21.6.2026

לכבוד

<u>משתתפים במכרז</u>

שלום רב,

<u>הנדון: מכרז 03/2026 לשירותי אכיפה משפטית – הודעה מס׳ 1 מענה לשאלות הבהרה</u>

<u>כללי</u>

1.1. בהתאם להוראות מסמכי המכרז מצ״ב בטבלה מסכמת שאלות ותשובות, הבהרות ושינויים.

1.2. כל התשובות, ההבהרות והשינויים האמורים במכתב זה, ייחשבו כאילו נכללו במסמכי המכרז מלכתחילה.

1.3. יובהר כי אין נוסח השאלות המפורט להלן זהה בהכרח לנוסח שנשאל על ידי המשתתפים.

1.4. אין להסתמך על כל הסבר או פירוש שניתן בעל פה או בכתב או בכל דרך אחרת על ידי מי מטעם החברה או ועדת המכרזים, ככל שניתן, בכל פורום או צורה שהיא. השינויים היחידים מהאמור במסמכי המכרז וכן כל הפירושים וההבהרות להם, הינם כמפורט במכתב זה בלבד, ובמכתבי הבהרות נוספים שיצאו מטעם התאגיד, ככל שיצאו.

1.5. בהתאם להוראות מסמכי המכרז על כל מציע להגיש כחלק מהצעתו מסמך זה חתום על ידו בעת הגשת ההצעה.

1.6. כאמור במסמכי המכרז, המועד האחרון להגשת הצעות הינו 07.07.2026 בשעה 12:00

כתובת: רח׳ בר כוכבא 2 קומה 2 מתחם העירייה החדש, אגף המסחר, לוד. מיקוד 7122302
טלפון: 1-800-800-160 | פקס: 08-9543001 | אתר: www.mei-lod.co.il

2. <u>להלן טבלת התשובות, ההבהרות והשינויים.</u>

מס"ד	עמוד	סעיף	שאלה / הבהרה	תשובת התאגיד
1	37	מסמך ה' נספח ה1 סעיף 2	סעיף 2 עוסק ב"דרישות ונהלים כלליים", ובין היתר קיימת הדרישה בעניין "תקנים", הקובעת כי: "תקנים בינלאומיים מקובלים מהווים מסגרת בסיסית לתשתית הגנת הסייבר הנדרשת אצל הספק". בנוסף, באותו חלק קיימת התייחסות לכך שביחס לספקי ענן גלובליים ניתן להסתפק בהסמכה לתקנים מקובלים כגון ISO 27001 או SOC2 **שאלת ההבהרה:** האם ניתן להכיר בהסמכת ISO 27001 של ספק אבטחת המידע המלווה את הארגון ואחראי על יישום, בקרה וליווי שוטף של מערך אבטחת המידע בארגון, בצירוף נהלי אבטחת מידע, בקרות קיימות, מערך ניטור XDR/SIEM/SOC והצהרת עמידה בבקרות רלוונטיות ובחוק הגנת הפרטיות כחלופה מספקת לדרישה להסמכת ISO עצמאית של המציע? **<u>הסבר</u>:** המציע אינו ספק ענן, ספק Hosting או ספק תשתיות, אלא ספק שירותי גבייה (פירמת עו"ד), הסמכת ISO עצמאית מלאה של המציע היא דרישה רחבה ויקרה, שאינה בהכרח מידתית לאופי השירות. תכלית הדרישה - קיום מסגרת אבטחת מידע מסודרת, מתקיימת	**התייחסות:** תקן ISO 27001 בוחן בעצם את תהליכי הליבה, משאבי האנוש, ניהול הסיכונים והאבטחה הפיזית של הארגון עצמו (משרד עורכי הדין), ולא רק של ספק ה-IT שלו. **תשובה:** מקובל לתת אפשרות לתקופת התארגנות (12-18 חודשים) להשגת הסמכת ISO 27001 למשרד. לחילופין מקובל ביצוע מבדק חוסן וסקר סיכונים על ידי גורם בלתי תלוי (כל 18 חודשים).

