

עיריית תל אביב-יפו
אגף טכנולוגיות ומערכות מידע

ב' חשון, תשפ"ז
13 אוקטובר, 2026

בקשה לקבלת מידע (RFI)

עיריית תל אביב-יפו (להלן: "העירייה") מעוניינת לקבל מידע בעניין מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של העירייה.

ניתן לעיין בנוסח הבקשה המלא באתר האינטרנט העירוני בכתובת <https://www.tel-aviv.gov.il> (שירותים > מכרזים ודרושים > קול קורא).

אופן הגשת מענה לבקשה זו:

1. את המענה לבקשה יש להגיש באמצעות דוא"ל hazan_t@mail.tel-aviv.gov.il עד ליום **29.10.2026 בשעה**

12:00.

2. יש לציין בנושא הודעת הדוא"ל "מענה לקבלת מידע (RFI) בעניין מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של העירייה".

העירייה תהא רשאית לפנות למשיבים לצורך קבלת הבהרות והשלמות.

עיריית תל אביב-יפו
אגף טכנולוגיות ומערכות מידע

הנדון: בקשה לקבלת מידע (R.F.I)

מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של עיריית תל אביב-יפו

1. המידע המבוקש

- 1.1. עיריית תל אביב-יפו (להלן: "העירייה") מעוניינת לקבל מידע בדבר מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של העירייה (להלן: "המערכת").
- 1.2. בקשה זו לקבלת מידע (RFI) (להלן: "הבקשה") נועדה לאפשר לעירייה לקבל מידע מספקים ו/או ממפתחים אודות מערכת קיימת כאמור, הואיל ובכוונת העירייה להתממשק עם מערכת קיימת.
- 1.3. על המעוניינים להגיש מענה לבקשה (להלן: "המשיבים") לצרף למענה מטעמים מפרט טכני של המערכת שברשותם וכן למלא את הנספחים המצורפים לבקשה, כמפורט להלן, שעניינם בעיקרם מידע בדבר יכולות המערכת, ניסיון ביישומה וכן אפשרויות פיתוחה.

2. אופן הגשת המידע

- 2.1. המשיבים רשאים לצרף מסמכים לגבי המערכת מושא הבקשה (כמו גם מתבקשים לצרף מפרט טכני, כאמור לעיל) וכן מתבקשים למלא את הנספחים שלהלן:
 - 2.1.1. נספח מס' 1 – **נתוני המשיב**.
 - 2.1.2. נספחים מס' 2א' ו-2ב' – **מידע על ניסיון המשיב**.
 - 2.1.3. נספח מס' 3 – **רשימת תכולה פונקציונלית**, בה המשיב נדרש לסמן האם התכונה/היכולת/המאפיין המנויים ברשימה קיימים/לא קיימים במערכת שברשותו, וככל שלא קיימים – לציין האם קיימת אופציית פיתוח ואת התקופה הנדרשת לכך.
- 2.2. המשיבים מתבקשים לצרף למענה מידע נוסף לצורך בחינת המערכת, ככל שישנו, ובכלל זה:
 - 2.2.1. מסמך ארכיטקטורה המתאר את מבנה המערכת והטכנולוגיות עליהן היא מבוססת.
 - 2.2.2. מסמך ה-Stack הטכנולוגי של המערכת.
 - 2.2.3. תיאור מנגנון עדכוני התוכנה וזמני ההשבתה של המערכת.
 - 2.2.4. כל מידע נוסף אשר עשוי לסייע לעירייה בהערכת המערכת.

3. פנייה להשלמת מידע ומסמכים

3. העירייה תבחן את המידע שיתקבל מהמשיבים וכן תהיה רשאית לפנות אל המשיבים, כולם או חלקם, בבקשה לקבל מהם הבהרות וכן כל מידע נוסף.

4. שאלות והבהרות בקשר לבקשה

- 4.1. שאלות ובקשות להבהרות ניתן לשלוח באמצעות דוא"ל לכתובת hazan_t@mail.tel-aviv.gov.il וזאת עד ליום **19.10.2026 בשעה 12:00**.
- 4.2. יש לציין בנושא הודעת הדוא"ל "**בקשה לקבלת מידע (R.F.I) – מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של עיריית תל אביב-יפו**".

עיריית תל אביב-יפו

אגף טכנולוגיות ומערכות מידע

4.3. העירייה תהא רשאית, על פי שיקול דעתה הבלעדי, להתייחס או שלא להתייחס לשאלות ו/או לבקשות ההבהרה.

5. אופן הגשת מענה לבקשה זו

5.1. את המענה לבקשה יש להגיש באמצעות דוא"ל hazan_t@mail.tel-aviv.gov.il עד ליום **29.10.2026**

בשעה 12:00

5.2. יש לציין בנושא הודעת הדוא"ל **"בקשה לקבלת מידע (R.F.I) – מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של עיריית תל אביב-יפו"**.

6. הוראות נוספות

6.1. מובהר בזאת כי הבקשה היא לקבלת מידע בלבד. אין להגיש הצעות כספיות במענה לבקשה. מסמכי המענה לבקשה יכללו דרישות טכניות ופונקציונליות מרכזיות של המערכת שברשות המשיב וכן פרטים ביחס למשיב.

6.2. כל האפיונים וההגדרות הטכניות המופיעים במסמכי הבקשה – חשובים, אולם אין מניעה מהגשת מענה לבקשה גם במקרה של אי עמידה בדרישה כזו או אחרת.

6.3. המידע שיתקבל בתשובה לבקשה ישמש את העירייה לצורך קבלת החלטה על אופן ביצוע ההליך/הליכים (אם בכלל) לבחירת ספק עבור קבלת השירות.

6.4. למען הסר ספק מובהר ומודגש בזאת, כי הבקשה נועדה לספק מידע ולסייע בבדיקת היתכנות וכדאיות בלבד. אין בבקשה כדי לחייב את העירייה בכל עניין שהוא, לרבות הזמנת המערכת ו/או שירותים כלשהם ו/או פרסום מכרז ו/או פרסום הליך תחרותי כלשהו ו/או לפנות למי מהמשיבים בהצעה לאספקת המערכת ו/או לאספקת שירותים כלשהם.

