

טופס "עדכון פרטים אישיים"

תוכן העניינים

3	כללי
3	מטרת הבדיקה
4	עבודת הבדיקה
4	ממצאים
4	מאגר המידע וההחלטה על עדכון
7	קבלת החלטה על הוצאת הפעילות למיקור חוץ
8	גיבוש והפצת "מסמך עדכון פרטים אישיים"
8	כללי
9	גיבוש "מסמך עדכון פרטים אישיים"
12	משך שמירת המידע אצל הספק
14	שליחת הטופס לעובדי העירייה
17	מעורבות גורמים עירוניים מקצועיים בפרויקט
17	כללי
18	מעורבות מחלקת אבטחת מידע
19	ליווי השירות המשפטי
21	מסקנות
22	המלצות
24	נספח 1 –
25	נספח 2 –

כללי

1. עיריית תל אביב יפו מעסיקה למעלה מ- 10,000 עובדות ועובדים. כל עובד עם כניסתו לראשונה לעבודה בעירייה נדרש למלא טופס פרטים אישיים הכוללים בין היתר פרטים משפחתיים, ניסיון תעסוקתי, השכלה ופרטי בנק.
2. במרוצת השנים, פרטים אלה ופרטים נוספים, יכולים להשתנות ועל העובד חלה החובה לעדכן על כל שינוי בפרטיו האישיים.
3. אגף משאבי אנוש (להלן: "האגף") עורך מדי מספר שנים, פעילות יזומה של עדכון פרטי העובדים. העדכון מתבצע באמצעות הפקת טופס הכולל את הפרטים האישיים של העובד, כפי שמופיעים במערכת משאבי האנוש העירוני, ושליחתו אל העובד. העובד נדרש לתקן את הדרוש עדכון, ובמידת הצורך לצרף לכך גם אסמכתה מבססת. תהליך עדכון הפרטים האחרון שבוצע (לפני הנוכחי, נשוא דוח בדיקה זה) היה בשנת 2018, ועל כן הוחלט על ידי האגף בחודש יולי, 2020 לקיים תהליך רוחבי של עדכון פרטי העובדים.
4. לשם ביצוע הפרויקט, הסתייע אגף משאבי אנוש בספק המעניק לעירייה שירותים נוספים בתחום הדיוור מכוח מכרז בו זכה.

מטרת הבדיקה

5. מטרת הבדיקה הייתה לבחון את תהליך ביצוע עדכון הפרטים האישיים של עובדי העירייה ובכלל זה:
 - א. בדיקת עמידת העירייה בהוראות החוק בכל הקשור לשימוש במאגרי מידע;
 - ב. בדיקת תהליך גיבוש והפצת טופס "מסמך עדכון פרטים אישיים" לרבות בחינת ממשקי העבודה מול הספק שביצע את הפרויקט;
 - ג. בחינת מעורבות הגורמים העירוניים הרלוונטיים בפרויקט.
- בכל הנוגע להליך הפצת טופס עדכון הפרטים האישיים, התמקדה הבדיקה בהליך הפצתו באמצעות הודעת הדוא"ל.

עבודת הבדיקה

6. במסגרת הבדיקה, התקיימו פגישות והתקבלו מסמכים מ: מנהל אגף משאבי אנוש, מנהל אגף מחשוב ומערכות מידע, מנהלת אגף מחשוב ומערכות מידע דאז, ס.י.א.ו. וארכיטקט ראשי באגף מחשוב ומערכות מידע, מנהל מחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע, מנהל מחלקת מידע ובקרה באגף כח אדם, מנהלת מחלקת מערכות מידע ארגוניות באגף מחשוב ומערכות מידע, מנהלת פרויקטים באגף מחשוב ומערכות מידע, עוזרת ראשית ליועמ"ש בשירות המשפטי, סגנית בכירה ליועמ"ש ומנהלת תחום דיני עבודה בשירות המשפטי, מנהל הוצאה לאור ותכנון טפסים באגף ארגון ותקינה, מנהלת פרויקטים בכירה לדיוור וטפסים באגף ארגון ותקינה, מנהל אגף רכש ולוגיסטיקה, מנהלת תחום רכש באגף רכש ולוגיסטיקה, מנהלת מחלקת שירות לקוחות ושרשרת האספקה באגף רכש ולוגיסטיקה.
7. הבדיקה נערכה במהלך החודשים יולי - דצמבר 2020 (לסירוגין).

ממצאים

מאגר המידע וההחלטה על עדכנו

כללי

8. חוק הגנת הפרטיות, התשמ"א – 1981 (להלן: "חוק") קובע בין היתר את ההגדרות הבאות:
- א. מאגר מידע – "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט:
- (1) אוסף לשימוש אישי שאינו למטרות עסק; או
 - (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשנלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם שעמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".
- ב. מחזיק לעניין מאגר מידע: "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש".
- ג. מנהל המאגר: "מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לענין זה".
9. בסעיף 9 (ב) לחוק בנושא "בקשה לרישום" נקבע בין היתר, כי: "בקשה לרישום מאגר מידע תפרט את - (1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל".

10. בהתאם לחוק הגנת הפרטיות, איסוף מידע רגיש על אדם יירשם כמאגר מידע. לכל מאגר מידע, יוגדר "מנהל מאגר" אשר יהיה אמון בין היתר על שמירת המידע ומתן הרשאות גישה למאגר.
11. במסגרת קבלת העובד, כמועסק בעיריית תל אביב יפו, מתבקש העובד למלא את הפרטים הבאים:
 - א. פרטי העובד.
 - ב. כתובת מגורים, טלפון וכתובת דוא"ל.
 - ג. מצב משפחתי ופרטי בן/בת הזוג.
 - ד. פרטי ילדים.
 - ה. פרטי בנק.
 - ו. השכלה.
 - ז. רישיון (מכל סוג שהוא).
 - ח. עדכון פרטי צבא.

ממצאים

12. עוזרת ראשית ליועמ"ש בשירות המשפטי, האמונה על תחום זה, מסרה לעורכי הבדיקה, כי: "המידע האישי על עובד נמסר על ידי העובד במסגרת יחסי העבודה בינו לבין העירייה. המידע מנוהל כמאגר מידע רשום לפי חוק הגנת הפרטיות, אשר הרשאות הגישה אליו נקבעות על ידי מנהל המאגר – אלון שורף (מנהל אגף משאבי אנוש)".
13. הרשות להגנת הפרטיות (להלן: "הרשות") הינה הגוף המסדיר, המפקח והאוכף על פי חוק הגנת הפרטיות בישראל. עורכי הבדיקה סקרו את אתר האינטרנט של הרשות להגנת הפרטיות ומצאו, כי בהתאם לסעיף 12(א) לחוק, קיימת אפשרות לעיין בפנקס מאגרי מידע. לצורך עיון בפנקס מאגרי המידע האתר מפנה אל אתר אחר בנושא "מאגרי המידע הממשלתיים" (data.gov.il).
14. בהתאם למידע המופיע באתר "מאגרי המידע הממשלתיים" עולה, כי לעירייה מאגר מידע רשום שמספרו 990043046 בנושא "כח-אדם עובדים ופנסיונרים" החל מיום 05/01/2005.
15. עורכי הבדיקה ביקשו לבדוק מי הגורם העירוני הרשום כמנהל המאגר אצל הרשות. עורכי הבדיקה פנו אל הרשות להגנת הפרטיות במשרד המשפטים במטרה לקבל את מסמכי הרישום העדכניים למאגר המידע בנושא "כח-אדם עובדים ופנסיונרים". מסקירת המידע שהתקבל מהרשות עולה, כי נכון לתאריך 29/12/2020 הגורם המוגדר "מנהל המאגר" הינו מנהל אגף משאבי אנוש.