			באמצעות ספק אבטחת מידע מוסמך, ליווי מקצועי שוטף, נהלים, בקרות וניטור אבטחתי ובעמידה מלאה בחוק הגנת הפרטיות.	
2	37	מסמך ה' נספח ה1 סעיף 3	במסגרת סעיף 3 ישנה דרישה ל"אבטחה במישור משאבי אנוש", ובפרט קיימת דרישה לכך שהספק יבצע תהליכים מקובלים לבחינת רמת המהימנות של עובדיו, ספקי צד שלישי וספקיו. **<u>שאלת הבהרה</u>:** **האם ניתן להבהיר כי הדרישה לבדיקות מהימנות תפורש כאמצעים סבירים ומקובלים ביחס לאופי השירות, וכי ניתן יהיה להסתפק בהצהרות עובדים, הסכמי סודיות, הדרכות אבטחת מידע, בקרת הרשאות, הרשאות לפי צורך לדעת, תיעוד גישה וביטול הרשאות בסיום העסקה?** **<u>הסבר</u>:** המונח "בדיקות מהימנות" עשוי להתפרש באופן רחב מאוד ולכלול בדיקות רקע חריגות, שאינן מקובלות ואינן מידתיות ביחס לשירותי גבייה הניתנים במשרדי עו"ד. כאשר הגישה למידע מנוהלת באמצעות	**התייחסות:** תקנות אבטחת מידע (הגנת הפרטיות) מחייבות הליכי מיון הולמים לעובדים בעלי הרשאות גבוהות או גישה למידע רגיש. הסכם סודיות הוא כלי משפטי, לא כלי לאימות מהימנות. **מקובל:** ביצוע תהליך קליטה מוסדר הכולל בדיקת ממליצים מעמיקה, אימות השכלה והסמכות (כולל רישיון עריכת דין ללא דופי), החתמה על תצהיר היעדר ניגוד עניינים, והגדרת מידור מחמירה כך שגישה למידע של התאגיד תינתן רק לצוות ייעודי וקטן שאושר מראש.

			הרשאות, התחייבויות סודיות, הדרכות, ניטור ובקרות גישה, ניתן להשיג את תכלית הדרישה ללא הטלת הליכי בדיקה חריגים שאינם תואמים את אופי השירות.	
3	37	מסמך ה' נספח ה1 סעיף 4	בסעיף 4 מפורטת הדרישה ל"אבטחה פיזית וסביבתית", ובפרט הדרישה שלכל עובד יונפק כרטיס עובד אישי הכולל שם, מספר עובד ותמונה עדכנית. באותו סעיף קיימת גם דרישה לבקרת כניסה, מצלמות, אזעקות ותיעוד כניסות ויציאות. **שאלת הבהרה :** האם ניתן להכיר במערכת בקרת כניסה ביומטרית קיימת, הכוללת זיהוי אישי של העובד ותיעוד כניסות ויציאות, כחלופה מספקת לדרישת הנפקת כרטיס עובד פיזי ייעודי? **הסבר:** תכלית הדרישה לכרטיס עובד היא זיהוי אישי, מניעת כניסה של גורמים בלתי מורשים ותיעוד גישה. מערכת ביומטרית קיימת ממשת תכלית זו ואף מספקת רמת ודאות גבוהה יותר מכרטיס פיזי, שכן כרטיס ניתן להעברה, שכחה או שימוש על ידי אדם אחר. לכן אין הצדקה תפעולית או אבטחתית להוסיף הנפקת כרטיסים ייעודיים כאשר קיים מנגנון זיהוי חזק ומתועד.	מקובל

