבלי לפגוע בכל סעד המוקנה לאגודה ולכל צד שלישי אחר, על פי כל דין.

## 4. בעלי תפקידים המורשים בגישה למידע אישי

החברה **לא** תעניק לעובד מעובדיה גישה למידע, אלא אם: (1) נוכחה לדעת שבמילוי משימותיו הקודמות אצל החברה, העובד הפגין יושרה ושיקול דעת זהיר הנדרשים כדי למלא כיאות תפקיד הכרוך בגישה למידע בעל רגישות גבוהה; (2) קיבלה הצהרה מהעובד וביצועה בדיקה סבירה בעצמה כדי לוודא שהעובד לא היה מעורב בעבר בעבירות הקשורות בשימוש במידע אישי; (3) העובד חתם כלפי החברה על התחייבות לסודיות הכוללת דרישות לסודיות במידע שלא תפחתנה מהדרישות בכתב התחייבות זה.

לפי דרישת האגודה, החברה תפסיק לאלתר את העסקתו של עובד, אם העובד אחראי, לפי שיקול דעתה של האגודה ולמיטב הבנתה, לכשל הנוגע לשמירה או להגנה על המידע מפני שימוש בלתי מורשה, או בלתי חוקי.

## 5. הדרכה

החברה מתחייבת להדריך כל עובד מעובדיה שעשוי להיות מעורב בביצוע השירותים לאגודה, בדבר תוכנו של כתב התחייבות זה ואופן יישומו, בדגש על השימושים המותרים והאסורים במידע.

## 6. אבטחת מידע

### 5.1 מנהל אבטחת מידע

- 5.1.1 החברה תמנה "מנהל אבטחת המידע" מקרב עובדיה הבכירים שהינו בעל ההכשרה והניסיון הרלבנטיים למילוי תפקיד זה, או בעל מקצוע חיצוני מתאים, בכפוף להנחיות חוק הגנת הפרטיות ולהנחיות הרשות.
- 5.1.2 החברה תצייד את מנהל אבטחת המידע במשאבים הדרושים לו לשם מילוי תפקידו.
- 5.1.3 מנהל אבטחת המידע לא יעסוק בתפקידים ביצועיים נוספים אשר עלולים לגרום לניגוד עניינים עם תפקידו ככזה.
- 5.1.4 תחומי אחריותו של מנהל אבטחת המידע יכללו, בין היתר:
  - 5.1.4.1 אחריות כוללת לישום מדיניות אבטחת המידע בקשר עם ביצוע ההסכם.
  - 5.1.4.2 פיתוח ומעקב של ישום תוכניות לאבטחת המידע אצל החברה ובחינה של אפקטיביות מערכות אבטחת המידע של מערכות החברה.
  - 5.1.4.3 טיפול באירועים חריגים בתחום אבטחת המידע.

### 5.2 אמצעי אבטחת מידע

#### 5.2.1 זיהוי

לכל עובד בעל גישה למידע יוקצה אמצעי זיהוי אישי וייחודי שיכלול לפחות שם משתמש ייחודי וסיסמה באורך שלא יפחת משישה תווים. אמצעי זיהוי שהוקצה לעובד, לא יוקצה לעובד אחר זולתו, אף לא במועד מאוחר יותר. החברה תקיים רישום של כל זהויות המשתמשים ותפעיל אמצעי אימות לפני כל הענקת גישה למידע. זהות משתמש שלא היתה פעילה במשך שישה חודשים, תוסר ממערכות המידע, למעט זהות משתמש שנועדה אך ורק למטרות תחזוקה ותמיכה. משתמש מורשה שנסתיימה או הופסקה מעורבותו בביצוע ההסכם – תימנע באופן מוחלט המשך הגישה שלו למידע.

#### 5.2.2 אימות

עובדים מורשים יהיו רשאים לגשת למידע אישי רק לאחר שעברו הליך לאימות זהות המשתמש שהוקצה להם.

#### 5.2.3 סיסמאות

החברה תאכוף מדיניות המקטינה את הסיכון לפגיעה בסודיות הסיסמה שבשימוש עובד מורשה. סיסמאות יאוחסנו באופן מוצפן המבטיח כי הן לא תהיינה קריאות ומובנות. החברה תקבע נוהל פנימי להקצאת, הפצת ואחסון סיסמאות. סיסמאות יכילו לפחות שישה תווים, לא יכללו מחרוזות שניתן בקלות לייחס למשתמש המורשה (כדוגמת שמו, שם בני משפחתו, תאריכי הולדת וכיו"ב). החברה תחייב כל משתמש מורשה להחליף את סיסמתו לפחות אחת לכל שלושה חודשים. החברה תדריך את עובדיה המורשים על האופן בו יש לשמור על סודיות הסיסמאות. זהות משתמש תיחסם באופן אוטומטי במידה ונכשלו שישה ניסיונות אימות רצופים.

