צרופה 2 למסמך ב' – המפרט הטכני

התאמת הספק לדרישות הדין הישראלי בעניין פרטיות ואבטחת מידע

הבהרות:

1.1. המסמך רלוונטי לאספקת שירותי ענן ושירותי אבטחת רשת בלבד (להלן במסמך זה "**השירות**").

1.2. המסמך מבוסס על הוראות הדין ופרשנותו המקובלת נכון ליום כתיבתו.

1.3. מסמך זה בא להוסיף על התחייבויות הספק לפי דרישות המפרט הטכני, המכרז ההסכם על כל נספחיהם.

1.4. רק הזוכה במכרז יידרש להשלים מסמך זה כתנאי לזכייתו ובטרם יחתום התאגיד על הסכם ההתקשרות עמו.

2. המסמך בוחן את התקיימותן של ההוראות שלהלן:

2.1. **תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017** (להלן: "**תקנות אבטחת מידע**").

2.2. **תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017** (בהתאמה להנחיית רשם מאגרי מידע מספר 3/2018 תחולת תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז - 2017 על ארגונים המוסמכים לתקן ISO/IEC 27001[1]).

2.3. **תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001**.

2.4. **הנחיית רשם מאגרי מידע מספר 2/2011** - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.

3. [על המציע למלא כאן את כותרות מסמכי ספק הענן עליהם הסתמך במסגרת המענה לנספח זה, ולצרף לינקים ככל שישנם למסמכים אלה]

4. הסבר לקריאה ומילוי המסמך:

[1] על הספק להיות מוסמך תקן ISO27001 על פי תנאי המכרז.

הטור הימני כולל את ההוראה שעל ספק הענן לעמוד בה בהתאם לדין הישראלי. על המציע למלא את הטור השמאלי, כך שיכלול את המענה הרלוונטי הניתן מסמכי ספק הענן עליהם הוא מסתמך לרבות הפנייה למיקום הספציפי של המענה במסמכיו.

טבלה מס' 1: תקנה 15(א)(2) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

מענה לדרישות לפי תקנה 15(א)(2) לתקנות אבטחת מידע	
ציטוט הדין הישראלי	**התייחסות הספק: פירוט, הסבר, וצירוף מסמכים**
(א) "המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות"	
(ב) "מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן"	
(ג) "סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות"	
(ד) "משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;"	
(ה) "אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;"	

(ו) "חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה (ה);"	
(ז) "התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו;"	
(ח) "חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה;"	
ס' 15(א)(3): בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע... יפרט בנוהל האבטחה של המאגר גם את העניינים המנויים בפסקה (2)(א) עד (ה), וכן יפנה בו במפורש להסכם עם הגורם החיצוני ולנוהל האבטחה שלו;	
ס' 15(א)(4): ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה."	

טבלה מס' 2: תקנות אבטחת מידע החלות על מחזיק שהוא מוסמך תקן ISO27001

הנחיית רשם מאגרי מידע מספר 03/2018 תחולת תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 על ארגונים המוסמכים לתקן ISO/IEC27001 פוטרת ארגונים כאמור ממספר תקנות, אם אותם גופים מקיימים הוראות נוספות[2].

יישום החובות על מחזיק מוסמך ISO27001 מכוח תקנות אבטחת מידע	
הפנייה לתקנה	**התייחסות הספק: פירוט, הסבר, וצירוף מסמכים**
תקנה 1. הגדרות	לא רלוונטי
תקנה 2. מסמך הגדרות מאגר	לא חל על מחזיק לפי תקנה 19(א)
תקנה 3. ממונה על אבטחת מידע ➢ **ממונה על אבטחת מידע כפוף לנושא משרה בכירה.**	

[2] **ההוראות הנוספות**:
1. הדרכות לעובדים לפי פריט 7.2.2. לנספח לתקן [*ISO 27001*] יקויימו בתדירות של לפחות אחת לשנתיים;
2. פריט 18.1.3 לנספח לתקן יקויים באופן בו הנתונים המפורטים בו ובפרשנותו בתקן 27002 ישמרו למשך 24 חודשים;
3. פריט 18.2 לנספח לתקן יקויים כך שהליכי הביקורת הנזכרים בו יבוצעו לכל הפחות בתדירות של אחת ל – 24 חודשים.

➢ יוכן נוהל אבטחת מידע. ➢ תוכן תוכנית לבקרה שוטפת, היא תבוצע, והממצאים יילקחו בחשבון. ➢ ממונה אבטחת המידע לא יהיה בניגוד עניינים עם תפקיד נוסף שלו. ➢ יוקצו המשאבים הנדרשים לממונה אבטחת המידע.	