4	37	מסמך ה' נספח ה1 סעיף 4	במסגרת סעיף 4 העוסק ב"אבטחה פיזית וסביבתית", נכללות גם הדרישות ל-"מערכת לניטור ובקרת הכנסת התקנים חיצוניים" וכן "תחנות קצה ושרתים מוקשחים USB - סגור באמצעות תוכנה." **<u>שאלת הבהרה</u>:** **האם ניתן להכיר בחסימת התקני USB המיושמת כיום ברמת GPOבתחנות הרלוונטיות המעבדות מידע של המזמין, כמענה מספק לדרישה ל-USB סגור באמצעות תוכנה", גם אם לא קיימת מערכת ייעודית נפרדת לניטור ובקרת התקנים חיצוניים?** **ככל שנדרש מענה רחב יותר לניטור התקנים חיצוניים, האם ניתן להכיר בחסימת USB באמצעות GPO בצירוף בקרות משלימות כגון הגנות על ה Endpoint, ניטור XDR/SOC, בקרת הרשאות, נהלי עבודה, הדרכות עובדים ותיעוד גישה - כאמצעים מפצים מספקים ?** **<u>הסבר</u>:** פתרון ייעודי לניהול התקנים חיצוניים הוא פרויקט תשתיתי נפרד, הכולל רישוי, הטמעה, מדיניות, תחזוקה ותפעול. הדרישה עשויה להיות סבירה בסביבות בעלות רגישות גבוהה במיוחד, אך החלה גורפת שלה על כלל הארגון אינה בהכרח מידתית ביחס לשירותי הגבייה המסופקים ע"י המשרד. נכון למקד את הדרישה רק במקומות שבהם מתבצע עיבוד מידע של המזמין, או לחלופין להכיר בבקרות קיימות כאמצעים מפצים.	**תשובה:** המשרד יפעיל חסימת חיבור התקני אחסון ניידים בתחנות הקצה באמצעות מערכות ההגנה הקיימות, ופתיחתם תתאפשר פרטנית, לאחר אישור ממונה אבטחת מידע, ועבור התקנים מוצפנים בלבד. **תשובה: יש** לשלוח הוכחה כי הארגון מפעיל שירות XDR מנוהל 24/7 בשילוב SOC, המעניק זיהוי ותגובה פרואקטיבית אקטיבית ולא רק ניטור פסיבי. יש לוודא שהמערכת אוספת לוגים לא רק מתחנות קצה, אלא גם מתשתית הרשת (Firewall) ושירותי ענן.

5	39	מסמך ה' נספח ה1 סעיף 5	בסעיף 5 מפורטות הדרישות ל"אבטחת תשתיות", שבו נדרש כי יהיו ברשות הספק מערכות אבטחה בתצורת Firewall, NAC, EDR, SOC/SIEM **<u>שאלת הבהרה</u>:** **האם ניתן להבהיר כי אין חובה להטמעת מערכת NAC ייעודית, וכי ניתן לעמוד בתכלית הדרישה באמצעות בקרות חלופיות כגון חומת אש, ניהול תחנות, הגנת XDR, הקשחות בתחנה, בקרת הרשאות, הפרדת גישה למידע וניטור אירועים באמצעות SOC/SIEM מנוהל?** **<u>הסבר</u>:** NAC הוא פתרון תשתיתי רחב המתאים בעיקר לסביבות רשת מורכבות, שבהן נדרש ניהול דינמי של חיבור התקנים לרשת. הטמעת NACמלאה כרוכה בעלויות גבוהות, התאמות רשת, מתגים תומכים	**תשובה:** מקובל, במקום NAC ייעודי, ניתן ליישם הגנות ברמת הרשת והתחנות קרי, ניהול רשת אלחוטית נפרדת לאורחים (Guest WiFi), חסימת פורטים פיזיים פתוחים בעמדות ריקות/אי חיבור שלהם למתגים, אכיפת הזדהות חזקה (MFA) ו-VPN מאובטח לחיבור מרחוק, ויכולת זיהוי ציוד לא מוכר על ידי שירות ה-XDR .