6.5. ככל שבעתיד תחליט העירייה לפעול לקבלת השירותים ו/או לאספקת המערכת מושא הבקשה, שומרת העירייה לעצמה את מלוא שיקול הדעת בקביעת ההליך לקבלת השירותים ו/או האספקה, תנאים, אופן ההתקשרות, התמחור וכל עניין אחר הנוגע להליך.

6.6. הגשת מענה לבקשה לא תקנה למשיבים כל יתרון או העדפה בכל הליך תחרותי אשר יפורסם ע"י העירייה, לרבות מכרז, ככל שייערך, בקשר עם רכישת המערכת ו/או ביצוע שירותים כלשהם או בכלל, ואין בהגשת מענה לבקשה כדי ליצור מחויבות כלשהי כלפי המשיבים מצד העירייה.

6.7. בהתאם לאמור, העירייה שומרת על זכותה שלא להתקשר עם חלק מהמשיבים לבקשה או עם אף לא אחד מהם, או שלא לרכוש את המערכת ו/או את השירותים מחלק מהמשיבים או מאף לא אחד מהם, או לרכוש מחברות או גופים שלא הגישו מענה לבקשה, או לצאת במכרז או לקיים כל הליך תחרותי אחר או נוסף, או להתקשר באמצעות סבב הצעות בין המשיבים או מי מהם או בין גופים נוספים או לנקוט בכל הליך אחר, והכל לפי שיקול דעתה הבלעדי ולמשיבים לא תהיה כל טענה בקשר לכך.

6.8. העירייה תבחן את המידע שיתקבל במסגרת המענה לבקשה, ולצורך זה תהא רשאית לפנות אל המשיבים, כולם או חלקם, בבקשה לקבל הבהרות ומידע נוסף, בכתב ובעל פה, ככל שיידרש. בין השאר, תשקול העירייה להזמין את המשיבים למפגש או לכנס או לפנות אליהם בשאלות בכל דרך, וללא כל מחויבות מצדה.

עיריית תל אביב-יפו

אגף טכנולוגיות ומערכות מידע

6.9. העירייה רשאית להשתמש במידע שיתקבל במענה לבקשה ללא תמורה, לכל צורך בו תחפוץ, לפי

שיקול דעתה הבלעדי, לרבות כתיבת מפרט או מסמך דרישות ולצורך הרכבת רשימת ספקים פוטנציאליים, ולהעביר את המידע ליועציה ולכל אדם הזכאי לקבלו ע"פ דין.

6.10. למען הסר ספק יובהר, כי כל ההוצאות הכרוכות במענה לבקשה תחולנה על המשיב בלבד ובשום מקרה לא יהא זכאי הוא לכל תשלום ו/או החזר ו/או פיצוי בגין ההוצאות ו/או נזקים שייגרמו לו בקשר למענה ו/או בקשר להכנת המענה ולהגשתו.

6.11. מבלי לגרוע מכלליות האמור לעיל מובהר, כי כל פרט מהפרטים המצוינים בבקשה נתון לשינוי על פי שיקול דעתה הבלעדי של העירייה ואין בו כדי לחייב את העירייה בכל דרך שהיא.

6.12. העירייה אינה מתחייבת להשתמש במידע שיתקבל או בחלקו לשם פרסום מכרז או "בקשה להצעת מחיר" או בדרך אחרת, אך תהיה רשאית לפרסם, בדרכים כאמור, פרטים אשר יתבססו על המידע אשר יצטבר כתוצאה מהליך זה.

6.13. העירייה שומרת לעצמה את הזכות המלאה והבלעדית לערוך שינויים במסמכי הבקשה, ככל שתראה לנכון, לרבות שינויים בדרישות המפורטות ודחיית המועדים למסירת מידע.

6.14. למען הסר ספק מודגש, כי בהליך זה יחול הדין הישראלי, ובית המשפט היחיד המוסמך לדון הוא ביהמ"ש המוסמך בתל אביב-יפו.

עיריית תל אביב- יפו
אגף טכנולוגיות ומערכות מידע

לכבוד
עיריית תל-אביב יפו

בקשה לקבלת מידע (RFI)
למערכת מערכת לניהול פעילויות, הדרכות, חללים, כניסות ומכירת כרטיסים למוזיאונים ולאירועים של עיריית תל אביב-יפו

נספח מס' 1 – נתוני המשיב

מס' סד'	המידע המבוקש	המענה
1.	שם המשיב	
2.	כתובת המשיב	
3.	מס' טלפון	
5.	שם איש הקשר למענה ותפקידו	
6.	מס' טלפון נייד של איש הקשר למענה	
6.	כתובת דואר האלקטרוני של איש הקשר למענה	

תאריך

חתימה וחותמת המשיב

שם המשיב

עיריית תל אביב- יפו
אגף טכנולוגיות ומערכות מידע

נספח מס' 2 – מידע על ניסיון המשיב

על המשיב לפרט את ניסיונו בכל הנוגע למערכת שברשותו, לרבות ביחס לשמות הארגונים בהם מותקנת המערכת, מספר המוקדים ביחס לכל ארגון, מספר השנים שבהן המערכת מותקנת אצל אותם ארגונים.

ניתן לצרף מסמכים תומכים, כגון הסכמים, מכתבים מלקוחות וכו'.

שם הגוף אצלו מותקנת המערכת	מספר מוקדים	מספר משתמשים	מספר השנים שבהם המערכת מותקנת	שם איש קשר בגופים בהם מותקנת המערכת	מספר הטלפון וכתובת המייל של איש הקשר

חותמת וחותימת המשיב

שם המשיב

תאריך

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

נספח מס' 3 – תכולה פונקציונלית

המשיב נדרש לסמן אם התכונה/היכולת/המאפיין קיימים/לא קיימים, וככל שקיימת אופציית פיתוח יש לציין מס' ימים נדרשים לפיתוח.

ניתן לצרף מסמכים תומכים, כגון מפרטים וכו'.