16. חוק הגנת הפרטיות, התשמ"א – 1981 קובע בסעיף 14 "תיקון מידע" בין היתר, כי:
"א' אדם שעדיין במידע שעליו ומצא כי איוו וכו', שלם, ברור או מעודכן, רשאי לפנות לבעל מאגר המידע, ואם הוא תושב חוץ - למחזיק מאגר המידע, בבקשה לתקן את המידע או למחוקו.
ד' מחזיק חייב לתקן מידע, אם בעל מאגר המידע הסכים לתיקון המבוקש או שבית משפט ציווה על התיקון".
17. עוזרת ראשית ליועמ"ש בשרות המשפטי מסרה לעורכי הבדיקה בהקשר לכך, כי: "אף כי החובה לעדכן את המידע חלה על העובד, אין מחלוקת כי העירייה מוסמכת לבקש מיוזמתה את עדכנו על ידי העובד".
18. בהתאם לסמכותו של מנהל אגף משאבי אנוש, המוגדר אף כמנהל המאגר הרשום ברשות, ערך אגף משאבי אנוש במהלך חודש יולי 2020 תהליך של עדכון פרטי העובדים (להלן: "הפרויקט"). הפרויקט כלל גיבוש של תבנית בו שולבו פרטיו האישיים של כל עובד (כפי שמופיע במערכת המידע העירונית) ומסירת הטופס לעובד לביצוע עדכון הפרטים. תהליך מסירת הטופס התבצע בשני מסלולים זאת מאחר ולמחצית מעובדי העירייה לא הוגדר מייל עירוני:
א. מסלול 1 – שליחת הודעת דוא"ל אל עובדי העירייה להם הוגדר מייל עירוני בנושא "עדכון פרטים אישיים לשנת 2020 – XXX (שם העובד)".
ב. מסלול 2 – הדפסת טופס "עדכון פרטים אישיים" לכל עובד שלא הוגדר לו מייל עירוני ומסירתו ידנית לצורך עדכון הפרטים.
19. עורכי הבדיקה מצאו, כי בשני המסלולים נדרשו העובדים לתקן את הטופס באופן ידני ולאחר מכן להחזירו באמצעות סגלי משאבי אנוש ביחידות.
20. מנהל אגף משאבי אנוש מסר לעורכי הבדיקה, כי מטרת הפרויקט הייתה ליישר קו לגבי נכונות הפרטים של העובדים, והוא בעיקר נבע מהסיבות הבאות:
א. עדכון כתובות לשליחת מכתבים – בעת משבר מגפת וירוס הקורונה נשלחו תלושי השכר של עובדי העירייה אל כתובת המגורים הרשומה במערכת המידע העירונית. למעלה מ-40% מהמכתבים חזרו.
ב. עדכון מספר טלפון נייד – בעת משבר מגפת וירוס הקורונה, בשונה משנים קודמות, חלוקת תווי השי לחג התקיימה באמצעות שליחת SMS. למעלה מ-30% ממספרי הטלפונים הניידים של העובדים לא היה קיים / מעודכן במערכת המידע העירונית.
ג. עדכון לאום העובד.
ד. עדכון לגבי רישיונות נהיגה.
ה. בדיקת התחייבויות של העובד – נשק, טלפון נייד, חניה, מחשב נייד, אייפד וכד'.

קבלת החלטה על הוצאת הפעילות למיקור חוץ

כללי

21. מאחר והפרויקט בוצע על ידי ספק המעניק לעירייה שירותי מיקור חוץ הסתייעו עורכי הבדיקה בבדיקתם בהנחית רשם מאגרי מידע ברשות להגנת הפרטיות¹ במשרד המשפטים, הנחייה מס' 2/2011 בנושא "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" (להלן: "הנחית רשם מאגרי מידע").

22. הנחיית רשם מאגרי מידע קובעת בסעיף 3.1.1.1 בנושא "הוצאת פעילות למיקור חוץ בדיקה מקדמית, היקף ומודל אספקת שירות", כי: "על ארגון המבקש להוציא פעילות למיקור חוץ לבחון האם הוא רשאי להוציא את המידע שהוא מבקש לעבד במיקור חוץ אל מחוץ לשליטתו בתהליך של מיקור חוץ, שכן עשויות להיות מגבלות חוקיות או אתיות, אשר מונעות העברה כאמור. אף אם אין מגבלה פורמלית כאמור, מומלץ לקיים הליך בחינה האם ראוי, לאור אופי המידע האישי שהשירות יתבקש לגביו ורגישותו, להעביר את המידע או את העיבוד שלו למיקור חוץ" (ההדגשה אינה במקור).

ממצאים

23. לעורכי הבדיקה לא הוצג, כי טרם ההחלטה על הוצאת הפרויקט למיקור חוץ, בוצע הליך בחינה של האפשרויות הקיימות לאגף לביצוע עדכון הפרטים האישיים בין אם בחצרות העירייה בין אם באמצעות מיקור חוץ.

מנהל אגף משאבי אנוש מסר בהתייחסותו לממצא, כי: "מזה שנים פרויקט "עדכון פרטים אישיים" מבוצע באמצעות מערכת דיוור עירונית שקיימת באגף המחשוב שעברה הליך של מכרז בעיריית תל אביב יפו ולכן לא בוצעה בחינה מקדימה למעט בדיקה שהמכרז עדיין בתוקף".

24. בנוסף יצינו עורכי הבדיקה, כי במסגרת הבדיקה נמצא אף שמחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע לא הייתה שותפה לתהליך ואף לא ייעצה לאגף בנושא. לפרטים נוספים אודות מידת מעורבותה המקצועית של מחלקת אבטחת מידע וסייבר ראה סעיפים 64 - 69 להלן.

¹ לשעבר רמו"ט – הרשות למשפט, טכנולוגיה ומידע.

מנהל אגף משאבי אנוש מסר בהתייחסותו לממצא, כי: "מנהל מחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע ציין כי ערוץ תקשורת (מערכת הדיוור העירונית) בין העירייה לספק הוא אכן ערוץ תקשורת מאובטח. כפי שציינו בפתח הדברים אגף משאבי אנוש פעל בהתאם לתנאי המכרז".

מנהל אגף מחשוב ומערכות מידע מסר בהתייחסותו לסעיף, כי: "מחלקת אבטחת מידע באגף המחשוב מודעת למערכת הדיוור העירוני ולכך שהיא עובדת בערוץ מאובטח מול 2 בתי הדפוס שמולם אנחנו עובדים. מחלקת אבטחת מידע יצרה את הערוצים המאובטחים שמאפשרים לעשרות תהליכים של הפצה (הדפסה / מייל) להתקיים באופן יומי ורציף".

הערת עורכי הבדיקה:

בתהליך המתואר בדוח הבדיקה, ישנן פעולות שלא בוצעו באמצעות מערכת הדיוור העירונית. כך לדוגמא, שליחת הודעת הדוא"ל (באמצעות ספק מיקור חוץ) אל עובדי העירייה להם קיים מייל עירוני, הכולל את טופס עדכון הפרטים.

גיבוש והפצת "מסמך עדכון פרטים אישיים"

כללי

25. לצורך ביצוע תהליך עדכון פרטים, בו הפרמטרים אותם מבקשים לבדוק הינם קבועים, אך רק הנתונים בו משתנים מעובד לעובד, נדרש לייצר תבנית אחידה בו נכללים הפרמטרים אותם מבקשים לתקף ועל בסיסו נכתבת "תוכנית הדפסה" לצורך שילוב הנתונים לתבנית.
26. עם סיום שלב גיבוש התבנית ו-"תוכנית ההדפסה", ולאחר ששולבו בטופס הנתונים האישיים של העובד, נדרש להעבירו לעובד, תוך הקפדה שיגיע לעובד הנכון.
27. לשם ביצוע הפרויקט, לרבות גיבוש התבנית, כתיבת "תוכנית הדפסה" ומסירתו לעובד, הסתייע אגף משאבי אנוש בשירותי חברת "א.פ.ת." (להלן: "ספק" או "חברת א.פ.ת.") אשר לה חוזה חתום עם העירייה מתאריך 11/07/2018 מכוח מכרז פומבי 219/2018 בנושא "מרכז פומבי להדפסת מסמכי דיוור ודיוור לדואר אלקטרוני".
28. בצד העירוני השותפים בתהליך היו אגף משאבי אנוש, אגף ארגון ותקינה ואגף מחשוב ומערכות מידע.