			ותפעול מתמשך. ביחס לאופי השירות, תכלית הדרישה - מניעת גישה בלתי מורשית למידע - יכולה להיות מושגת באמצעות בקרות קיימות ואמצעים מפצים, ללא חיוב במערכת NAC ייעודית.	
6	40	מסמך ה' נספח ה1 סעיף 7	בסעיף 7 העוסק ב"ניהול משתמשים והרשאות" נדרשת מדיניות סיסמאות הכוללת לפחות 12 תווים, החלפה כל 3 חודשים, מורכבות סיסמה, נעילת מסך וחסימה לאחר 3 ניסיונות שגויים. בנוסף, בנספח ההתקשרות עם מחזיק במאגר מידע, סעיף 28.2, מופיעה דרישה שונה: סיסמה באורך מינימלי של 8 תווים והחלפה כל 6 חודשים. **<u>שאלת הבהרה</u>:** **לאור חוסר האחידות בין הדרישות במסמכי המכרז, האם ניתן לאשר כי מדיניות הסיסמאות תיושם בהתאם להמלצות CIS benchmark/NISTוליכולות סביבת Microsoft 365 / Entra לרבות: נעילת חשבונות, מניעת סיסמאות חלשות או פרוצות, ניטור ניסיונות גישה חריגים ומדיניות סיסמאות חזקה?** **<u>הסבר</u>:**	**התייחסות:** לפי המלצות מיקרוסופט אפשר לבטל החלפת סיסמאות יזומה, בתנאי שמופעלת הזדהות רב-שלבית (MFA/2FA). עם זאת, תקנות הגנת הפרטיות בישראל עדיין דורשות (במאגרים ברמת אבטחה בינונית/גבוהה) מורכבות והחלפה. **תשובה:** מקובל לפי חובת הזדהות רב-שלבית (MFA) מלאה לכלל המשתמשים ולכל גישה חיצונית או פנימית למידע הרגיש, בתוספת חסימת סיסמאות נפוצות

			בסביבות Microsoft מודרניות, רמת האבטחה אינה נשענת רק על החלפה תקופתית קשיחה של סיסמאות, אלא על שילוב של MFA Conditional access,מניעת סיסמאות חלשות, ניטור סיכונים ונעילות חכמות. בנוסף, קיימת אי-אחידות במסמכים עצמם בין 12 תווים / 3 חודשים לבין 8 תווים / 6 חודשים. לכן נכון לבקש שהיישום יתבצע לפי Best Practice של מסגרות עבודה נפוצות והיכולות הטכנולוגיות הקיימות.		
7	מסמך ה'	מסמך ה'	במסגרת סעיף 8 העוסק ב"גיבוי, שחזור והתאוששות", נדרשים בין היתר גיבויים יומיים, שבועיים, חודשיים ושנתיים, כאשר הגיבוי השנתי יישמר לעד"Forever" **<u>שאלת הבהרה</u>:** **האם ניתן להכיר במנגנון הגיבוי הקיים של המציע, הכולל גיבויים שוטפים, שמירה לתקופה מוגדרת, אחסון מאובטח ובדיקות שחזור תקופתיות, כמענה מספק לדרישת הגיבוי, ללא חובה לשמירת גיבוי שנתי לעד?** **<u>הסבר</u>:** דרישת גיבוי Forever היא דרישה חריגה בעלת השלכות כספיות, תפעוליות ומשפטיות. היא יוצרת עלויות אחסון גבוהות, צורך בניהול מדיות לטווח ארוך, אבטחת עותקים היסטוריים, וכן קושי אפשרי מול עקרונות מחיקת מידע וצמצום מידע בסיום התקשרות. תכלית	**התייחסות:** גיבוי יומי מיועד להתאוששות מאסון/כופרה מטווח קצר. שמירה לטווח ארוך נועדה לצורכי תחקור פורנזי או דרישות דין. **תשובה:** נדחה במערכות הגיבוי (כמו Veeam, או גיבוי בענן) קיימת אפשרות להגדיר חוק שלוקח עותק מהגיבוי היומי הקיים, ונועל אותו "כבלתי מחיק" (Immutable) פעם בשנה בענן בעלות זניחה. כמו כן שדרוג של מדיניות הגיבוי הקיימת לשמירת "Snapshot" ארוך טווח.