הערות	מס' ימים הנדרשים לפיתוח	האם קיימת אופציה לפיתוח	לא קיים	קיים	תכונה/יכולת/מאפיין של המערכת	
1. דרישות כלליות						
					מערכת מבוססת SAAS	1.1
					ממשק ניהול מבוסס Web	1.2
					תמיכה במובייל וטאבלט	1.3
					ממשק ניהול בשפה העברית	1.4
					המערכת בעלת יכולת שמירת נתונים היסטוריים והחצנתם תועבר למערכת Syslog לאורך כל תקופת השימוש בה ולאחריה	1.5
					למערכת יכולת שמירת לוג על פעילויות לפי הגדרת מומחה היישום בעירייה (מי ביצע, תאריך ושעה, הרכיב שאליו בוצע הגישה, סוג הגישה, היקפה, האם הגישה אושרה או נדחתה)	1.6
2. ניהול הרשאות						
					הקמת קבוצה/ות הרשאות באופן עצמאי ע"י מנהל/ת המערכת בארגון	2.1
					ניהול הרשאות לפי תפקידים כמו – קופאי, מנהל הדרכות, מנהל אתר, מנהל מתחם ועוד	2.2
3. ניהול מוצרים, אירועים וכרטיסים						
					המערכת מאפשרת יצירה וניהול אירועים (חד-פעמיים / סדרתיים – כולל תאריכי מפגשים ונושאים לכל מפגש)	3.1
					המערכת מאפשרת מכירת מגוון מוצרים וביניהם: כרטיסים, מנויים- סדרות של מפגשים, כרטיסיות (יתרה בכרטיס הלקוח שהוא יכול לנצל לסוג אירועים שהוגדר מראש), שוברי מתנה, הדרכות וסיורים, מוצרים נלווים וביניהם קטלוגים ומוצרי חנות	3.2
					המערכת מאפשרת מכירת כרטיסים ומנויים מסומנים ולא מסומנים	3.3

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

					לאירועים שונים, כולל בחירת מושבים לפי מפת אולם	
					המערכת מאפשרת הקצאת מקומות ישיבה (אולם ממוספר / אזור חופשי) וניהול מכסות וזמינות בזמן אמת	3.4
					המערכת מאפשרת הגדרת/מכירת שעות שימוש בחללים השונים (השכרה מתמשכת או שימוש מזדמן)	3.5
					המערכת מאפשרת הגדרה של סיורים, הדרכות ואירועים לקבוצות וארגונים	3.6
					המערכת מאפשרת קביעת מחירים דינמית, מדרגות מחיר והנחות. המערכת מאפשרת הגדרת סוגי מחירים לכרטיסים (רגיל, VIP, ילד, סטודנט, חייל, גמלאי, דיגיתל ועוד) וקביעת מחיר בהתאם לסטטוס הרוכש, כולל התממשקות לקבלת מידע על מאפייני הרוכש ממערכות של העירייה (כגון דיגיתל ועוד).	3.7
					המערכת מאפשרת ניהול מבצעים, קופונים והנחות	3.8
					המערכת מאפשרת הגדרת תמחור שונה לפי מיקום באולם	3.9
					המערכת מאפשרת חלוקת כרטיסי הזמנה ורישום הזמנות לאירועים ללא תשלום	3.10
					המערכת מאפשרת הקמה שוטפת של סיורים והדרכות. מאפשרת הגדרת שעות הפעילות, מספר המשתתפים המקסימלי והגדרת תקופות מכירה ותעריפי מכירה לסיורים, להדרכות ולאירועים השונים.	3.11
ניהול חללים ופעילות						4.
					ניהול מערכת שעות לפעילויות המוזיאון (קבועות ומזדמנות) וניהול תפוסת חדרים לפי תאריך ושעות.	4.1
					ניהול צוות מדריכים ושיבוצם להדרכות / חדרים	4.2
					המערכת מאפשרת הקמה וניהול של חללים (אולם, מתחם, אזור פתוח, חדר), כולל ניהול קיבולת מקסימלית, חלוקה לאזורים (יציעים, גושים, אזורי VIP וכו' (Map)), ניהול שורות ומושבים (Seat) והגדרת נגישות (מקומות לכיסאות גלגלים, אזורי נגישות).	4.3

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

					מאפשרת הקמת אולמות מסומנים ולא מסומנים.	
					ניהול סוגי פעילויות (הדרכות, השכרות, מופעים), כולל הגדרת כמות משתתפים	4.4
					ניהול והצגת סטטיסטיקות תפוסה ושימוש	4.5
תמחור, מכירות וגביית תשלומים						5.
					המערכת מנהלת מחירונים לפעילויות השונות, כולל גמישות לפי אופי הפעילות, מספר משתתפים, מפת אולם - עלות שונה לפי מושב / אזור, מאפייני הלקוח והנחות	5.1
					המערכת מנהלת מחירונים להשכרת חללים וחדרים ומאפשרת מכירת שעות שימוש בחללים השונים (השכרה מתמשכת או שימוש מזדמן)	5.2
					המערכת מאפשרת חלוקת כרטיסי הזמנה ורישום הזמנות לאירועים ללא תשלום	5.3
					המערכת מאפשרת מכירת סיורים ואירועים לקבוצות וארגונים	5.4
					ניהול גבייה ללקוחות מזדמנים וקבועים	5.5
					אפשרות להבניית קודי קופון והנחות במערך התמחור (קודים, הפניות)	5.6
					המערכת מאפשרת קביעת מחיר והנחות בהתאם לסטטוס הרוכש (רגיל, חייל, גמלאי, דיגיתל ועוד), כולל התממשקות לקבלת מידע על מאפייני הרוכש ממערכות העירייה, כגון: דיגיתל (באמצעות API).	5.7
					המערכת מנהלת ממשק סנכרון מול מועדוני לקוחות	5.8
					המערכת מאפשרת ערוצי מכירה שונים קופה, שיחת טלפון, אתר web ייעודי, קיוסקים שונים.	5.9
					המערכת מנהלת אתר web ייעודי למכירת כרטיסים אונליין, כולל עיצוב מותאם ללקוח, תמיכה במובייל, תמיכה בשפות (ובניהן עברית, אנגלית, ערבית), נגישות בהתאם להוראות הדין.	5.10
					המערכת מאפשרת הקמת חנות web ייעודית למכירת מוצרים נלווים	5.11
					המערכת תומכת באמצעי התשלום: מזומן, אשראי, אפליקציות תשלום כגון ביט, Apple Pay / Google Pay, צ'ק, העברה בנקאית ועוד	5.12