גיבוש "מסמך עדכון פרטים אישיים"

כללי

29. תהליך גיבוש "מסמך עדכון פרטים אישיים" התנהל במספר שלבים –

- א. שלב 1 - בניית תבנית על ידי הספק אשר על בסיסה שולבו הנתונים של כל עובד ועובד בעירייה כפי שמופיעים במערכת משאבי אנוש העירוני לרבות כתיבת "תוכנית ההדפסה".
- ב. שלב 2 - שליחת בסיס הנתונים הכולל את פרטי העובדים המופיעים במאגר המידע "כח-אדם עובדים ופנסיונרים" אל הספק באמצעות "מערכת הדיוור העירוני".
- ג. שלב 3 – ביצוע בדיקות על נאותות "תוכנית ההדפסה" לשילוב הנתונים במקומות המתאימים בתבנית.

ממצאים

30. אגף ארגון ותקינה בשיתוף אגף משאבי אנוש אמון על בחינת נאותות גיבוש התבנית אשר על בסיסה שולבו הנתונים. מנהל הוצאה לאור ותכנון טפסים באגף ארגון ותקינה מסר לעורכי הבדיקה, כי מאחר ולא מדובר בפרויקט המבוצע לראשונה, התבנית אשר על בסיסה שולבו הנתונים ותוכנית ההדפסה היו כבר קיימים אך נדרש היה לבצע בהם מספר התאמות. בנוסף מסר, כי מאחר וההוצאה העיקרית, בפרויקטים מסוג זה, הינה גיבוש התבנית ותוכנית ההדפסה, הספק שנבחר לבצע את הפרויקט הינו אותו ספק שביצע את הפרויקט בשנת 2018 – חברת "א.פ."

מנהל אגף מחשוב ומערכות מידע מסר בהתייחסותו לסעיף, כי: "בשנת 2018 נשלח המופס ב-2 ערוצים – **Print ו-Mail**. הדבר נעשה בעזרת בית הדפוס 'א.פ.'. בשנת 2015 נתבקש בית הדפוס 'א.פ.' רק להדפיס את המופס".

31. הנחיית רשם מאגרי מידע קובעת בסעיף 3.1.1.2 בנושא "הוצאת פעילות למיקור חוץ בדיקה מקדמית, היקף ומודל אספקת שירות", מספר מודלים להעברת המידע אל ספק הנותן שירותי מיקור חוץ. בין היתר נכללים המודלים הבאים:

- א. "שירות המחייב העברה או העתקה של מאגר מידע שלם, או חלק מהותי ממנו, מהמזמין לקבלן.
- ב. שירות המחייב טיפול במידע אישי בדרך של מתן הרשאות גישה או עדכון למידע במאגר המידע אצל המזמין, בהיקף הנדרש לצורך מתן שירות ספציפי, ללא העברת מאגר המידע במלואו".

- בסיפא של הסעיף מציין הרשם, כי כנקודת מוצא יש להעדיף את חלופה ב' מאחר ובחלופה הראשונה "מאבדת" העירייה את יכולת השליטה בשימוש במאגר המידע.
32. עורכי הבדיקה מצאו, כי במקרה הנבדק הועבר אל הספק קובץ שהופק ממאגר המידע הכולל את פרטיהם האישיים של עובדי העירייה. לאמור, העירייה בחרה בחלופה א' הפחות מומלצת על פי הנחית רשם מאגרי המידע.
33. עורכי הבדיקה ביקשו לדעת האם התקשורת עם הספק, לרבות תהליך העברת קובץ מאגר המידע בו כוללים פרטי העובדים, התבצעה בצורה מאובטחת, ובסוף כל פעולה התקבל אישור מהספק על קבלת הנתונים.
34. מנהלת פרויקטים באגף מיחשוב ומערכות מידע מסרה לעורכי הבדיקה, כי התקשורת עם הספק לביצוע תהליך הפקת "טופס עדכון פרטים אישיים", בדיקתו ואישורו להפצה, נערכה באמצעות מערכת עירונית שפותחה באגף המחשוב ושמה "מערכת הדיוור העירוני". עוד הוסיפה מנהלת פרויקטים, כי "מערכת הדיוור העירוני" מהווה ערוץ מאובטח להעברת מידע רגיש מחצרות העירייה לספקי מיקור חוץ באמצעות Site to Site VPN בין שרת העירייה לשרת FTP של הספק.
35. לשאלת עורכי הבדיקה מסר מנהל מחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע, כי ערוץ תקשורת זה בין העירייה לספק, הוא אכן ערוץ תקשורת מאובטח.
36. עורכי הבדיקה יצינו, כי במסגרת דוח הבדיקה לא נבדקה רמת האבטחה של ערוץ תקשורת זה. עורכי הבדיקה הסתמכו על דברי נציגי אגף מיחשוב ומערכות מידע כי ערוץ התקשורת מהווה ערוץ תקשורת מאובטח.
37. מנהלת פרויקטים באגף מחשוב ומערכות מידע העבירה לעיון עורכי הבדיקה צילום מסך "מערכת הדיוור העירוני". מסקירת צילום המסך עולה, כי הוא כולל תיעוד לתהליך העברת המידע מחצרות העירייה לספק "שליחת הזמנה", לרבות אישור הספק על קבלת הנתונים "אישור רגיל להזמנה", כדלהלן:

מעקב הזמנות - הזמנה מספר 9327				
Drag a column header and drop it here to group by that column				
מסד	פעולה	תאריך פעולה	יזם פעולה	סטטוס
אישור רגל להזמנה	15/07/2020 12:40:40	אישור		
[15/07/2020 12:40:40 , ...] הפעולה אושרה [15/07/2020 09:21:09] [עירייה]				
אודע פרינס	14/07/2020 13:32:34	החלחה	BzTalk	
אישור	14/07/2020 10:17:09			
[14/07/2020 10:17:09] הפעולה אושרה [14/07/2020 08:52:05] [עירייה] הזמנה מס' 9327 נוצרה בהצלחה				
אישור	14/07/2020 08:51:53	גילה ווקנין		

38. מנהלת פרויקטים מסרה לעורכי הבדיקה בהקשר לכך, כי: "האישור נערך במסגרת שליחת הזמנה לבית הדפוס באמצעות המערכת. לאחר שהמערכת מעבירה את ההזמנה והקבצים המצורפים להזמנה לשרת בית הדפוס בערוץ מאובטח, בית הדפוס שולח לנו אישור שקיבל את ההזמנה. האישור מתבצע במערכת".

39. בנוסף, עורכי הבדיקה ביקשו לבדוק האם בוצעו בדיקות על תוכנית ההדפסות לרבות שילוב הנתונים במסגרת התבנית שגובשה. מנהלת פרויקטים באגף מחשוב ומערכות מידע העבירה לעיון עורכי הבדיקה צילום מסך "ממערכת הדיוור העירוני" בו נכלל תיעוד לבקשת הספק לביצוע בדיקות של העירייה על תוכנית ההדפסות, כדלהלן:

מעקב הזמנות - הזמנה מספר 9327				
Drag a column header and drop it here to group by that column				
מסד	פעולה	תאריך פעולה	יזם פעולה	סטטוס
אישור רגל להזמנה	15/07/2020 12:40:40	אישור		
[15/07/2020 12:40:40 , ...] הפעולה אושרה [15/07/2020 09:21:09] [עירייה]				
אודע פרינס	14/07/2020 13:32:34	החלחה	BzTalk	
אישור	14/07/2020 10:17:09			
[14/07/2020 10:17:09] הפעולה אושרה [14/07/2020 08:52:05] [עירייה] הזמנה מס' 9327 נוצרה בהצלחה				
אישור	14/07/2020 08:51:53	גילה ווקנין		

40. מנהלת פרויקטים מסרה לעורכי הבדיקה בהקשר לכך, כי: "במסגרת העבודה במערכת הדיוור מתקבלים מסמכים. מסמכים הינם תלושים/מפסים אקראיים של העבודה הנדרשת. אלו קבצי PDF שמראים הלכה למעשה את התלוש/טופס המשלבים את הגרפיקה עם נתונים מתוך קובץ הנתונים. מסמכים אלו שמוגעים בצורה מאובטחת למערכת הדיוור, נבדקים ע"י הלקוחות העירוניים שהפיקו את הקובץ ושולחו את ההזמנה לבית הדפוס. בהתאמה, הלקוחות העירוניים מאשרים או לא מאשרים את ההפקה או מבקשים תיקון מבית הדפוס המחייב מסמכים חדשים".

