

27 אפריל 2020

**הנדון: מכרז פומבי מספר 1/20, לליווי וקיום מבדק הסמכה לתקן PCI DSS עבור משרד ראש הממשלה –  
רשות התקשוב הממשלתי**

1. בהתאם לסמכותה על פי מסמכי המכרז, לרבות סעיף 4.2 בפרק א' הליך המכרז, מתכבדת בזאת ועדת המכרזים ליתן הודעה למציעים, להלן בנספח א', בדבר שאלות שהועברו אל הועדה בכתב ותשובות ועדת המכרזים או מי מטעמה, וכן הבהרות יזומות.
2. כל ההבהרות והשינויים בהודעה זו יחשבו לחלק בלתי נפרד ממסמכי המכרז.
3. אלא אם נאמר אחרת, לכל המונחים האמורים בהודעה זו תהיה המשמעות שנקבעה להם במסמכי המכרז.
4. אין להסתמך על כל הסבר או פירוש שניתן בעל פה או בכתב או בכל דרך אחרת על ידי מי מטעם ועדת המכרזים או על ידי כל גורם אחר, ככל שניתן, בכל פורום או צורה שהיא. השינויים היחידים מהאמור במסמכי המכרז וכן כל הפירושים וההבהרות להם, הינם כמפורט בכתב זה בלבד, ובמכתבי הבהרות נוספים שיצאו מטעם ועדת המכרזים, ככל שיצאו.
5. אין בהודעה זו כדי לשנות מהוראות מסמכי המכרז, אלא ככל ששינוי כזה נעשה במפורש.

בכבוד רב,

מרכזת ועדת המכרזים

1.1. נספח אי - שאלות שהועברו אל הועדה בכתב ותשובות ועדת המכרזים או מי מטעמה

תשובות לשאלות ההבהרה	פירוט השאלה	סעיף	פרק	מס' סד'
<p>הנושא נבחן, בהתאם למצב השורר בעקבות נגיף הקורונה. אם יהיה שינוי לגב דרכי הגשת הצעות, הדבר יפורסם באתר האינטרנט של מנהל הרכש הממשלתי שכתובתו</p> <p><a href="http://www.mr.gov.il/OfficesTenders/Pages/SearchOfficeTenders.aspx">http://www.mr.gov.il/OfficesTenders/Pages/SearchOfficeTenders.aspx</a></p> <p>יש להתעדכן לפני המועד האחרון להגשת הצעות.</p>	<p>אם תיבדק מצדכם האפשרות להגשת המכרז באופן דיגיטלי</p> <p>מוצפן, שלא מצריך הגעה פיזית בשל "תקופת הקורונה" בה אנו נמצאים המגבילה התניידות ומפגשים וכן אפשרות לביצוע בידוק בטחוני בהתחברות מרחוק לשיחת וידאו?</p>	4.4	א	1.
<p>פעילויות חובה משלימות להסמכה – כגון:</p> <p>א. סריקות ASV רבעוניות</p> <p>ב. סריקות VA</p> <p>ג. מבדקי חדירות – לרשת</p> <p>ד. מבדקי חדירות – לאפליקציות</p> <p>כל פעילויות אלו מתבצעות באחריות ממשל זמין והתוצאות מוצגות לגוף המבצע את המבדק.</p> <p>הגוף הסוקר נדרש רק להנחות את ממשל זמין בפעולות הנדרשות לקבלת ההסמכה וביניהן מהן העדויות שיש להציג ומהם התיקונים שיש לבצע במקרה ונתגלו ליקויים במבדקי החדירות ובסריקות.</p>	<p>שאלה כללית בנושא פירוט השירותים - בנושא הפעילויות חובה המשלימות להסמכה - בתכולת המכרז באף פרק או נספח אין כלל התייחסות לנושא הפעילויות חובה המשלימות להסמכה ולכן לא מובן כיצד לתמחר את נושא פעילויות החובה המשלימות להסמכה (שניתן לבצען במקביל לשלבי ההסמכה) שנכללים בהן הסעיפים הבאים:</p> <ul style="list-style-type: none"> <li>• סריקות ASV רבעוניות – עפ"י התקן יש לבצע סריקות אחת לרבעון לכתובות</li> <li>מסביבת כרטיסי האשראי הנגישות מהאינטרנט- האם יש 4 סריקות ASV</li> <li>תקינות? על כמה כתובות מדובר?</li> <li>• בדיקות חדירה שנתיות תשתיות לרשת (פנימית וחיצונית) – לכמה סביבות/מערכות?</li> <li>• בדיקות חדירה שנתיות לאפליקציות המטפלות בכרטיסי אשראי בסביבת האשראי- על כמה אפליקציות מדובר?</li> </ul>	כללי	ג	2.
<p>הגוף הסוקר נדרש רק לבצע את סקר הפערים ולהנחות את ממשל זמין בתיקון הליקויים אשר התגלו במהלך הסקר – במטרה לטפל בממצאים ככל שעלו – לעמוד בדרישות התקן וכל זאת לצורך קבלת תעודת ההסמכה.</p>	<p>אין התייחסות במכרז לנושא טיפול בפערים שימצאו במהלך ההסמכה- האם נושא זה כלול בתכולת המכרז או לא?</p>	כללי	ג	3.