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

					5.13	המערכת תומכת בפיצול תשלומים, החזרות, ביטולים וזיכויים
					5.14	המערכת מפיקה חשבוניות/קבלות אוטומטית
					5.15	התממשקות מובנית עם מערכות גבייה: ש.ב.א., סולקי כרטיסי אשראי, אפליקציות תשלום ועוד
					5.16	התממשקות מובנית עם פינפד
6. ניהול לקוחות ואנשי קשר						
					6.1	המערכת מנהלת מאגר נתוני לקוחות, סוכנים ושותפים, הכולל מידע ממוקד, בין היתר ת.ז. כתובת דואר וכתובת דוא"ל, אלפונים, מאפיינים ייחודיים, תיוגים שיווקיים ועוד.
					6.2	המאגר יכול להכיל היסטוריית רכישות
					6.3	המערכת מזהה לקוחות חוזרים
7. כרטיסים דיגיטליים ובקרת כניסה						
					7.1	המערכת מאפשרת הפקת כרטיס דיגיטלי עם QR Code / ברקוד חד ערכי לכל כרטיס (בין אם כרטיס בודד, קבוצתי, או כרטיס סוכן)
					7.2	המערכת כוללת סריקת כרטיסים באפליקציה ייעודית לסורקים, סורקים ניידים, טלפון ועוד, ותתממשק עם מערכות לבקרת כניסה ובכלל זאת שערים אוטומטיים
					7.3	המערכת מאפשרת משלוח כרטיסים ללקוחות באמצעות הודעות SMS, WhatsApp, הודעות מייל והדפסה במקום.
					7.4	המערכת מנהלת את הכניסות בזמן אמת, כולל: זיהוי כרטיס כפול / שימוש חוזר סטטוס כניסה לכרטיס (נכנס / לא נכנס)
8. הנהלת חשבונות וניהול תקציב						
					8.1	המערכת תומכת בכל תהליכי הניהול והתפעול הנדרשים לצורך ביצוע הנהלת חשבונות וגבית התשלומים
					8.2	המערכת מאפשרת הפקת דו"חות גבייה והכנסות בחלוקה לפי סוגי פעילות, סוגי מכירה, סעיפים תקציביים ועוד
					8.3	המערכת כוללת דוחות לתמיכה בתהליכי הנהלת חשבונות כמו: דו"ח התאמות אשראי, דוחות תקבולים, פקודות יומן ועוד

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

					למערכת יכולת התממשקות עם מערכת הנהלת החשבונות של העירייה ועם מערכת הנהלת החשבונות של החברה למוסדות חינוך, באמצעות ממשקי API דו כיוונים	8.4
התממשקות עם מערכות עירוניות ואחרות						9.
					המערכת מספקת ממשקי אינטגרציה WebService דו-כיווני	9.1
					למערכת יכולת התממשקות עם מערכות אחרות באמצעות ממשקי API דו-כיוונים, לרבות מערכות עירוניות (כגון דיגיתל, אתר העירייה, מערכת ה-CRM, מערכת הנהלת החשבונות) וחישוביות (לרבות ספקי שירותי קצה וביניהם חברות למשלוח הודעות SMS ומיילים, מועדוני לקוחות, אתרי תוכן ומכירה ומערכת הנהלת החשבונות של החברה למוסדות חינוך).	9.2
					המערכת מספקת ממשקים למערכות סליקה ועומדת בתקנים הרלוונטיים DSS-PCI	9.3
					למערכת יכולת שליחת מיילים שיווקיים ומעוצבים באמצעות ממשק פנימי	9.4
					למערכת יכולת שליחת מיילים שיווקיים ומעוצבים דרך התממשקות לספק חיצוני	9.5
					המערכת מאפשרת התממשקות עם מדפסות כרטיסים שונות וביניהם מדפסות כרטיסים ייעודיות, מדפסות תרמיות וקיוסקים להדפסת כרטיסים	9.6
					המערכת מאפשרת התממשקות עם מגוון סורקים, קבועים וידניים לצורך בקרת כניסה.	9.7
					המערכת מאפשרת התממשקות עם מערכות בקרת כניסה ויציאה מסוג שערים אוטומטיים.	9.8
					המערכת מאפשרת התממשקות עם קיוסקים למכירת כרטיסים באופן ישיר.	9.9
דוחות						10.
					המערכת כוללת מחולל דוחות לבניית דוחות על ידי משתמש, על ידי הגדרת פרמטרים ושדות מידע.	10.1
					המערכת כוללת דוחות מובנים כדוגמת: דו"ח כניסות, דו"ח תפוסת ספורים, דו"ח תפוסת חללים, דו"ח תפוסה למנויים, דו"ח תפוסה לאירועים, דו"ח	10.2

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

					אמצעי תשלום, דו"ח הכנסות כוללות לפי מאפיינים כמו: סוגי אירועים/הכנסות, דו"ח יתרות סוכנים, דוח מכירות בפילוח יומי, דוח מכירות בפילוח לפי סיור / אירוע, דו"ח מנויים, דו"ח ביטולים, דו"ח הצלבת לקוחות ולקוחות כפולים ועוד. דוחות לתמיכה בתהליכי הנהלת חשבונות כמו: דו"ח התאמות אשראי	
					המערכת מאפשרת ייצוא מלא של בסיס הנתונים כולל היסטוריית הלקוחות לקבצי Excel / CSV.	10.3
					המערכת כוללת לוח בקרה גרפי (Dashboard)	10.4
טעינת נתונים						11.
					המערכת מספקת יכולת מיגרציה של הנתונים מהמערכת הקיימת כיום בעירייה, באמצעות טעינת קבצי Excel / CSV	11.1
נגישות						12.
					המערכת מאפשרת נגישות מלאה בתהליכי שיבוץ ומכירה	12.1
עיצוב						13.
					המערכת מאפשרת התאמה לשפה העיצובית העירונית: התאמת הלוגו, צבעים ועוד	13.1
שיווק ותקשורת						14.
					למערכת יכולת עצמאית לשלוח מסרונים ומיילים	14.1
					למערכת יכולת עצמאית לשלוח מיילים שיווקיים ומעוצבים	14.2
					למערכת יכולת לבצע קמפיינים שיווקיים לפי קהל יעד	14.3
					למערכת יכולת לבצע Upsell / Cross-sell במהלך הרכישה	14.4
ממשק למערכת ההזדהות העירונית AD						15.
					המערכת כוללת ממשק מלא ל- Azure Active Directory - אשר מאפשר התחברות של משתמשים פנימיים לממשק הניהול, ללא צורך בסיסמה.	
אבטחת מידע						16.
יש להציג מסמכים רלוונטיים					המערכת עומדת בדרישות אבטחת המידע המפורטות בנספח 4 שלהלן.	