#### 5.2.4 בקרת גישה

החברה תקבע כללים למתן הרשאות למורשי הגישה כלפי רכיבים שונים במערכות המידע של החברה. כללים אלה יביאו בחשבון את המידע (לרבות מידע אישי) שצריך להיות נגיש למורשה הגישה לצורך מילוי תפקידו, את רמות הסיכון הנגזרות מתחום האחריות של כל מורשה גישה, סמכותו ההיררכית ורגישות המידע האישי המדובר. הכללים למתן הרשאות הגישה יבחנו ויאושרו באופן תקופתי ויאכפו בפועל באמצעות הענקת הרשאות מתאימות למערכות המידע. החברה תקבע קריטריונים ויישם מנגנון ניתוק (time out) לאחר פרק זמן שבו לא היתה פעילות מצד מורשה הגישה. פרק הזמן ייקבע תוך התחשבות בהערכת הסיכונים.

**מעקב** 5.2.5  
החברה תיישם מערכות שיערכו תיעוד ומעקב אחר כל גישה וניסיון גישה למידע אישי. התיעוד יכלול את זהות המשתמש שניגש (או שניסה לגשת), מועד הגישה (או הניסיון), המידע שאליו נעשתה הגישה (או ניסיון הגישה) והאם הוענקה הגישה או שניסיון הגישה נחסם. החברה תוודא כי לא ניתן לנטרל את פעולתן של מערכות תיעוד ומעקב אלה וכי הן נגישות אך ורק למנהל אבטחת המידע. המידע הנאסף ממערכות תיעוד ומעקב אלה יישמר למשך שלוש שנים לאחר קרות האירוע המתועד על-ידן. מנהל אבטחת המידע יבחן את דוחות מערכות התיעוד והמעקב מדי חודש לשם איתור תקריות ואנומליות. החברה תמסור לאגודה עם דרישתה כל מידע שנאסף באמצעות מערכות לבקרת גישה כאמור.

**גישה מרחוק** 5.2.6  
גישה מרחוק למערכות מידע לא תיעשה אלא בטכנולוגיה המשלבת זיהוי ואימות המשתמש, סודיות ושלמות הנתונים ומניעת הכחשה (non-repudiation). תוך התקשורת המשמש לגישה מרחוק יהיה מוצפן.

**קישוריות לאינטרנט** 5.2.7  
קישוריות מערכות המידע לאינטרנט תיעשה באמצעות שרת נפרד של החברה, לצורכי גלישה ודואר אלקטרוני בלבד ותוך יישום אמצעי אבטחת מידע עדכניים ככל שיידרש אך לפחות אנטי-וירוס עדכני, מסנני תוכן (content filtering), מערכת לאיתור נסיונות חדירה (IDS) ו-Firewall.

**אמצעי אחסון** 5.2.8  
אמצעי האחסון של מערכות המידע יסומנו, יתויגו וימוקמו בסביבה הנגישה רק לעובדי החברה בעלי צורך לגיטימי לכך. גישתם של עובדים אלו תתועד. החברה תקיים שיטה לתיעוד אמצעי מדיה שמתקבלים אצל החברה מאת גורם אחר כלשהו ושנמסרים מהחברה אל גורם אחר כלשהו. התיעוד יכלול בין היתר את סוג המדיה, תאריך ושעת הקבלה/המשלוח, זהות השולח והמקבל. מסירת מדיה מהחברה לגורם אחר תיעשה רק לאחר שבוצע תהליך נאות לאימות תוכנה ולוודוא העדרו של כל מידע אישי העשוי להשתתיר במדיה. מדיה המתקבלת מגורם אחר תיבדק לגילוי וירוסים. השמדת מדיה או ביעורה ייעשו בדרך המונעת את שחזור המידע שהושמד.

**גיבוי** 5.2.9  
החברה תקבע נוהל לביצוע גיבוי למידע אישי, שבו ייקבעו, בין היתר, תדירות הגיבוי, אופן ביצועו ומקום אחסנת עותק הגיבוי. החברה תפעל לפי נוהל הגיבוי כל עוד היא מחזיקה במידע.

**תקריות אבטחה** 5.2.10  
החברה תקבע נוהל לתגובה, לדיווח ולניהול תקריות אבטחה הקשורים, או קיים חשד שקשורים במידע אישי. החברה תקיים רישום לכל תקרית אבטחה שהגיעה לידיעתה, ובו יתועד מועד התקרית, זהות המדווח, זהות הנמענים של הדיווח ותוצאות התקרית. דיווח על תקרית אבטחה יימסר לאגודה בהקדם האפשרי. החברה תקבע נהלים לשחזור מידע אישי שאבד או שנפגם עקב תקרית אבטחה. נהלים אלה יחייבו תיעוד מדוקדק של פעולות השחזור שנקטו ויחייבו קבלת אישור מקדים בכתב מהאגודה לכל פעולת שחזור מידע אישי.