41. עורכי הבדיקה ביקשו לבדוק את נאותות תהליך ביצוע הבדיקות על תוכנית ההדפסה שנכתבה אשר באמצעותה שולבו הנתונים בתבנית. מנהלת פרויקטים בכירה לדיוור וטפסים באגף ארגון ותקינה העבירה לעיון עורכי הבדיקה תיעוד בהודעות דוא"ל לאישורים הבאים:

א. אישור של מנהלת פרויקטים בכירה לדיוור וטפסים באגף ארגון ותקינה, לתבנית שהוגדרה ולהעברתה לטפסים לשילוב התבנית עם תוכנית ההדפסה.

ב. אישור של רכזת מידע ומבקרה באגף משאבי אנוש, לתקינות נאותות שילוב הנתונים בתבנית שהוגדרה.

משך שמירת המידע אצל הספק

כללי

42. הנחיית רשם מאגרי מידע קובעת בסעיף 3.1.7.4 בנושא "משך שמירת המידע, ביעור המידע", כי: "על המזמין לדרוש מן הקבלן תצהיר המאמת ביצוע פעולות מחיקה, ביעור והשמדה של כל המידע שהגיע אליו במסגרת ההתקשרות עמו".

ממצאים

43. עורכי הבדיקה ביקשו לבדוק האם בסיום תהליך גיבוש התבנית ושילוב הנתונים, וידאה העירייה מול הספק כי קובץ מאגר המידע בו נכללו פרטי עובדי העירייה נמחק ממערכות המידע של חברת "א.פ.". עורכי הבדיקה מצאו, כי לא התקבל מהספק אישור על מחיקת מאגר המידע ואף לא נערך בירור מול הספק לוודא כי המידע אכן נמחק.

44. מנהלת פרויקטים באגף מחשוב ומערכות מידע מסרה לעורכי הבדיקה בהקשר לכך, כי: "אין ברשותנו אישור מתועד של בית הדפוס על מחיקת קבצי הנתונים שאנחנו שולחים אליו. משיחה עם גורם המחזיק את תיק הלקוח של עיריית תל אביב יפו בבית הדפוס, הובן כי קבצי הנתונים שמועברים לבית הדפוס נמחקים כשבועיים לאחר הפצת המידע".

עוד הוסיפה מנהלת פרויקטים, כי: "בית הדפוס מחוייב למבדקי איזו, ביניהם אבטחת מידע ושמירת הנתונים ומחיקתם". לעיון עורכי הבדיקה הועברה תעודה של מכון התקנים הישראלי לעמידה של חברת "א.פ." בהוראות תקן ISO 27001 בנושא "ניהול אבטחת מידע" ובהוראות תקן 27799 ISO בנושא "אבטחת מידע רפואי".

45. יצוין, כי מסקירת הסכם ההתקשרות עם חברת "א.פ." עולה כי בסעיף 6.8.10 לנספח ב' בחוזה, נכללת התייחסות לחובה למחוק את המידע שהתקבל מהעירייה, כדלהלן: "פרק הזמן שמותר לספק להחזיק במידע לצורכי ביצוע עבודתו הינו עד 60 יום מיום העברת מסמכי הדיוור לעירייה ו/או לספק החלוקה. בחלוף זמן זה על הספק למחוק את כל המידע שנכנסו שנהגו אליו מהעירייה, בכל אמצעי מדיה". על אף האמור, עורכי הבדיקה רואים חשיבות בבחינה, לכל הפחות תקופתית, של תהליך מחיקת המידע אשר אצל ספק שירותי הדפוס.

46. בחודש מרץ 2019 הוגש למחלקת אבטחת מידע וסייבר דו"ח מסכם בנושא "מיפוי וסקירת מאגרי המידע ותאימותם לתקנות הגנת הפרטיות" אותה ערכה חברת "א.פ. ו. ס.". מסקירת הדו"ח המסכם עולה בין היתר, כי אחד הליקויים שנמצאו בעקבות הסקר, הוא שגורמי מיקור חוץ העושים שימוש במאגרי המידע העירוניים, אינם חתומים על מסמך בו הם מתחייבים לשמירה על סודיות המידע בהתאם לדרישות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

47. מנהל מחלקת אבטחת מידע וסייבר מסר לעורכי הבדיקה בהקשר לכך, כי לצורך עמידה בהוראות החוק גיבש השירות המשפטי מסמך שמירת סודיות (התואם להוראות החוק) אשר הועבר אל כל הספקים ונותני השירותים בעירייה לצורך חתימה.

עורכי הבדיקה ביקשו לבדוק האם חברת "א.פ." חתומה על מסמך לשמירה על סודיות המידע בהתאם לדרישות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. עוזרת ראשית ליועמ"ש בשירות המשפטי מסרה לעורכי הבדיקה, כי מאחר ומועד החתימה על החוזה היה בסמוך לכניסת התקנה לתוקף התווסף לחוזה סעיף, (סעיף 6.8 למפרט הטכני – נספח ב' לחוזה), העונה על דרישות תקנות הגנת הפרטיות (אבטחת מידע). לפירוט נוסח סעיף 6.8 ראה נספח 1 לדוח הבדיקה.

עוד הוסיפה עוזרת ראשית ליועמ"ש, כי עם כניסת התקנה לתוקף בשנת 2018, הוקם צוות על ידי סמנכ"ל לתכנון ארגון ומערכות מידע לצורך הטעמת התקנות בעירייה, לרבות עם ספקי מיקור החוץ, אשר בין היתר ערך מיפוי של ספקי מיקור חוץ להם גישה למאגרי המידע העירוניים ואף גיבש מסמך הצהרה לשמירה על סודיות הגנת הפרטיות ואבטחת מידע העומד בדרישות התקנות. מאחר והתווספת להסכם עם חברת "א.פ." (סעיף 6.8) הייתה מספקת ואף לא הייתה

שונה במהותה מהנוסח החדש, לא הועברה דרישה נוספת לספק לחתום על מסמך שמירת הסודיות בנוסח החדש.

48. עורכי הבדיקה יצינו בהקשר לכך, כי מאחר והגורם העירוני האחראי על ההתקשרות עם חברת "א.פ." היה אגף רכש ולוגיסטיקה, עורכי הבדיקה פנו בתחילה לבירור נושא החתימה על הנוסח המעודכן אל האגף. מנהל אגף רכש ולוגיסטיקה מסר לעורכי הבדיקה, כי לאגף אין מידע לגבי הדרישה להחתמת ספקים על מסמך ייעודי לשמירה על סודיות המידע כפי שנדרש בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

מנהל אגף רכש ולוגיסטיקה מסר בהתייחסותו לממצא, כי: "כפי שציינתי הנושא לא מוכר וחשוב שיובהר ויוסדר בצורה המתבקשת".

מנהל אגף מחשוב ומערכות מידע מסר בהתייחסותו לממצא, כי: "רכש ולוגיסטיקה (חוזים והתקשרויות) ביצעו/מבצעים התהליך קודם עם חוזים חדשים ומאוחר יותר על הוספת נספח לחוזים קיימים".

הערת עורכי הבדיקה:

מהתייחסות הנבדקים: אגף רכש ולוגיסטיקה ואגף מחשוב ומערכות מידע ניכר כי קיימת סתירה בין שתיהן. מחד גיסא נטען על ידי אגף רכש ולוגיסטיקה כי "הנושא לא מוכר וחשוב שיובהר ויוסדר בצורה המתבקשת" ומאידך גיסא נטען על ידי אגף מחשוב ומערכות מידע כי "רכש ולוגיסטיקה (חוזים והתקשרויות) ביצעו/מבצעים התהליך...". קיים חשש שתהליך חשוב של החתמת ספקים על התחייבויות לשמירה על סודיות ואבטחת מידע, בהתאם לדרישות תקנות הגנת הפרטיות, לא יתקיים בפועל.