נספח 4 – דרישות אבטחת המידע והגנת הפרטיות

1. הגדרות

- 1.1. **מידע אישי** - "מידע" ו"מידע רגיש" ו/או "בעל רגישות מיוחדת" כהגדרתם בחוק הגנת הפרטיות, תשמ"א-1981, מידע אשר ניתן לזהות באמצעותו, במישרין או בעקיפין, אדם פרטי באופן ישיר וכן מידע אשר יוגדר כמידע אישי על ידי העירייה.
- 1.2. **מידע אישי של העירייה** - כל מידע אישי הקשור באופן כלשהו לעירייה ו/או ללקוחותיה של העירייה ו/או לעובדיה של העירייה ו/או לכל גורם אחר הקשור באופן כלשהו לעירייה ו/או לחוזה ו/או כל נתון אחר שהעירייה הודיעה לספק כי היא רואה בו "מידע אישי" ובכלל זאת, בין היתר, כל מידע (כולו או חלקו) שהועבר ו/או יועבר לספק ו/או שניתנה לספק גישה אליו על ידי העירייה ו/או על ידי מי מטעמה, לרבות מידע אישי ממאגרי המידע של העירייה ומידע אישי שהספק יעבד כחלק ממתן השירותים לעירייה.
- 1.3. **עיבוד** - כל פעולה המבוצעת על מידע אישי ו/או באמצעות או בקשר למידע אישי, לרבות איסוף, הפקה, אחסון, שמירה, העברה, גישה, מתן גישה, תיקון, עיון, בדיקה, טיוב, שינוי, עריכה, העתקה, מחיקה, השמדה וכל פעולה אחרת בקשר למידע האישי.
- 1.4. **תקנות אבטחת מידע** - תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.
- 1.5. המונחים "מאגר מידע", "מחזיק במאגר מידע", "בעל מאגר מידע", "בעל שליטה במידע" תהא פרשנותם בהתאם להוראות חוקי הגנת הפרטיות.

2. עקרונות יסוד

- 2.1. הספק מתחייב לעמוד בדרישות אבטחת מידע מפורטות יותר, שיבואו בנוסף למפורט במסמך זה, ואשר יוגדרו על ידי מחלקת אבטחת מידע וסייבר עם תחילת העבודה.
- 2.2. אישור הפרויקט יינתן בכפוף לבחינת יישום התהליכים על ידי הספק בדגש לאבטחה פיזית, ארכיטקטורה, יישום רכיבי אבטחת מידע ושירותי הגנה הנדרשים בשירות, גישה מאובטחת לספק כולל הלבנת חומרים, סקר אבטחת מידע שיבוצע על ידי הספק וטיפול בממצאים טרם הפעלת המערכת על חשבון הספק.
- 2.3. כל שינוי בתצורת המערכת וזרימת המידע, יחייב בחינה מחודשת ואישור מחלקת אבטחת מידע וסייבר בעירייה.
- 2.4. כתנאי מתלה לחתימת העירייה על החוזה, הספק יפרט את המנגנונים והאמצעים האבטחתיים במטרה להפחית את הסיכונים ולהגן על המידע במסגרת השירות המבוקש. הספק יפרט את מפרט האבטחה, כולל תקני האבטחה שבידו ואישוריה, והכל מעבר למפורט בסעיף דרישות האבטחה בחוזה.
- 2.5. הספק יוכל להעביר הערות לדרישות אבטחת המידע, כולל חלופות ואמצעים שונים מהמפורט בחוזה.
- 2.6. העירייה שומרת לה את הזכות לקבל או לדחות הערות/שינויים שיציע הספק.
- 2.7. הספק מתחייב לחתום על נספח אבטחת מידע, בהתאם לדרישות האבטחה בחוזה, וכן להתחייב לשמירה על סודיות.

עיריית תל אביב-יפו

אגף טכנולוגיות ומערכות מידע

3. סיכונים מרכזיים

- 3.1 גישה בלתי מאושרת למידע ולמערכת המידע בשירות הספק.
- 3.2 גישה בלתי מאושרת לרשת העירייה באמצעות שירות הספק.
- 3.3 גישה למידע רגיש בעקבות הימצאות המידע במערכת שאינה בשליטת העירייה.
- 3.4 פגיעה באמינות, שלמות וסודיות המידע.
- 3.5 שימוש לא מורשה בהרשאה, או חריגה מהרשאה.
- 3.6 אי הכרת ההנחיות והנהלים של העירייה על ידי העובדים המספקים את השירות.
- 3.7 שיבוש המידע, המנוהל במערכת המידע אצל הספק, כתוצאה מכתובת קוד לקויה מצד הספק או הכנסת קוד זדוני.
- 3.8 פגיעה בזמינות המידע וברציפות התפעולית בשל התלות בספק.
- 3.9 דלף מידע אישי ורגיש כתוצאה מתקיפה חיצונית של ספק שירותי הענן, או כתוצאה מקונפיגורציה לקויה.
- 3.10 התחזות טכנולוגית, אנושית וקולית להשגת גישה פיזית ו/או לוגית ו/או לצורך עדכון.
- 3.11 גניבה ו/או פגיעה ו/או והשמדה של החומרים הפיזיים המועברים או המצויים אצל הספק, שהינם חומרים קריטיים בעלי ערך כספי, תפעולי או רגולטורי גבוה.
- 3.12 אי הקפדה על יישום דרישות חוק הגנת הפרטיות וחוקים החלים על העירייה הרלוונטיים לשירותים, כולל עדכונים מעת לעת.

4. דרישות אבטחת המידע

- 4.1 יוקצה לעירייה בסיס נתונים ייעודי ונפרד משאר לקוחות הספק.
- 4.2 המערכת תמצא מאחורי WAF/FW בעל שרידות גבוהה. ה-FW ינוטר באופן רציף.
- 4.3 המערכת או השירות יפעלו ברשת סגורה, אשר תהא חסומה תקשורתית לכל גישה יוצאת או נכנסת, מלבד קישור פנימה לשרת ה-web בשירות מאובטח (<https://443>) מרשת האינטרנט, וגישה נכנסת מתחנת ניהול ייעודית ברשת ניהול מאובטחת נפרדת.
- 4.4 תשתיות הספק יוגדרו ויוקשחו בהתאם למסמכי best practice רלוונטיים לכל סוג תשתית, מערכת הפעלה, ציוד תקשורת, מערכות תומכות, מערכות אבטחת מידע וכל רכיב נוסף ברשת, בהתאם להוראות יצרן ותקנים מקובלים.
- 4.5 הספק יספק קו תקשורת VPN Site-to-Site, הצפנה מלאה של התעבורה IPsec.
- 4.6 נדרש יישום מדיניות QoS מלאה לתעדוף תעבורת מידע קריטית.
- 4.7 ארכיטקטורת המערכת נדרשת להיות מאובטחת, כולל חלוקה לשכבות ומניעת גישה ישירה לבסיס הנתונים.