**סביבת פיתוח** 5.2.11  
פיתוח כלים חדשים למערכות המידע, לרבות תהליכי בדיקות לכלים חדשים, ייעשו במערכות מידע נפרדות ממערכת המידע המשמשת לתפעול ועבודה שוטפת.

**סקר בטיחות פנימי** 5.2.12

החברה תקבע ותאכוף נוהל לבחינה תקופתית של מערכות המידע, במטרה לאתר חולשות, פריצות אבטחה וכשלי אבטחה. הבחינה התקופתית לא תפחת מפעם בחצי שנה וביצועה יתועד בכתב. במידה והבחינה איתרה חולשות, פריצות אבטחה או כשלי אבטחה אחרים, החברה תערוך בהקדם האפשרי תוכנית פעולה לתיקונם ותפעל בזריזות ליישמה.

#### **5.2.13 ביקורת**

האגודה רשאית לבצע סקר ביקורת הן לנוהלי אבטחת המידע של החברה והן לאמצעי האבטחה המיושמים אצלה, לרבות בדיקת חדירות המערכות (Penetration Test). ממצאי הביקורת יסוכמו לדו"ח שיכלול המלצות לצעדים האופרטיביים הנדרשים כדי לרפא ליקויים שנמצאו (אם נמצאו). מנהל אבטחת המידע יהיה אחראי ליישום המלצות הדו"ח. מנהל אבטחת המידע יגיש לאגודה תכנית פעולה ליישום המלצות הדו"ח. בנוסף, מנהל אבטחת המידע יגיש לאגודה דו"ח המאשר שההמלצות יושמו בפועל.

#### **5.2.14 פיקוח**

החברה תמסור מעת לעת דיווחים לאגודה לפי דרישתה של האגודה, בכל דבר ועניין הנוגע לביצוע הוראות כתב התחייבות זה. החברה מתחייבת להעניק לאגודה ולכל צד שלישי מטעם האגודה, גישה לעובדי החברה לצורך תשאולם בכל דבר ועניין הנוגע לביצוע הוראות כתב התחייבות זה, וכן גישה לכל מידע המצוי במערכות המידע של החברה ולכל מסמך קשיח המצוי בידי החברה, לצורך בדיקה, עיון והעתקה של אלה – הכל, בהתאם לדרישתה של האגודה. הגישה תוענק, לפי בחירת האגודה, בנוכחות פיזית במשרדי החברה לאחר תיאום מראש עם החברה ובליוי נציגה, או בחיבור מרחוק למערכות המידע של החברה. החברה תפעל בשיתוף פעולה מלא עם האגודה, בתום-לב ובלא עיכוב, במסירת כל מידע שיידרש ובמילוי כל התחייבויותיה על-פי כתב התחייבות זה.

#### **5.2.15 תיקונים**

האגודה זכאית לדרוש מהחברה תיקונם של כל הליקויים שיתגלו בפיקוח ו/או בכל דרך אחרת והחברה מתחייבת לתקן על חשבונה את כל הליקויים כאמור ולהביא תיקונים אלה לאישורה של האגודה - הכל בתוך פרק זמן סביר שהאגודה תקבע לכך. החברה מתחייבת לשאת בעלות בדיקה חוזרת המיועדת לוודא כי הליקויים תוקנו כנדרש. למען הסר ספק, החברה מצהירה כי ידוע לה וכי היא מאשרת שבמידה והאגודה תבחר שלא לממש את זכות הפיקוח הנתונה לה לפי הוראות כתב התחייבות זה ו/או לא תמסור לה את הערותיה או דרישותיה לתיקון ליקויים בעקבות פיקוח שנעשה – לא יהיה בכך כדי לפטור את החברה ממילוי התחייבויותיה על-פי כתב התחייבות זה ו/או כדי למנוע מהאגודה כל טענה, תביעה ו/או דרישה כלפי החברה בגין אי-מילוי הוראות כתב התחייבות זה.

### **7. משך שמירת המידע וביעור**

לא יאוחר משבעה ימים מיום סיום ההסכם או פקיעתו מכל סיבה שהיא, תעביר החברה לאגודה, לפי הנחיות האגודה, עותק מלא מהמידע המצוי ברשותה כתוצאה מביצוע ההסכם. מיד לאחר קבלת אישור האגודה בכתב על העברת המידע לשביעות רצונה, החברה תשמיד את כל העותקים של המידע, לרבות מכל כונן קשיח, מכל אמצעי גיבוי ומכל מדיה דיגיטאלית. עם ביצוע ההשמדה כאמור, תמציא החברה לאגודה הצהרה ערוכה וחתומה על ידה כי ביצעה בפועל את ההשמדה, המאמת את ביצוע פעולות המחיקה, ביעור והשמדה של כל המידע.