שליחת הטופס לעובדי העירייה

כללי

49. תהליך מסירת הטופס לעובד לביצוע עדכון הפרטים התבצע כאמור, בשני מסלולים:

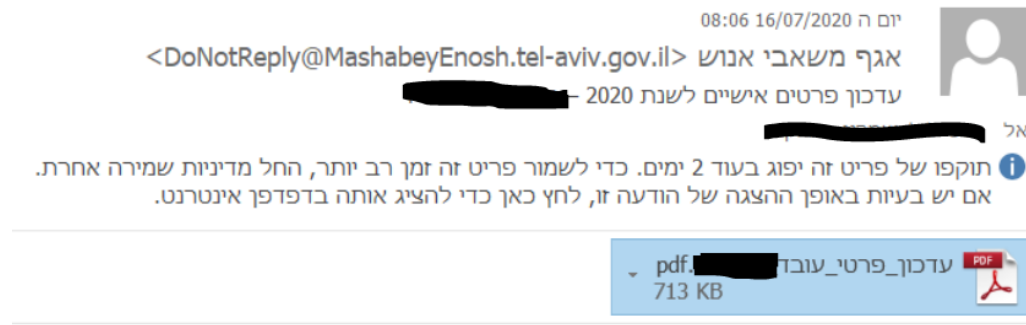
א. מסלול 1 – שליחת הודעת דוא"ל אל עובדי העירייה להם הוגדר מייל עירוני בנושא "עדכון פרטים אישיים לשנת 2020 – XXX (שם העובד)".

ב. מסלול 2 – הדפסת טופס "עדכון פרטים אישיים" לכל עובד ומסירתו ידנית לעובד לצורך עדכון הפרטים.

50. הבחירה בשני המסלולים הנ"ל נבעה בשל העובדה שלמחצית מעובדי העירייה לא הוגדר מייל עירוני.

ממצאים

51. במהלך חודש יולי הועברה אל עובדי העירייה, אשר הוגדר להם מייל עירוני, הודעת דוא"ל בבקשה לעדכון פרטיהם האישיים. להלן דוגמא להודעות דוא"ל שהועברה:



הודעת הדוא"ל כללה הנחיות למילוי והחזרת הטופס וכן מספר דגשים עליהם ביקשו באגף משאבי אנוש לשים לב בעת מילוי הטופס. לקריאת ההודעה המלאה ראה נספח 2.

52. מנהלת פרויקטים באגף מחשוב ומערכות מידע מסרה לעורכי הבדיקה, כי הפצת הודעת הדוא"ל בו נכלל "טופס עדכון פרטים אישיים" נעשתה באמצעות ספק בית הדפוס. העירייה סיפקה את כתובות הדוא"ל וספק בית הדפוס הפיץ ההודעות.

53. בהקשר לתהליך האמור, מסר מנהל מחלקת אבטחת מידע וסייבר בעירייה כי שליחת הודעת דוא"ל משרת חיצוני (ספק) לשרת פנימי (עירייה) בתוספת הכותרת של הודעת הדוא"ל – "עדכון פרטים אישיים לשנת 2020" הינה פרצה באבטחת המידע אשר בין היתר חושפת את הודעת הדוא"ל ליירוט על ידי גורם עוין.

54. עורכי הבדיקה ביקשו לבדוק האם בטרם ביצוע שליחת הודעת הדוא"ל אל עובדי העירייה, אשר הוגדר להם מייל עירוני, נערכו בדיקות על תהליך השליחה ותהליך הקבלה של הודעת הדוא"ל, במטרה לבחון שלמות ומהימנות שליחת הודעת הדוא"ל.

מנהל אגף משאבי אנוש מסר בהתייחסותו לממצא, כי: "אגף משאבי אנוש ביצע 'מסמכים' מדגמיים על תהליך השליחה ותהליך הקבלה של הודעות הדוא"ל בטרם נשלחו ההודעות בדוא"ל לעובדים".

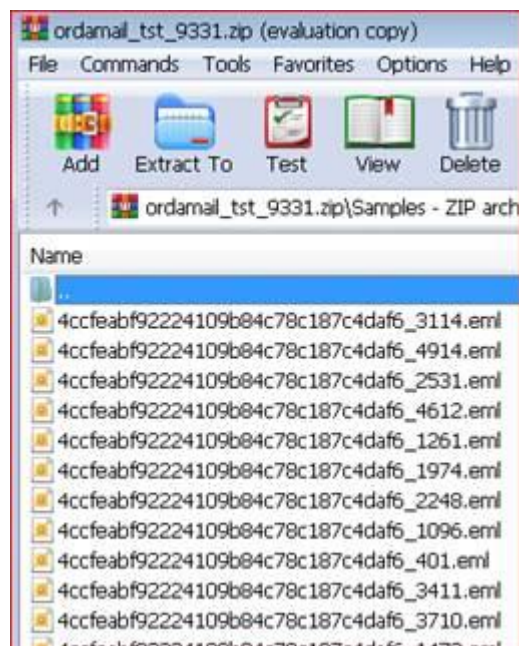
55. מנהלת פרויקטים באגף מחשוב ומערכות מידע העבירה לעיון עורכי הבדיקה צילום מסך "מערכת הדיוור העירוני". מסקירת צילום המסך עולה, כי הוא כולל תיעוד לבקשת הספק לביצוע הבדיקה על תהליך שליחת הודעת הדוא"ל, כדלהלן:

מעקב הזמנות - הזמנה מספר 9331

Drag a column header and drop it here to group by that column

מסר	פעולה	תאריך פעולה	יזם פעולה	סטטוס
+	אישור רגיל להזמנה	20/07/2020 10:01:33		אישור
+	סטטוס על הזמנה	16/07/2020 08:50:43	BizTalk	העלחה
	[BizTalk, 08:50:43 16/07/2020] הגיע קובץ , מספר הזמנה: 9331, פרטים: תחום:משאבי אנוש, שם הפעילות: עדכון פרטים אישיים - מייל, סוג ההפצה: דואר אלקטרוני			
+	שלוחת הזמנה	15/07/2020 12:40:02		אישור
+	יצירת הזמנה	15/07/2020 11:58:05	איציק אלטשולר	אישור

56. בנוסף, מנהלת פרויקטים העבירה תיעוד לקובץ הטסטים אשר הכיל הודעות דוא"ל אקראיות שנשלחו במסגרת הבדיקה, כדלהלן:



57. מנהלת פרויקטים מסרה לעורכי הבדיקה בהקשר לכך, כי: "תהליך הבדיקה של המופס במייל אינו שונה מהבדיקה של המופס המודפס. בית הדפוס שולח מסמים אקראיים של המיילים שאותם יפיץ אם יתקבל האישור מהלקוח העירוני. רק הסיומת של קבצי המסמים שונה כיוון שמדובר בקבצי eml ולא בקבצי pdf".

58. עוזרת ראשית ליועמ"ש בשירות המשפטי מסרה לעורכי הבדיקה, בהקשר לכך בין היתר כי: "לצורך כך, נשלח המידע האישי הקיים במאגר במישרין לכל עובד באמצעות המייל הפנים עירוני המאובטח. על פי ההנחיות בטופס המענה של העובד ובו עדכון הפרטים מוחזר לסגל משאבי אנוש ביחידה, לבנעל הרשאת גישה מתאימה. דרך זו מבטיחה שרק הגורם הרלוונטי ייחשף לפרטים האישיים שבטופס".

כאמור לעיל, תהליך שליחת הודעות הדוא"ל נעשה באמצעות ספק בית הדפוס זאת על אף טענתה של עוזרת ראשית ליועמ"ש שמסרה שמבחינתה התהליך תקין מאחר והוא בוצע "באמצעות המייל הפנים עירוני המאובטח".