עיריית תל אביב-יפו

אגף טכנולוגיות ומערכות מידע

- 4.8. עדכוני אבטחת מידע ייושמו באופן שוטף, כאשר עדכוני אבטחת מידע המוגדרים ברמה קריטית יותקנו באופן מיידי. שאר עדכוני אבטחת המידע יעודכנו לתקופה אשר לא תעלה על 3 חודשים, בתיאום עם נציג העירייה.
- 4.9. פעילויות כלל הגורמים ברשת יירשמו במנגנון audit trail ויועברו על פי דרישה למחלקת אבטחת מידע וסייבר של העירייה. הספק יבצע בקרה שוטפת, באמצעות הלוגים, אחר פעילות חשודה. בכל מקרה יופעל מנגנון אשר מונע מחיקת לוגים.
- 4.10. לוגים יישמרו לתקופת זמן של לא פחות משנתיים (24 חודשים).
- 4.11. הספק יישם גיבוי מאובטח של הנתונים – כולל הצפנה בזמן גיבוי של מידע רגיש ופתיחת הצפנה בזמן שחזור נתונים.
- 4.12. הספק ימסור לידי מנהל אבטחת המידע בעירייה תמצית מנהלים של "מבדק חדירות" מעודכן, שבוצע במערכות הליבה של הספק, הרלוונטיות לשירותים, עד 60 יום מקבלת הודעת העירייה על אישור ההתקשרות עמו. לעניין זה, מבדק חדירות Penetration Test, הוא בקשר לביצוע של מתקפה יזומה, מתוכננת ומבוקרת על מערכת המחשוב בארגון הספק, לרוב מבוצע על ידי גורם חיצוני, במטרה לאתר חולשות אבטחה.
- 4.13. הספק יפעיל ניטור ממוכן של הסביבה, בין היתר באמצעות מערכות WAF ו-SIEM.
 - 4.13.1. ניתן יהיה לזהות חשדות לאירועי אבטחת מידע אצל הספק ולהתריע על אירועי אבטחת מידע, בזמן קרוב ל-On-Line, למערכת ה-SIEM העירונית.
 - 4.13.2. ניטור הלוגים האפליקטיביים יתואם בין מנהל אבטחת המידע בעירייה לבין הספק.
 - 4.13.3. נדרש להטמיע רכיבי הגנה על web-services.
 - 4.13.4. נדרשת הצפנה של נתונים רגישים בבסיס הנתונים.
 - 4.13.5. נדרשת התקנה ופעולה של מערכת אנטי-וירוס בכל שרתי המערכת.
 - 4.13.6. הגישה לגורמים מאושרים מצוות התמיכה הייעודי תבוצע באמצעות VPN / ZTNA.
 - 4.13.7. כל קובץ שיעלה למערכת יידרש לעבור סינון ובקרה לתוכן, לצורך מניעת העלאה של תוכן זדוני.
 - 4.13.8. נדרשת תמיכה ב-SSO ויכולות פדרציה, כולל אפשרות לתמיכה ב-MFA.
- 4.14. על הספק לוודא, שככל שנדרש להעביר מידע רגיש, הוא יועבר בצורה מאובטחת בתקשורת SSL או בהצפנה אפליקטיבית.
- 4.15. על הספק, לתמוך במחיקת מידע עודף, כפי שיוגדר על ידי העירייה, ובמימוש זכות העיון, בהתאם להגדרות חוק הגנת הפרטיות.
- 4.16. על הספק לנטר את המערכות שלו, בדגש על מערכות השירות לנתונים של העירייה. לספק תהיינה מערכות ניטור, בקרה והתרעה אוטומטיות 7x24 על אירועי אבטחת מידע ומתקפות סייבר.
- 4.17. על הספק לבצע היערכות ארגונית מתאימה, לרבות: נהלים, בקורות, מינוי אחראים, צוותי כ"א מיומנים לניטור ומעקב, טיפול באירועים ומשברים וכדו'.

עיריית תל אביב-יפו

אגף טכנולוגיות ומערכות מידע

4.18. כל מתקני המחשב של היצרן וספק הענן, בהם מופעל היישום ומתארח המידע, יעמדו בתקני אבטחה

פיזית (הכוונה למניעת גישה פיזית של בלתי מורשים) ויונחו לפחות על ידי הגורמים המוסמכים בכל מדינה בה מאוחסן המידע, בהתאם לעקרונות חוזה זה, ובאישור מראש של העירייה.

4.19. על הספק לקיים מערכות ביטחון ואבטחה פיזית של מרכזי המחשבים במקום נעול, עם בקרת כניסה,

התראות, והרתעות לבלתי מורשים, אתרי DR ואתרי אחסון המידע, לרבות: אבטחה אנושית, בקרת כניסות וציאות, הקלטה ומצלמות במעגל סגור, מערכות ניטור והתרעה אלקטרוניות ואמצעים נוספים.

4.20. על הספק לנקוט באמצעים נוספים להתמודדות ראויה ומהירה מול סיכוני אבטחת מידע חיצוניים ופנימיים.

4.21. כל תשתיות הספק יהיו מוגנות ע"י אמצעי אבטחת מידע, כולל:

4.21.1. תשתית FW להגנה והפרדה רשתית.

4.21.2. IPS להגנה מפני תקיפות רשת.

4.21.3. תשתית הגנה מפני מתקפות מניעת שירות DOS.

4.21.4. תשתית הגנה אפליקטיבית WAF.

4.21.5. תשתית הגנה על בסיסי נתונים DBFW.

4.21.6. תשתית הגנה מפני ווירוסים ותקיפות zero day על שרתים פיזיים.

4.21.7. תשתית התרעות על אירועים חריגים.