תשובות לשאלות ההבהרה	פירוט השאלה	סעיף	פרק	מס' סד'
<p>תשובה מפורטת לשאלה זו תימסר למציעים פוטנציאליים (אך ורק לחברות המסמיכות לעמידה בדרישות תקן PCI), לאחר חתימה על התחייבות לשמירת סודיות כמקובל ברשות התקשוב ובממשל זמין.</p> <p>התשובה תחייב את כל המציעים גם אם הגישו הצעה מבלי לבקש את התשובה המפורטת ו/או מבלי לחתום על ההתחייבות לשמירת סודיות.</p>	<p>בסעיף זה כתבתם רשימת שירותים כללית- ממעבר על הבקשה אנו רואים, שאין כלל התייחסות לסביבת האשראי הקיימת, אנו מבקשים להוסיף נספח המתאר את הסביבה הקיימת – מספר אפליקציות רלוונטיות המאחסנות, מעבדות או משדרות את נתוני בעל הכרטיס (כולל מערכות הקלטה) אופן השימוש בכרטיסי אשראי: e-commerce, עסקאות טלפוניות, POS (קריאת פס מגנטי או צ'יפ) חלוקה לאתרים גיאוגרפיים, האם קיימת סגמנטציה בין המערכות המאחסנות נתוני כרטיסי אשראי ושאר הרשת, סדר גודל של רכיבי תשתית בסביבת האשראי, האם נשמרים נתוני כרטיסי אשראי (בארגון) או שנעשה שימוש בצד שלישי לשם כך – לדוגמה פתרון טוקניזציה, (כמות וסוגי בסיסי נתונים התומכים באפליקציות אשר בתיחום ( Oracle, MS SQL, DB2) כמות שרתים המאחסנים, מעבדים או משדרים נתוני בעל הכרטיס התומכים באפליקציות שבתחום, סוגי מערכות ההפעלה של השרתים ( MS, UNIX, Linux, AS400, etc ) מספר כתובות IP נגישות מהאינטרנט, האם יש טכנולוגיית wireless בשימוש ברשת אם כן, האם נתוני כרטיסי אשראי מועברים ע"ג רכיבי wireless, האם חלק כלשהו מסביבת האשראי במיקור חוץ, האם קיים גורם צד שלישי, ספקי מיקור חוץ, או שותפים עסקיים המחוברים לרשת, האם יש לארגון סט נהלי אבטחת מידע, האם תואמים לדרישות ה- PCI, אפשר לציין במענה שלכם לשאלות שלנו שזו הסביבה הנוכחית וייתכנו שינויים בסביבה בהמשך.</p>	1.3.1	ג	4.
<p>החלפת נותן שירותים על פי דרישת המשרד יכולה להיות גם על פי הנחיה של גורמי בטחון אשר לא תמיד מנמקים את סיבותיהם לאי-התאמה בטחונית של נותן שירותים זה או אחר. בהתאם לנסיבות, המשרד ישקול את האפשרות של מתן נימוקים.</p> <p>אין שינוי למסמכי המכרז.</p>	<p>יש לשים לב לדרישת קביעות הצוות שיועמד לצורך מתן השירותים. כמו כן החלפת מי מנותני השירותים מטעם הספק תהיה כפופה לאישור המשרד. למשרד אף הזכות לדרוש את החלפת מי מנותני השירותים מטעם הספק, ללא נימוק- נשמח אם כן נוכל לקבל נימוק.</p>	2.1.3	ג	5.