עוזרת ראשית ליועמ"ש וסגנית בכירה ליועמ"ש ומנהלת תחום דיני עבודה מהשירות המשפטי מסרו לעורכי הבדיקה בהתייחסותן לממצא, כי: "השירות המשפטי למד לראשונה על שימוש במיקור חוץ לטובת העברת המידע מטימות הממצאים".

הערת עורכי הבדיקה:

עורכי הבדיקה מעלים חשש כיצד נושא רגיש של אבטחת פרטי העובדים לא הובא באופן מלא בפני השירות המשפטי.

59. סגנית בכירה ליועמ"ש ומנהלת תחום דיני עבודה בשירות המשפטי מסרה לעורכי הבדיקה בנוגע למעורבות השירות המשפטי בתהליך שליחת המסמכים במייל, כי: "לגבי הפצתו של הטופס במייל כתבנו: 'על פי ההנחיות בטופס יש להעביר אותו לסגל משאבי אנוש ביחידה. דרך זו מבטיחה שרק הגורם הרלוונטי ייחשף לפרטים האישיים שבטופס. נראה לי נכון וסביר'".

60. כאמור, כמחצית מעובדי העירייה קיבלו את הטופס עדכון הפרטים האישיים באמצעות הודעת דוא"ל. עורכי הבדיקה מצאו, כי העובדים אשר קיבלו את הטופס במייל נדרשו להדפיסו, לבצע תיקונים עליו באופן ידני ולאחר מכן להעבירו פיזית אל סגלי משאבי אנוש שביחידותיהם, בכדי שאלו יוכלו לעדכן את הנתונים במערכת.

61. מנהל אגף משאבי אנוש מסר לעורכי הבדיקה בהקשר לכך, כי בפעמים הבאות, בהם ידרשו העובדים לעדכן את פרטיהם האישיים באופן ייזום על ידי העירייה, קיימת כוונה שהתהליך יבוצע באופן ממון, כך שהעובדים ידרשו להתחבר למערכת ולעדכן בעצמם את הנתונים.

מעורבות גורמים עירוניים מקצועיים בפרויקט

כללי

62. תהליך בו מידע אישי ורגיש על עובדי העירייה (הרשום אף כמאגר מידע רגיש), מועבר לספק מיקור חוץ ובהמשך נשלח ממנו אל עובדי העירייה, באמצעות הודעת דוא"ל, ראוי כי יהיה מלווה ומבוקר על ידי גורמים עירוניים רלוונטיים (מחלקת אבטחת מידע וסייבר והשירות המשפטי).

ממצאים

63. עורכי הבדיקה מצאו, כי לא קיימת בנהל או בהנחיית עבודה, התייחסות לפעולות אותן יש לקיים, בתהליכים דוגמת התהליך שנבדק, בו מידע אישי ורגיש הרשום כמאגר מידע, מועבר אל ספקי מיקור חוץ לצורך עיבודו, ולאחר מכן נשלח מהם באמצעים טכנולוגיים אל תפוצה רחבה של אנשים.

מעורבות מחלקת אבטחת מידע

כללי

64. הנחיית רשם מאגרי מידע קובעת בסעיף 3.1.4.1 בנושא "אבטחת מידע ובקרה על פעילות במיקור חוץ", כי: "קיום חובת אבטחת המידע חייבת להיות תנאי יסודי בכל התקשרות לצורך ביצוע שירות מיקור חוץ".

65. בסעיף 3.1.4.2 בהנחיית רשם מאגרי מידע נקבע בין היתר, כי: "במסגרת אפיון השירות, עוד בטרם התקשרות, על המזמין לבחון ולהגדיר את האיומים והסיכונים הנובעים מסוג המידע המועבר לקבלן, ולקבוע את אמצעי אבטחת המידע להתמודדות עימם".

ממצאים

66. עורכי הבדיקה ביקשו לבדוק האם מחלקת אבטחת המידע וסייבר בעירייה, הכירו את התהליך המבוקר ואף ליוו אותו במתן דגשים בנושא אבטחת המידע. יצוין, כי מנהל מחלקת אבטחת מידע וסייבר בעירייה משמש גם כאחראי על אבטחת המידע במאגרים הרשומים בעירייה.

67. עורכי הבדיקה פנו בתחילת הבדיקה אל מנהלת אגף מיחשוב ומערכות מידע דאז על מנת לדעת מי הם הגורמים באגף שלקחו חלק בתהליך. בתשובתה השיבה מנהלת האגף כי: "מאצלנו הובילו את התהליך ה. (סי.מי.או. וארכיטקט ראשי) ומ. (מנהל מחלקת אבטחת מידע וסייבר). יחד עם זאת משאבי אנוש הובילו בפרקטיקה את המהלך".

68. במסגרת פגישה בנושא אותה קיימו עורכי הבדיקה עם CTO וארכיטקט ראשי ועם מנהל מחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע עלה, כי שניהם אינם מכירים את התהליך המדובר ואף לא היו שותפים לתהליך. עוד הוסיפו, כי נודע להם על התהליך רק עם קבלת הודעת הדוא"ל הכולל את "טופס עדכון הפרטים האישיים" בדומה לשאר עובדי העירייה.

מנהל אגף מחשוב ומערכות מידע מסר בהתייחסותו לטיטוט הממצאים, כי:

"מנהל אבטחת המידע וסייבר ו/או CTO וארכיטקט ראשי לא עודכנו מראש על תהליך עדכון הפרטים ובמידה וכן ניתן לבחון סוגיות רלוונטיות שעלו בדו"ח קודם לביצוע.

כמו כן, העובדה שקיים חיבור מאובטח בין העירייה לבתי הדפוס הדבר אינו מהווה תחליף לתהליך אישור שימוש במידע כפי שניתן מראש – כלומר עצם העובדה שספק מקבל את כל המידע על מנת לבצע את העבודה שבשבילה מועסק אינה מייתרת אישור ו/או הבניית תהליך סדור לשימוש במידע מהמאגר כדי לבצע פעולת אימות נתונים".

הערת עורכי הבדיקה:

התייחסות אגף מחשוב ומערכות מידע מחזקת את ממצאי הבדיקה.

69. CTO וארכיטקט ראשי מסר בנוסף, כי: "להערכתי נדרש בכל פעולה, אשר עיקרה העברת מידע אישי רגיש, לפעול מתוך הבנה של ניהול סיכונים ועמידה ברגולציה ונהלים וכל זאת בהתאם להנחיית גורמי המקצוע".

מנהל אגף משאבי אנוש מסר בהתייחסותו לממצאים 66 - 69, כי: "מנהל מחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע ציין כי ערוץ תקשורת (מערכת הדיוור העירונית) בין העירייה לספק הוא אכן ערוץ תקשורת מאובטח. כפי שצינו בפתח הדברים אגף משאבי אנוש פעל בהתאם לתנאי המכר".

הערת עורכי הבדיקה:

מתגובת אגף משאבי אנוש ניכר, כי לא נלקחו בחשבון מכלול הסיכונים בתהליך שבוצע והחשיפה הקיימת לרגולציה בנושא.

לוח השירות המשפטי

70. עורכי הבדיקה ביקשו לבדוק האם השירות המשפטי היה שותף לתהליך שבוצע לעדכון פרטים האישיים של העובדים. מנהל מחלקת מידע ובקרה באגף כוח אדם מסר לעורכי הבדיקה, כי: "השירות המשפטי לא היה מעורב בתהליך".

מנהל אגף משאבי אנוש מסר בהתייחסותו לממצא, כי: "אגף משאבי אנוש פעל בכפוף לתנאי מכרז 219/2018 להדפסת מסמכי דיוור וכן להפקת מסמכי דיוור לדואר אלקטרוני שהוזכר לעיל ושאושר גם על ידי השירות המשפטי. בנוסף, אגף משאבי אנוש העביר את המופס לשירות המשפטי לצורך קבלת חוות דעת לגבי הפרטים שהעובדים מתבקשים למלא במופס העדכון".