4.21.8. תשתית לבקרה וביצוע עדכונים עבור אפליקציות, תשתיות צד שלישי ורכיבי תוכנה.

4.21.9. תשתית הגנה להעלאת קבצים כולל סריקה ובקרה על סוגי קבצים, גודל, איתור נזקות וכו'.

4.21.10. תשתית הגנה על ממשקי API.

4.21.11. גישה מרחוק ל-DC של העירייה:

4.21.11.1. הגישה לרשת ה-DATA CENTER תתבצע באמצעות SSL VPN. דרישה זו תקפה

לכל הניגשים לרשת בה יופעל הפתרון ומכל מקום, גם מקומית מרשת הספק וגם מרשתות מרוחקות.

4.21.11.2. על תשתית SSL VPN לאכוף מדיניות ברמת התחנה המתחברת ולכלול תוכנת הגנת

תחנת קצה מעודכנת עם חתימות וסריקה עדכנית, וכן הגדרות אבטחה נוספות.

4.21.11.3. בתום 30 דקות של אי-פעילות – ה-VPN ינתק את המחשב מהשרת והמשתמש יידרש להזדהות מחדש.

4.21.11.4. שרתים בסביבת ה-DC לא יאפשרו שיתוף משאבים מקומיים של מחשבי קצה /

שרתים המתחברים לסביבת ה-DC מרחוק או מסגמנטים אחרים. כל תקשורת

תעבור אך ורק דרך ה-FW.

4.21.11.5. העברת מידע דורשת אישור ותהליך נפרד, ואין לבצעה במסגרת חיבור משתמשים לסביבה.

- 4.21.11.6. על סביבת ה-DC נדרש להפעיל AUDIT על LOGIN / LOGOUT של משתמשים, וכן על פעילויות רלוונטיות אחרות. הדוחות יישמרו למשך 90 יום ו-24 חודש בגיבוי.
- 4.21.11.7. לא תמאפשרת גישה ישירה לשרתים בפרוטוקול SSH / RDP. יש לאפשר גישה אך ורק דרך שרת TERMINAL מאובטח / VDI, העומד בכל תנאי ההקשחה בחוזה.
- 4.21.12. חשבונות רכיבי תוכנה (תהליכים / שירותים): במערכות הפעלה שבפתרון יוגדרו חשבונות ייעודיים לרכיבי תוכנה (Service Accounts). על חשבונות אלו יחולו הגדרות אבטחה שונות מאשר על חשבונות אנושיים, כולל מדיניות סיסמאות שונה, מדיניות נעילת משתמשים שונה, מדיניות ניטור ובקרה וכו'.
- 4.21.13. כל קובץ שעובר לצד העירייה יידרש לעבור הלבנה דרך תשתית ההלבנה של העירייה. הספק יצטרך לתמוך בטכנולוגיה הקיימת המבוססת על תיקייה IN ותיקייה OUT לאחר סריקה מוצלחת. המערכת תידרש לתת מענה למקרים בהם הקובץ לא עבר סינון בהצלחה, ע"י הצגת הודעה מתאימה למשתמש. במסגרת התקנת המערכת – הספק יידרש לבצע את האינטגרציה אל מול התשתית.
- 4.21.14. ככל שהמערכת תופעל במודל ענן SAAS, על הספק מוטלת האחריות המלאה לביצוע הלבנות של קבצים מקצה לקצה.
- 4.21.15. יופעל מנגנון לוג על כל תהליך של העברת קבצים.
- 4.21.16. המערכת נדרשת לאפשר הגבלת מספר וגודל הקבצים שלקוח יכול לשלוח דרך ערוץ תקשורת.

5. אבטחת אפליקציות וממשקים

- 5.1. כלל האפליקציות והממשקים יתוכננו, ייפתחו וייבדקו בהתאם למתודולוגית פיתוח מאובטח ובהתאם לסטנדרטי אבטחת מידע מתאימים של OWASP.
- 5.2. ישולבו מנגנונים ידניים/אוטומטיים לביצוע סריקות לאיתור פערי אבטחת מידע בקוד, כחלק משלבי פיתוח התוכנה.
- 5.3. הפעלת ממשקים תתבצע בתווך מוצפן ובאימות תעודה, תוך שימוש באלגוריתמי הצפנה עדכניים.
- 5.4. המערכת תומכת בניהול גישה עובדי העירייה למערכת על בסיס SSO, באמצעות ענן ציבורי.
- 5.5. גישה הממשק בין מערכת ה- AZURE AD/AWS למערכת הספק הנו בפרוטוקול SAML2, והאחריות לבחינת טווחי כתובת, MFA ושאר חוקי סינון, תהיה בצד של העירייה.
- 5.6. כל שינוי בשיטת הזיהוי ליחידות העירוניות וללקוחות השונים יתואם עם מנהל מחלקת אבטחת מידע וסייבר ועם מנהל הפרויקט באגף טכנולוגיות ומערכות מידע.
- 5.7. הסיסמא למערכת תוכפף למדיניות סיסמאות, כפי שתופעל על ידי העירייה.
- 5.8. הספק נדרש ליישם מנגנוני בדיקות קלט לכלל הממשקים האפליקטיביים (ממשק משתמש, ממשק אפליקטיבי וממשקים מול מערכות נוספות), ע"ב שיטת ה-white list לכל פרמטר.