			הדרישה היא זמינות, שלמות ויכולת שחזור. אם מתקיים גיבוי יומי שוטף, בדיקות שחזור ושמירה מאובטחת לתקופה סבירה - יש בכך מענה מידתי ומספק.	
8	38	מסמך ה' נספח ה1 סעיף 5	בסעיף העוסק ב: "אבטחה לוגית ופיתוח מאובטח." **<u>שאלת הבהרה</u>:** **נבקש להבהיר כי דרישות פיתוח מאובטח והגנה אפליקטיבית, לרבות WAF, OWASP ,SSLDC מבדקי חדירה אפליקטיביים , CDR,בקרות URL ובקרות קלט/פלט, יחולו רק ככל שהמציע מפתח, מפעיל או מספק למזמין מערכת אפליקטיבית ייעודית, פורטל, שירות SaaS או רכיב תוכנה במסגרת השירות.** **ככל שתכולת השירות של המציע אינה כוללת פיתוח תוכנה או אספקת מערכת אפליקטיבית ייעודית למזמין, נבקש לאשר כי סעיפים אלו אינם חלים.** **<u>הסבר</u>:** דרישות אלו רלוונטיות לספקי תוכנה, פורטלים, מערכות SaaS או ספקים המפתחים ומתחזקים מערכת עבור המזמין. כאשר השירות אינו כולל פיתוח או הפעלת מערכת אפליקטיבית ייעודית, החלת הדרישות באופן גורף אינה תואמת את אופי השירות ועלולה ליצור חובות, עלויות ובדיקות שאינן רלוונטיות לתכולת ההתקשרות בפועל.	**תשובה:** מקובל המשרד מתחייב לדאוג לעדכוני תוכנה וניהול טלאי אבטחה למערכות הקיימות ברשותו.

			לסיכום, יצוין כי המציע מספק שירותים לבנקים, חברות כרטיסי אשראי, חברות ממשלתיות ורשויות מקומיות רבות, ובמסגרת התקשרויות אלו הוכרה בעבר עמידה בדרישות אבטחת מידע באמצעות מערך אבטחת מידע מנוהל ומלווה על ידי ספק אבטחת מידע המחזיק בהסמכת ISO 27001.	
9	16	מסמך ב(3) - דוגמא לאישור מקבל שירות	לגבי הדרישה בעמ' 4 סע' 4א' לצרף המלצות המוכיחות עמידה בתנאי הסף 3(א)(1) - **נודה לאישורכם כי ניתן לצרף להצעה המלצה שקיבל המציע מהמזמינה (תאגיד המים מי לוד).**	מאושר
10	8 + 17	מסמך א' הנחיות טבלת ניקוד איכות ההצעה	בשורה השלישית בטבלה שבעמ' 8 נרשם ש"אמת המידה" היא **"היקף גביה מצטבר מעבר להיקף המוגדר בתנאי סף 3א'1"**, ובנוסף נרשם בתחתית הטבלה שלצורך הוכחת ניקוד האיכות יש לצרף אישור רו"ח בהתאם לנוסח שבנספח ב(4) – **נא הבהרתכם כי לצורך הוכחת אמת מידה זו – ניתן לפרט** (באישור רו"ח – מסמך ב(4)) **נתונים – <u>אך ורק לגבי היקפי גבייה – עבור תאגידי מים וביוב, בין השנים 2022-2025.</u>**	לא מאושר. ההתייחסות לגבי היקף גבייה מצטבר הינה לגופים אשר צוינו בתנאי סף 3א'1, דהיינו לשני תאגידי מים וביוב ובנוסף ל-3 תאגידי מים וביוב / רשויות מקומיות. בנספח ב(4)
11	8 + 17	מסמך א' הנחיות טבלת ניקוד איכות ההצעה	בשורה השלישית בטבלה שבעמ' 8 נרשם ש"אמת המידה" היא **"<u>היקף גביה מצטבר</u> מעבר להיקף המוגדר בתנאי סף 3א'1"**, ובנוסף נרשם בתחתית הטבלה שלצורך הוכחת ניקוד האיכות יש לצרף אישור רו"ח בהתאם לנוסח שבנספח ב(4) – **נא הבהרתכם ואישורכם כי לצורך חישוב הניקוד שינתן לגבי הוכחת אמת מידה זו (היקפי הגבייה) – יילקח בחשבון (וניתן לפרט) סכום היקף גבייה כולל של כל התאגידים יחד - שיפורט** (באישור רו"ח –	לא מאושר. ההתייחסות לגבי היקף גבייה מצטבר הינה לגופים אשר צוינו בתנאי סף 3א'1, דהיינו לשני תאגידי מים וביוב ובנוסף ל-3 תאגידי מים וביוב / רשויות מקומיות.