71. לצורך בירור מעורבות הגורמים העירוניים שלקחו חלק בתהליך, פנו עורכי הבדיקה בין היתר לסגנית בכירה ליועמ"ש ומנהלת תחום דיני עבודה בשירות המשפטי אשר מסרה לעורכי הבדיקה בנוגע לכך, כי:

"למיטב זכרוני, לפני שהופצה הבקשה לעדכון פרטים אישיים לעובדים, התבקש תחום דיני עבודה בשירות המשפטי לחוות דעתו לגבי הפרטים שהעובדים מתבקשים למלא בטופס העדכון. לגבי הפרטים המתבקשים בטופס לא כתבנו חוות דעת: העבירו לנו את הטופס, בחנו את הפרטים המתבקשים בו ואישרנו את הפרטים המתבקשים בו כפי שהוא הופץ בסופו של דבר".

עוזרת ראשית ליועמ"ש וסגנית בכירה ליועמ"ש ומנהלת תחום דיני עבודה מהשירות המשפטי מסרו לעורכי הבדיקה בהתייחסותן לממצא, כי:

"כפי שנוקבע בסעיף 70 למיומנות הממצאים, השירות המשפטי לא ליווה את תהליך עדכון הפרטים האישיים.

לפני תחילת התהליך השירות המשפטי נדרש אך ורק לשאלה אם ניתן לדרוש מהעובדים לחשוף בפני סגלי משאבי אנוש את הפרטים האישיים שצוינו בטופס העדכון, וקבע שכן.

במסגרת הביקורת (המענה במקור, מדובר בתהליך בדיקה), נתבקשה עמדת השירות המשפטי ביחס לסמכות של אגף משאבי אנוש לבקש ולקבל את עדכון הפרטים האישיים של העובדים, והשירות המשפטי חיווה דעתו בדבר קיומה של סמכות כאמור. השירות המשפטי הוסיף, כי האופן בו בוצעה העברת המידע מהעירייה לעובד (באמצעות הדוא"ל העירוני) ומהעובד לעירייה (במסירה פיזית לידי סגל משאבי אנוש ביחידה) הוא תקין ומבטיח את אבטחת המידע וחשיפתו למורשים בלבד.

השירות המשפטי למד לראשונה על שימוש במיקור חוץ לטובת העברת המידע ממיומנות הממצאים".

לתשומת לב:

התייחסויות המבוקרים ואחרים לטיטוט ממצאי הביקורת בשלב אימות הממצאים, מצורפות לדוח בפרק הנספחים, ומהוות חלק בלתי נפרד מדוח הביקורת. הנספחים להתייחסויות (אם צורפו) שמורים במשרד מבקר העירייה.

נספח א – השירות המשפטי מתאריך 20.1.2021.

נספח ב – אגף משאבי אנוש מתאריך 19.1.2021.

נספח ג – אגף רכש ולוגיסטיקה מתאריך 24.1.2021.

נספח ד – אגף מחשוב ומערכות מידע מתאריך 31.1.2021.

מסקנות

72. הנחיית רשם מאגרי מידע קובעת, כי: "על ארגון המבקש להוציא פעילות למיקור חוץ... לקיים הליך בחינה האם ראוי, לאור אופי המידע האישי שהשירות יתבקש לגביו ורגישותו, להעביר את המידע או את העיבוד שלו למיקור חוץ".
- מממצאי הבדיקה עולה, כי בניגוד להנחיה זו, לא בוצע הליך בחינה של האפשרויות הקיימות לאגף לביצוע עדכון הפרטים האישיים בין אם בחצרות העירייה בין אם באמצעות מיקור חוץ, טרם קבלת ההחלטה על הוצאת הפרויקט למיקור חוץ.
- עורכי הבדיקה סבורים, כי יש להעדיף עד כמה שניתן לבצע פעילויות הקשורות במידע הכלול במאגרי מידע עירוניים בחצרות העירייה ולא להעביר המידע או את עיבודו למיקור חוץ.
73. הנחיית רשם מאגרי מידע קובעת מספר מודלים להעברת המידע אל ספק הנותן שירותי מיקור חוץ כאשר המודל הפחות מומלץ לדעת רשם מאגרי מידע הוא "שירות המחייב העברה או העתקה של מאגר מידע שלם, או חלק מהותי ממנו, מהמזמין לקבלן". עורכי הבדיקה מצאו, כי לצורך ביצוע הפרויקט בחרה העירייה במודל שצוין כפחות מומלץ. עורכי הבדיקה סבורים, כי לו הייתה מתבצעת בחינה מקדימה של החלופות האפשריות להעברת המידע, עשויה הייתה להימצא דרך לשימוש במודל אחר עליו המליץ הרשם.
74. הנחיית רשם מאגרי מידע קובעת, כי: "על המזמין לדרוש מן הקבלן תצהיר המאמת ביצוע פעולות מחיקה, ביעור והשמדה של כל המידע שהגיע אליו במסגרת ההתקשרות עמו". עורכי הבדיקה מצאו, כי לא התקבל מהספק אישור על מחיקת מאגר המידע ואף לא נערך בירור מול הספק לוודא כי המידע אכן נמחק.
75. מממצאי הבדיקה עולה, כי מנהל אגף רכש ולוגיסטיקה לא היה מודע כלל לדרישה של השירות המשפטי, להחתים כל ספק ונותן שירותים הנעזר במאגר מידע עירוני רשום, על מסמך שמירת סודיות הגנת הפרטיות ואבטחת המידע, המתוקף בהתאם תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. לדעת עורכי הבדיקה קיימת חשיבות להביא את הנושא לידיעת כלל מנהלי היחידות העירוניות.
76. אחת הדרכים בהם השתמש אגף משאבי אנוש למסירת טופס "עדכון פרטים אישיים" לעובד הייתה באמצעות שליחתו בהודעת דוא"ל. מממצאי עורכי הבדיקה עולה, כי הפצת הודעת הדוא"ל נעשתה באמצעות ספק בית הדפוס. מנהל מחלקת אבטחת מידע וסייבר מסר, כי שליחת הודעת דוא"ל משרת חיצוני (ספק) לשרת פנימי (עירייה) בתוספת הכותרת של הודעת הדוא"ל – "עדכון פרטים אישיים לשנת 2020" מהווה פרצה באבטחת המידע אשר בין היתר חושפת את הודעת הדוא"ל ליירוט על ידי גורם עוין.

77. עורכי הבדיקה מצאו, כי השירות המשפטי לא היה מודע הן לגבי אופן גיבוש טופס עדכון הפרטים האישיים והן לגבי שליחתו לעובדי העירייה באמצעות מיקור חוץ. למעשה, רק בעת חשיפתו לטיוטת הממצאים הובהר לו לראשונה, כי הפרויקט בוצע באמצעות מיקור חוץ. לדעת עורכי הבדיקה, עדכון השירות המשפטי על הכוונה לבצע את הפרויקט באמצעות מיקור חוץ, עשוי היה לשנות את חוות הדעת שנתן.

78. כמחצית מעובדי העירייה קיבלו את הטופס עדכון הפרטים האישיים באמצעות הודעת דוא"ל. עורכי הבדיקה מצאו, כי העובדים אלו נדרשו להדפיסו, לבצע בו תיקונים ידניים ולאחר מכן להעבירו פיזית אל סגלי משאבי אנוש שביחידותיהם, בכדי שאלו יוכלו לעדכן את הנתונים במערכת. לדעת עורכי הבדיקה, תהליך זה שנבחר, לבד מהיותו חשוף לטעויות גרם גם לבזבז משאבים (נדרש עובד אחד למילוי הטופס ועובד אחד לעדכונו במערכת).

79. עורכי הבדיקה מצאו, כי לא הוגדרו בנוהל או בהנחיות עבודה, תהליכי עבודה אותם יש לקיים, במקרים בהם מידע אישי ורגיש הרשום כמאגר מידע, מועבר אל ספקי מיקור חוץ לצורך עיבודו, ולאחר מכן נשלח מהם באמצעים טכנולוגיים אל תפוצה רחבה של אנשים. עורכי הבדיקה סבורים, כי הגדרת מסגרות עבודה, מנגנוני בקרה וממשקים עם גורמים עירוניים וחיצוניים הינם חיוניים לשלמות התהליך ועמידתו בסטנדרטים מקובלים.