עיריית תל אביב- יפו

אגף טכנולוגיות ומערכות מידע

- 5.9. הספק נדרש ליישם מנגנוני בדיקות פלט לכלל הממשקים האפליקטיביים (משתמש, ממשק אפליקטיבי וממשקים מול מערכות נוספות), במטרה למנוע התקפות הרצות ב-client side (XSS, Local Sql Injection, Mobile Attacks ועוד).
- 5.10. הספק יתעד כל פיתוח או רכישה של אפליקציות, מערכות, בסיסי נתונים, תשתיות ושירותים חדשים, באופן המאפשר לדעת את מהות השינוי, בדיקות האבטחה אשר בוצעו, רמת האבטחה הנגזרת מכך והשפעתה (ככל שישנה) על רמת האבטחה בשאר רכיבי המערכת.
- 5.11. יישום מנגנונים למניעת התקפות אוטומטיות כגון Captcha, במקומות הרלוונטיים.
- 5.12. יישום מנגנוני Anti-Phishing לאתר.
- 5.13. הגדרת אירועים אפליקטיביים המייצרים התראות, כגון מספר רב של ניסיונות התחזות כושלים.
- 5.14. קוד מקור, אשר יפותח ע"י הספק עבור העירייה, יישמר באמצעים מאובטחים הן בשרתים והן בעמדות העבודה, כאשר לכל הפחות יהיה מוצפן באחסון ונגיש רק לגורמים הנדרשים.
- 5.15. יישום עבודה מאובטחת מול בסיס הנתונים באופן המונע התקפות Injection.
- 5.16. תקשורת בין כלל הרכיבים תבוצע באמצעות פרוטוקולים מאובטחים בלבד.
- 5.17. עבודת כלל ה-services השונים והמשתמשים האפליקטיביים תהיה עם הרשאה מינימלית ובכל מקרה ללא הרשאת Admin/root/dba.
- 5.18. מניעת מתקפות אפליקטיביות: המערכת תידרש לדעת להתמודד עם מתקפות אפליקטיביות נפוצות ברמת היישום ולמנוע אותן, וכן להתמודד בהמשך עם מתקפות חדשות.
- 5.19. העברת מידע אישי ורגיש מן העירייה לספק ומן הספק לעירייה, ככל שתידרש, תהיה באמצעים מקובלים, כפי שינחה מנהל אבטחת מידע וסייבר, בתיאום עם הספק.

6. ניהול זהויות ובקרת גישה

- 6.1. המערכת תומכת בניהול הרשאות מבוסס תפקיד (RBAC).
- 6.2. תהליך הזדהות יתבצע בתווך SSL.
- 6.3. תתקיים הצפנת סיסמאות ופרטי חשבונות משתמשים הניגשים למאגרי מידע וממשק.
- 6.4. ניהול ההרשאות יוקצה רק לבעלי התפקידים האחראים בצוותים העירוניים, כך שכל רפרנט יורשה לניהול הרשאות רק לסוג המידע והמודול שבאחריותו.
- 6.5. המערכת תחשוף ממשק ניהול משתמשים והרשאות ייעודי, שיאפשר ניהול משתמשים. כל אירוע גישה למערכת או לרכיב ברשת יתועד באופן המתאים, בהתאם להוראות תקנות אבטחת מידע, לרבות תיעוד ניהול מורשי הגישה.
- 6.6. המערכת תומכת בתהליכי תיקוף הרשאות, לרבות יצוא רשימת המורשים, לטובת וידוא ההרשאות התקפות במערכת, לצורך אישור על ידי הגורמים העירוניים האחראים לפעילות, כל אחד בתחומו, כך שהעירייה תוכל לבצע בקרה בעניין זהות מורשי הגישה למערכות בהן מצויים נתונים עירוניים.
- 6.7. המערכת תומכת בגישה למסמכים מסווגים ברמת רגישות גבוהה יותר, דוגמת הערכות עובדים.

7. אישורים נדרשים

- 7.1. הספק מתחייב לספק אישור ביצוע בדיקות חדירות, כולל תיקון ליקויים, ככל שנמצאו, אחת לשנתיים, ע"י גורם צד-שלישי.
- 7.2. הספק מתחייב, כי ככל שהמידע יאוחסן בשירותי ענן – השירותים יינתנו רק על ידי חברות העומדות בתקנים ISO/IEC 27001, בתקן CSA Star או בתקן מקביל תקף.
- 7.3. כל חשיפת אבטחת מידע, אשר תימצא באחריות הספק, תדווח למחלקת אבטחת מידע וסייבר, וכל חשיפה מוסכמת ברמה בינונית ומעלה – הספק יידרש לתקנה על פי הזמנים שיוגדרו על ידי העירייה, בהתאם לאופי החשיפה ועל חשבון הספק.

8. גיבויים

גיבוי, שחזור והתאוששות :

- 8.1. הספק מתחייב לבצע גיבויים של המידע בתדירות יומית, שבועית, חודשית ושנתית, בצורה מאובטחת.
- 8.2. הספק מתחייב לאחסן את מדיות הגיבוי בכספת מוגנת אש ומים, הנמצאת מחוץ למתקן המחזיק את מאגרי המידע. הספק יעשה שימוש באמצעים שיבטיחו את שלמות המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.
- 8.3. הספק מתחייב לבצע שחזורים מדגמיים של המדיות ולבדוק את תקינותן.

9. להלן סוגי המידע המהווים מידע אישי ורגיש אשר יש לתעד את הגישה אליהם :

ניסיון מקצועי – למשל: קו"ח, או כל מסמך או שדה המפרט את הניסיון המקצועי של האדם.	מגדר – מין זכר/נקבה.
כתובת מייל – אישית של אדם, לא כתובת מייל ארגונית.	פרטי קשר – טלפון, כתובת מגורים, כתובת מייל.
מידע ביומטרי – כל נתון המאפשר לבצע זיהוי ביומטרי, וביניהם: תבניות ותמונות טביעות אצבע, תביעת פנים, דגימות קול	אילן יוחסין – מידע על שייכות משפחתית וקשרים משפחתיים של אדם.
מידע דמוגרפי תעודת זהות גיל מין ארץ לידה מידע על נישואין מידע על גירושין כתובות הווה ועבר מעברים גיאוגרפיים	נתוני תקשורת נתוני מיקום בנקודת זמן מסוימת נתוני מנוי נתוני תעבורה
מידע אודות הרגלי צריכה או התנהגות – העדפות בתחום התרבות והפנאי, מקומות בילוי, מידע על בעלי חיים שבעלות האדם ומשויכים אליו בהיבטי רישום וכדומה.	מידע גנטי

עיריית תל אביב-יפו

אגף טכנולוגיות ומערכות מידע

מידע על עבר פלילי	דעות פוליטיות
מידע כלכלי: חובות – כל סוג חוב שיש לאדם, למשל – חוב שנצבר לבעל עסק ומשווץ אליו אישית.	השתייכות דתית
מידע כלכלי: נכסים – נכסי נדל"ן או כל סוג נכס אחר המשווץ לאדם אישית.	נטייה מינית
מידע על מצב רפואי	נתוני השכלה – תעודות השכלה, כל מסמך או שדה המפרט את השכלתו האישית של אדם.
מידע על מצב נפשי	הקלטות אודיו או וידאו – צילומים והקלטות הנשמרים ממצלמות ו/או נתוני צפייה בזמ"א.