			מסמך ב(4)) – **<u>המתייחס להיקף גבייה *מצטבר* למספר תאגידי מים להם נתן המציע שירותים.</u>**	
12	53	מסמך ב(2) הצעת המחיר	בעמ' 53 נדרשים המציעים להציע אחוז הנחה של עד 10% לגבי מספר קריטריונים. **נבקש אישורכם לכך שאחוז ההנחה שיוצע לא יחול לגבי 3 הרכיבים הראשונים בטבלה בעמ' 53** (פתיחת תיק, שכר טרחה שנקבע ע"י בימ"ש או הוצל"פ, ותיק שהוסדר/שולם ולא נקבע שכ"ט ע"י בימ"ש או הוצל"פ) – מהנימוקים הבאים: א. מכיוון שכפי שגם נכתב בעמ' 53 בצד הימני של הטבלה הנ"ל 3 רכיבים הנ"ל הם "על בסיס הצלחה, נגבה ישירות מהצרכן" – והגבייה הזאת היא מעבר לגביית סכום החוב עצמו, ואינה מפחית מגביית סכום החוב עצמו – שיועבר לתאגיד. ב. מכיוון ששכ"ט שנפסק ע"י בימ"ש ו/או הוצל"פ ו/או לפי כללי לשכת עורכי הדין התעריף המינימלי – הינו כבר בסכום המינימלי החוקי – ולא סביר שיופחת עוד מסכומים מינימליים אלו אחוז הנחה נוסף.	הבקשה מאושרת.
13			אבקש את הבהרתכם בעניין המכרז שבנדון כדלקמן: סעיף 3 (1) לחוברת המכרז קובע כדלקמן: בעל ניסיון במתן שירותי אכיפה משפטית)לרבות גביית חובות, ניהול תיקי הוצאה לפעול ותביעות לגביית חובות בבתי משפט, ניהול הליכי כינוס ופשיטת רגל(**לשני תאגידי מים**	הדרישה הינה לסה"כ 5 גופים המורכבים מ 2 תאגידי מים וביוב **ובנוסף** 3 תאגידי מים וביוב ו/או רשויות.

			וביוב ול- 3 תאגידי מים וביוב / רשויות מקומיות בנוסף, בהיקף גבייה מצטבר מינימלי של 4מליון ש״ח בין השנים 2022-2025 נראה כי נפלה טעות שכן מצד אחד מדובר על ניסיון במתן שירותי אכיפה משפטית לשני תאגידי מים וביוב ומצד שני ל 3 תאגידי מים וביוב /רשויות מקומיות בנוסף . נבקש את הבהרתכם מה מספר תאגידי המים הנדרש לצורך עמידה בתנאי הסף ? כמו כן נבקש את הבהרתכם האם לצורך מניין הגופים להם ניתנו שירותי אכיפה משפטית, ניתן למנות גם רשויות מקומיות (או רק תאגידי מים) .	

הודעה זו מהווה חלק בלתי נפרד ממסמכי המכרז, ועל המשתתפים במכרז להגישה, ביחד עם יתר מסמכי המכרז, כשהיא חתומה על ידם.

למעט האמור לעיל אין שינוי בהוראות מסמכי המכרז.

בכבוד רב,

מי לוד בע״מ

העתק: חברי ועדת המכרזים

כתובת: רח' בר כוכבא 2 קומה 2 מתחם העירייה החדש, אגף המסחר, לוד. מיקוד 7122302
טלפון: 1-800-800-160 | פקס: 08-9543001 | אתר: www.mei-lod.co.il