80. CTO וארכיטקט ראשי ומנהל מחלקת אבטחת מידע וסייבר באגף מחשוב ומערכות מידע אשר אמונים בשגרה על אבטחת המידע בארגון לא היו מודעים לתהליך המבוצע של עדכון הפרטים האישיים. למעשה, הפעם הראשונה שנודע להם על התהליך היה רק עם קבלת הודעת הדוא"ל הכוללת את "טופס עדכון הפרטים האישיים" בדומה לשאר עובדי העירייה. לדעת עורכי הבדיקה, אי שילובם של גורמים מקצועיים אלו בתהליך מעין זה עלול לחשוף את העירייה לסיכונים אבטחת מידע.

המלצות

81. בטרם הוצאת פעילות למיקור חוץ, באחריותו של הגורם העירוני המבקש להוציא מידע הכלול במאגר עירוני רשום למיקור חוץ, בשיתוף הגורמים הגורמים העירוניים המקצועיים, לקיים בחינה ולתעדה האם ראוי, לאור אופי המידע האישי שהשירות יתבקש לגביו ורגישותו, להעביר את המידע או את העיבוד שלו למיקור חוץ.

82. בעת בחינה של הוצאת פעילות למיקור חוץ תיבחנה החלופות האפשריות להעברת המידע באופן שישאיר את השליטה במידע, ככל הניתן, אצל הגורמים הממונים העירוניים.

83. יש לקבוע תהליך מוסדר מול ספק ונותן שירותים בו גורם עירוני יפקח על הפעולות המבוצעות על ידי הספק עם מידע עירוני לרבות פיקוח על פעולות מחיקה, ביעור והשמדה של כל המידע שהגיע אליו.
84. באחריות מנהלי היחידות בשיתוף השירות המשפטי להקפיד על יישום התהליך המבוצע להחתמת ספקים על מסמך שמירת סודיות הגנת הפרטיות ואבטחת המידע, המתוקף בהתאם תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.
85. מומלץ לפעול בהקדם למיכון תהליך עדכון הפרטים האישיים של העובדים כך שבמקרים בהם עובד מעוניין באופן נקודתי לעדכן את פרטיו תהיה לכך אפשרות ממוכנת באופן מלא, ולא באמצעות השלמת התהליך בטפסים ידניים.
86. יש לקבוע בנוהל או בהנחיית עבודה את הפעולות אותן יש לקיים, בעת העברת פעילות הכוללת נתונים הכלולים במאגר מידע עירוני רשום, למיקור חוץ. יש לקבוע את הגורמים המעורבים הנדרשים להתייעץ איתם במסגרת אותם פעולות.

נספח 1 – סעיף 6.8 למפרט הטכני – נספח ב' לחוזה עם חברת א.פ.

- 3.1 העירייה מודיעה בזאת על הוספת סעיף 6.8 למפרט הטכני – נספח ב' לחוזה, שנוסחו יהא כדלקמן:
- 6.8 הספק מצהיר ומתחייב כי יפעל בכל הקשור והנוגע לחוזה זה על נספחיו בהתאם לקבוע בהנחיות רשם מאגרי המידע בעניין שימוש בשירותי מיקור חוץ ובהתאם לסעיף 15 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 אשר פורסמו ביום 8/5/17 ואשר תחולתן מיום 8/5/18 בכלל ובהתאם להנחיות המפורטות להלן בפרט:
- 6.8.1 הנתונים המועברים ע"י העירייה (להלן-המידע) ישמשו אך ורק לביצוע המטרה/ הפעילות המקורית שלשמה הועברו לספק.
- 6.8.2 גישה למידע תהיה נתונה אך ורק לעובדי הספק אשר קיבלו הרשאה לכך ואך ורק לצורך ביצוע המטרה/הפעילות המקורית שלשמה הועבר.
- 6.8.3 בעלי הרשאה למידע מטעם הספק יחתמו על מסמך שמירת סודיות המידע.
- 6.8.4 הספק יעמוד במסמך אבטחת מידע מחייב המצורף כנספח ד' לחוזה.
- 6.8.5 הספק לא יעביר את המידע לצד שלישי כלשהו.
- 6.8.6 הספק יפריד את הפעילות המבוצעת עבור העירייה בהתאם לחוזה זה, מיתר הפעילויות המבוצעות על ידו.
- 6.8.7 הספק ידווח לעירייה באופן שוטף בכל הנוגע לאופן ניהול המידע ועיבודו.
- 6.8.8 הספק ידווח לעירייה על כל חריגה בשימוש ו/או בגישה למידע של העירייה ו/או על כל מקרה של חשש לדליפת מידע ו/או אירוע אבטחה.
- 6.8.9 לעירייה שמורה הזכות לפקח על פעילותו של הספק בקשר למידע לרבות עריכת ביקורת אצל הספק ובחינת השימוש במידע ואבטחתו.
- 6.8.10 פרק הזמן שמותר לספק להחזיק במידע לצורכי ביצוע עבודתו הינו עד 60 יום מיום העברת מסמכי הדיור לעירייה ו/או לספק החלוקה. בחלוף זמן זה על הספק למחוק את כל המידע שברשותו שהגיע אליו מהעירייה, בכל אמצעי מדיה.
- 6.8.11 עם סיום ההתקשרות יצחיר הספק בפני העירייה על ביצוע פעולות מחיקה וביעור של כלל המידע שהועבר לספק מהעירייה במסגרת ההתקשרות.

נספח 2 – הודעת הדוא"ל שהועברו אל עובדי העירייה בבקשה לעדכון הפרטים האישיים



עיר ללא הפסקה

אגף משאבי אנוש שמח להעביר לך טופס לעדכון פרטים אישיים. הטופס מציג את פרטיך כפי שהם מופיעים במערכת משאבי אנוש. עליך להדפיס את הטופס, לבדוק את הנתונים המופיעים בו ובמקרה של נתון חסר או לא מעודכן להשלים בשורה מתחת. יש לצרף אסמכתאות מתאימות כגון צילום תעודת זהות, מסמך רשמי על חשבון בנק ועוד. בתום המילוי יש לחתום על הטופס ולהעבירו לסגל משאבי אנוש ביחידתך, גם אם אין שינוי, עד 31.8.2020.

מספר דגשים

1. מצב משפחתי, סעיף 5 – יש לוודא כי המצב המשפחתי מעודכן כפי שהוא מופיע בתעודת הזהות.
2. עובדים שמצבם המשפחתי שונה מהרשום בתעודת הזהות (פרוד או ידוע בציבור), יכולים לדווח על כך בסעיף 4.
3. יש לוודא שהפרטים המופיעים בסעיף 7 בטופס אכן נמצאים ברשותך.
4. חשוב לעדכן בטופס את כתובת הדואר האלקטרוני (מייל) ומספר טלפון נייד כדי שהודעות אגף משאבי אנוש יגיעו אליך במסרון sms.
5. חשוב לציין בסעיף 16 על הסכמתך לקבל מידע עירוני בדואר אלקטרוני ובמסרון sms.

אגף משאבי אנוש

חשוב מאוד לעדכן פרטי מוטבים בכל אחת מקופות הגמל, בקרן ההשתלמות ובקרן הפנסיה. עדכון מוטבים חשוב בעת שינויים במצב משפחתי: נישואים, גירושין, לידת ילד וכו'. פרטים אלה ניתנים לבדיקה בדוחות התקופתיים המתקבלים מהקרן.

לעובדים שהצטרפו לביטוח בריאות ושיניים של הפניקס מומלץ לבדוק את הזכאות של בני המשפחה ואת הניכוי המתאים בהתאם בתלוש השכר.



חשוב לעדכן בטופס המצורף את כתובת הדואר האלקטרוני (מייל) ואת מספר הטלפון בכדי שהודעות אגף משאבי אנוש יגיעו אליך במסרון (sms) כדי להיכנס לפורטל לחץ כאן

אופיין והופק בעיריית תל אביב ע"י

אמ"א | אגף מחשוב ומ"מ | הוצאה לאור או"ת