תשובות לשאלות ההבהרה	פירוט השאלה	סעיף	פרק	מס' סד'
<p>אישור התאמה ביטחונית – הניתן על ידי גורמי הבטחון אשר למשרד אין שליטה עליהם - הינו תנאי לשיתוף נותן השירותים בפעילויות המבדק. על הטפסים יש לחתום לפני תחילת המבדק. תוקף אישור ההתאמה הביטחונית הינו לשנה אחת, אלא אם כן ניתנו הנחיות חדשות ואז נדרש גם לחתום על טפסים נוספים במהלך השנה. לפני המבדק העוקב יהיה צורך לחתום שוב על הטפסים במקרה והאישור הקודם אינו תקף – והדבר הינו נתון להחלטה של גורמי הבטחון אשר למשרד אין שליטה עליהם.</p>	<p>תת סעיף 4 - מה התוקף של ההתאמה הביטחונית ומה הכוונה בהתייבבות לשם חתימה על טפסים מעת לעת- על כמה פעמים בשנה מדובר?</p>	2.2	ג	.6
<p>נוכל לאשר מתן שירותים ללא צורך בנוכחות פיזית של נותני השירותים של הספק ככל שלא תהיה פגיעה באבטחת המידע (ככלל מידע יכול לעבור בשיחה טלפונית או שיחת וידאו וככל שלא תהיה פגיעה בלוחות הזמנים של המבדק עקב קשיים בקיום השיחות/מפגשים והעברת הידע מהמשרד אל הספק).</p>	<p>ביצוע השירותים – האם תהיה התחשבות ב"תקופת הקורונה" בה אנו נמצאים ותאשרו מתן שירותים ללא צורך בנוכחות פיזית או לפחות חלק מהם?</p>	2.4	ג	.7
<p>בסעיף 3.2 לפרק ג', מקום המילה "לאלתר" יבוא "תוך זמן סביר". מעבר לכך אין שינוי במסמכי המכרז</p>	<p>במקום המילה "לאלתר" האם ניתן לכתוב את המילים "תוך זמן סביר". כמו כן האם אפשר למחוק את חלקו האחרון של המשפט, המתחיל במילים "כן יהיה רשאי המשרד לעכב את התשלום" ועד למילים "המשרד לא יידרש לשלם בגין ביצוע חוזר של המשימה".</p>	3	ג	.8
<p>הסעיף יתוקן כדלקמן: "בכל מקרה שבו יחולו שינויים בהוראות הדיון, שחלים על ספקים דוגמת הספק, באופן המשפיע על ביצוע ההסכם, הוא יישא בעלויות של שינויים אלו."</p>	<p>אנו מבקשים למחוק סעיף זה.</p>	3.1.3	ד	.9

מס' סד'	פרק	סעיף	פירוט השאלה	תשובות לשאלות ההבהרה
10.	ד	4.4	האם יש להחתים את כל העובדים שיבצעו את הפעילות רק לאחר הזכייה או עם הגשת טפסי המכרז?	רק לאחר זכייה במכרז.
11.	ד	6.1	אנו מבקשים למחוק את המילים "ובמועדם לשביעות רצון המזמין".	אין שינוי למסמכי המכרז.
12.	ד	8.1	אנו מבקשים לסייג את האחריות והשיפוי לנזקים ישירים בלבד שייגרמו לחברה, בכפוף לפסק דין חלוט של רשות שיפוטית מוסמכת אשר יקבע את אחריות הספק. כמו כן, יש להוסיף בסוף הסעיף את הסייג כדלקמן: "הספק לא יהא אחראי בגין נזקים עקיפים, לרבות נזקי אובדן רווחים, חבות מוצר וכיוב'. אחריות הספק על פי הסכם זה בכל מקרה לא תעלה על סך התמורה שהתקבלה בפועל אצל הספק מהמזמין בגין השירותים נשוא ההסכם".	בסוף הסעיף ייוסף: "על אף האמור, הספק לא יהא אחראי בגין נזקים עקיפים, לרבות אובדן רווחים, או חבות מוצר."
13.	ד	11.1	למזמין הזכות להפסיק את ההתקשרות מכל סיבה שהיא בהודעה מראש של 60 ימים, מדובר בזכות חד צדדית של המזמין בלבד - האם ניתן לשנות לזכות 2 הצדדים - המזמין והספק?	אין שינוי למסמכי המכרז.
14.	ד	11.2	לתשומת ליבכם כי במקרה של אי קיומו של תקציב מאושר, תופסק ההתקשרות לאלתר.	לא ברור מה השאלה. בכל מקרה, לא ייחתם הסכם עם הספק הזוכה אלא באישור הגורמים המוסמכים.
15.	ד	11.4	לאחר המילים "בהתראה של 30 יום" אנו מבקשים להוסיף את המילים "ובלבד וההליכים המפורטים להלן לא בוטלו או הופסקו".	מקובל.
16.	ד	12.1, 12.3	במסגרת ההצעה יש לקחת בחשבון כי לא תשולם תמורה נוספת בעבור פעולות "חפיפה" עם ספק אחר-כמה זמן יש לקחת בחשבון? והאם לכלול את נושא ה"חפיפה" בהצעה?	הסעיף דורש שיתוף פעולה "בהעברת האחריות בביצוע חובותיו על פי הסכם זה". כגורם מקצועי, על הספק לדעת ולהביא בחשבון מה פרק הזמן הנדרש לצורך שיתוף הפעולה האמור. על המחיר המוצע על ידי המציע לשקף את כל העלויות. אין לציין מחיר נפרד ל"חפיפה" או לכל רכיב אחר מלבד האמור במסמכי המכרז.
17.	ד	12.2	אנו מבקשים למחוק סעיף זה	אין שינוי למסמכי המכרז.
18.	ד	13.1.1	אנו מבקשים למחוק את סעיפים 7 ו-9.	אין שינוי למסמכי המכרז.