תקנה 4. נוהל אבטחה ➢ **(א) ייקבע נוהל אבטחת מידע מחייב.** ➢ **(ב) נוהל האבטחה המפורט הוא מסווג בהתאם לתקנה.** ➢ **(ה) הנוהל יעודכן באופן תקופתי לפי הצורך.**	

תקנה 5. מיפוי מערכות המאגר וביצוע סקר סיכונים ➢ **5(ב): מסמך מיפוי מבנה המאגר יימסר רק לבעלי הרשאה בהיקף הנדרש לביצוע תפקידיהם.** ➢ **5(ג): סקר סיכונים אחת לשמונה עשר חודשים לפחות.** ➢ **5(ד): נדרשים מבחני חדירה, אחת לשמונה עשר חודשים לפחות.**	

תקנה 9. זיהוי ואימות **במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה-** ➢ **(ב)(1) אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה**	
תקנה 10. בקרה ותיעוד גישה (ד) – (ה): ➢ **נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.** ➢ **בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.**	

תקנה 11. אירועי אבטחה **(ג) – (ד):** ➢ **יש לדון באירועי אבטחת מידע רבעונית** ➢ **יש לדווח לרשם על אירוע אבטחה חמור באופן מיידי**	
תקנה 12. התקנים ניידים **הגבלה או מניעת אפשרות לחיבור התקנים ניידים.** **אם מתאפשר חיבור התקנים ניידים, יינקטו אמצעי הגנה סבירים כגון שימוש בשיטות הצפנה מקובלות.**	
תקנה 14. אבטחת תקשורת **(ג) גישה מרחוק תהיה באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה.**	

תקנה 18. גיבוי ושחזור של נתוני אבטחה **18(א)(2): ייקבע נוהל שחזור, ובלבד שביצוע השחזור יהיה באישור מנהל המאגר**	
תקנה 19. חובות בעל מאגר חלות על מנהל מאגר ומחזיק בו ותיעוד ביצוע פעולה **(ב) מי שמוטלת עליו בתקנות אלה חובה או אחריות לביצוע פעולה שאינה יצירת מסמך, נדרש לתעד באופן סביר את אופן ביצוע הפעולה לפי העניין.**	

טבלה מס׳ 3: תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס״א-2001

קיום תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה)	
תיאור הדין הישראלי	**התייחסות הספק: פירוט, הסבר, וצירוף מסמכים**
1. הגבלת העברה של מידע לחו״ל העברה אפשרית היא העברה למדינה המחילה על עצמה ומקיימת את ה-GDPR	
2. תנאים להעברת מידע לחו״ל על אף האמור בתקנה 1, רשאי בעל מאגר מידע להעביר מידע או לאפשר העברה של מידע ממאגר מידע שלו בישראל אל מחוץ לגבולותיה, אם התקיים <u>אחד</u> מאלה: ➢ (4) המידע מועבר למי שהתחייב בהסכם עם בעל מאגר המידע שממנו מועבר המידע, לקיים את התנאים לאחזקת מידע ולשימוש בו החלים על מאגר מידע בישראל, בשינויים המחויבים ➢ (8) המידע מועבר למאגר מידע במדינה – (1) שהיא צד לאמנה האירופית להגנת הפרט בקשר לעיבוד אוטומטי של מידע רגיש	

(2) המקבלת מידע ממדינות החברות בקהיליה האירופית, לפי אותם תנאי קבלה – עמידה בהוראות חוזיות Standard Contractual Clauses [3]	
תקנה 3: התחייבות להבטחת פרטיות בהעברת מידע לפי תקנה 1 או 2 יבטיח בעל מאגר המידע, בהתחייבות בכתב של מקבל המידע, כי מקבל המידע נוקט אמצעים מספיקים להבטחת פרטיותם של מי שהמידע עליהם, וכי הוא מבטיח שהמידע לא יועבר לכל אדם זולתו, בין באותה מדינה ובין במדינה אחרת.	

[3] החלטה EU/2010/87.

בנוסף לתקנות אבטחת מידע, **הנחית רשם מאגרי המידע מס' 2/2011 – שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי** מעלה דרישות מתחום הפרטיות לגבי שימוש במיקור חוץ. אלו הדרישות שנותרו לאחר כניסת תקנות אבטחת מידע לתוקף:

טבלה מס' 4: הנחיית רשם מאגרי המידע מס' 2/2011 – שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי

מענה לדרישות הפרטיות בהנחיית מיקור חוץ	
תיאור ההנחיה בישראל	**התייחסות הספק: פירוט הסבר, וצירוף מסמכים**
3.1.3.2 – במקרה בו הקבלן אוסף מידע ישירות מנושא המידע, על המזמין לוודא כי הקבלן יקיים ויקפיד הקפדה יתירה על קיום חובת ההודעה הקבועה בסעיף 11 לחוק. נוסח ההודעה ואופן קיומה צריכים להיקבע על ידי המזמין, או להיות מאושרים על ידו.	
3.1.3.3 – על המזמין לאסור במפורש על הקבלן לאסוף מידע בדרכים בלתי- חוקיות, או לעשות שימוש במאגרי מידע בלתי חוקיים.	
3.1.3.4 – על חוזה ההתקשרות עם הקבלן להכיל בטוחות, לרבות חיוב עריכת ביטוח אחריות מקצועית, סעדים וכלי בקרה אפקטיביים שיאפשרו תגובה מהירה ויעילה של המזמין להפרות של הוראות החוק והחוזה.	
3.1.3.5 - במקרים המתאימים, על המזמין לדרוש ייחוד עיסוק של הקבלן, הפרדה תאגידית בין הקבלן	

לגופים אחרים העוסקים במידע או הפרדה מבנית בתוך התאגיד הקבלן, על מנת לצמצם ככל הניתן סיכון לשימוש במידע ממאגר המידע של המזמין לצרכים אחרים של הקבלן או לקוחותיו.	
3.1.5 - זכויות נושא המידע. על המזמין לקבוע מראש הוראות ונהלים ביחס למימוש - זכויות העיון והתיקון על ידי נושא המידע, כולל התייחסות לעניין זמני תגובה, עלויות.	
3.1.7 – משך שמירת המידע, ביעור המידע	