תשובות לשאלות ההבהרה	פירוט השאלה	סעיף	פרק	מס' סד'
מאחר ועשוי להיות מחלוקת אם הפרה היא יסודית או לא, הרי שבדרך כלל מקובל שהצד הנפגע יתן התראה לצד המפר לפני ביטול חוזה. יחד עם זאת, ייתכנו מקרי קיצון שהמזמין בתור צד נפגע, ירצה או יצטרך להיזקק לבטל את החוזה לאלתר, ולכן אין שינוי למסמכי המכרז.	במקום המילים "ללא התראה נוספת" אנו מבקשים להוסיף את המילים "ובלבד שהספק לא תיקן הפרה יסודית זו תוך 14 ימים מקבלת התראה בכתב מהמזמין". במקום המילים "במכרז, בהסכם או על פי כל דין" אנו מבקשים להוסיף את המילים "בכפוף לאמור בסעיף 8.1 להסכם זה"	13.2	ד	.19
אין שינוי למסמכי המכרז.	קיימת זכות קיזוז לטובת המזמין בלבד ואשר אינה מוקנית לספק. רצוי שזכות הקיזוז תהיה הדדית או שאנא מחקו סעיף זה.	13.4	ד	.20
ככל שאין התייחסות לפיצויים מוסכמים ביתר מסמכי המכרז, הרי שהמלל כאן אינו רלבנטי ויש להתעלם ממנו.	הסעיף מתייחס לפיצויים מוסכמים, לא ברור לאיזה פיצויים הכוונה. אנו מבקשים לקבל הבהרה ובכל מקרה נושא הפיצויים המוסכמים הינו בעייתי עבורנו ולכן אנו מבקשים למחוק התייחסות זו.	13.6	ד	.21
יתווספו החריגים הבאים: מידע שהספק הוכיח כי הוא פותח על ידו באופן עצמאי, מידע שהספק הוכיח כי היה ברשותו קודם לקבלתו על ידי המשרד ושהגיע לידו ללא הפרת חובת סודיות, מידע שהתקבל מצד שלישי ללא הפרת חובת סודיות.	חסרים סייגים נוספים להגדרת מידע סודי: מידע שפותח באופן עצמאי על ידי הספק, מידע שהיה ברשות הספק קודם לקבלתו מהמשרד, מידע שהתקבל מצד שלישי.	3	נספח ג' – התחייבות לסודיות	.22

תשובות לשאלות ההבהרה	פירוט השאלה	סעיף	פרק	מס' סד'
<p>ניגוד עניינים הוא מושג שאינו ניתן בהכרח להגדרה מדוייקת ואינו בהכרח צופה את כל המצבים האפשריים. כך למשל, עלול להיות במקרה והגורם המסמיך המגיש את ההצעה קשור עם ספק אחר (גורם מסמיך אחר) המתמודד במכרז דבר העלול לפגוע בתחרות או שהוא קשור עם ספקי ציוד בדרך העלולה להשפיע לרעה על בדיקת רכיבי הציוד המרכיבים את סביבת נתוני האשראי של ממשל זמין. לשם הבנת המושג "ניגוד עניינים", ניתן להיעזר בהנחיית היועץ המשפטי לממשלה מספר 1.1555.</p>	<p>יש להביא לידיעת המזמין כל חשש לקיום ניגוד עניינים- מה הכוונה כל חשש?</p>	6	נספח ג' – התחייבות לסודיות	.23