15 בפברואר 2024
ו' באדר א', התשפ"ד

איסוף ושימוש במידע ביומטרי לדיווח ולבקרת נוכחות עובדים במקום העבודה

נוסח מעודכן בעקבות תיקון 13

מבוא

1. בשנים האחרונות משתמשים ארגונים בטכנולוגיות לזיהוי או אימות ביומטרי לדיווח ולבקרת נוכחות עובדים במקום העבודה, וזאת לרוב במסגרת כניסה ויציאת עובדים ממקומות עבודה (check-in & access), ותוך שימוש בשעון נוכחות ביומטרי.

2. שימוש זה מציב אתגר בנוגע להגנה ולכיבוד זכותם של עובדים לפרטיות. מטרת המסמך היא להציב זרקור על התופעה ועל הסיכונים לפרטיות הגלומים בה, לסקור את הרקע המשפטי הרלוונטי, ולהציג לארגונים הנחיות והמלצות בעניין זה.[1]

3. המסמך מיועד בעיקרו לארגונים פרטיים וציבוריים המשתמשים, או שוקלים להשתמש, בטכנולוגיות זיהוי ביומטרי של עובדים. **המסמך מבקש להרחיב ולעדכן את עמדת הרשות להגנת הפרטיות (להלן: 'הרשות') בנושא, כפי שבאה לידי ביטוי במסמך 'שימוש בבקרת נוכחות ביומטרית במקום העבודה'**, שפרסמה הרשות בשנת 2012.[2] עוד יצוין כי המסמך עומד בהלימה עם העקרונות המפורטים במסמך המדיניות הלאומית ליישומים ביומטריים בישראל של מערך הסייבר הלאומי.[3]

4. יובהר כי המסמך אינו מבקש לאסור את השימוש בטכנולוגיות לזיהוי ביומטרי של עובדים למטרות של דיווח נוכחות ומעקב אחר שעות עבודה, אלא רק להבטיח כי הוא ייעשה תוך מתן התייחסות הולמת לפרטיותם של העובדים. עוד יובהר כי המסמך אינו עוסק בשימוש במערכות ביומטריות לזיהוי כלל הנכנסים בכניסה לבתי עסק לצרכי אבטחה וביטחון, אלא אך ורק בנושא בקרת נוכחות עובדים במקום העבודה.

זיהוי ביומטרי במקומות עבודה – רקע

5. ככלל, זיהוי ביומטרי הוא זיהוי אדם באמצעות מאפיינים אנושיים, פיזיולוגיים וייחודיים שלו, כגון טביעת האצבע של אדם, קולו או תווי פניו (Physical biometrics), או באמצעות מאפיינים

---

[1] מסמך זה עוסק באיסוף ושימוש במידע ביומטרי לבקרת נוכחות במקום העבודה. עם זאת, הדברים האמורים בו הם נכונים, בשינויים המחויבים, גם בנסיבות בהן איסוף המידע הביומטרי לשם לבקרת נוכחות עובדים ולמעקב אחר שעות עבודתם נעשה במסגרת של העסקת עובדים באופן מקוון ומרחוק. להרחבה בנושא פרטיות עובדים במסגרת העסקה מרחוק ראו: הרשות להגנת הפרטיות "היבטי פרטיות במעקב אחר עובדים בעבודה מרחוק" (17.5.2023).

[2] הרשות למשפט, טכנולוגיה ומידע "שימוש בבקרת נוכחות ביומטרית במקום העבודה" (18.12.2012). ראו גם הרשות להגנת הפרטיות "שימוש במידע ביומטרי בשעון הנוכחות בעבודה – שאלות ותשובות" (27.10.20), הרשות להגנת הפרטיות "בקרת נוכחות ביומטרית במקום העבודה" (27.10.20).

[3] מערך הסייבר הלאומי, היחידה להזדהות וליישומים ביומטריים "מדיניות לאומית אינטגרטיבית ליישומים ביומטריים" (2.11.2016), (להלן: 'מסמך מדיניות לאומית ליישומים ביומטריים').

התנהגותיים שלו, כגון צורת הליכתו (Behavioral biometrics), הניתנים למדידה ממוחשבת ולשימוש לזיהוי אוטומטי. זיהוי ביומטרי נועד על-פי רוב לתת מענה לשאלה מיהו האדם המבקש להזדהות, ולאמת את זהותו.

6. מידע ביומטרי הוא מידע שאדם "נושא" עמו באופן תמידי, ואשר למעשה מהווה חלק ממנו. ככלל, מידע ביומטרי של אדם בוגר הוא קבוע ואינו משתנה באופן קיצוני לאורך מרבית שנות חייו, משכך הוא מאפשר זיהוי חד ערכי של האדם. מידע ביומטרי מהווה אפוא מעיין "מפתח" אוניברסלי לזיהוי אדם.

7. שימוש ארגונים בטכנולוגיות לזיהוי ביומטרי של עובדים נעשה, על-פי רוב, למטרות דיווח ובקרת נוכחות עובדים, קרי לשם מעקב אחר שעות הימצאותם במקום העבודה.[4] ככלל, לשם שימוש בטכנולוגיות אלו מבקשים מעסיקים לאסוף ולשמור נתונים ביומטריים של עובדיהם במאגרי מידע הנמצאים בבעלותם או בחזקתם. על פי רוב, נתונים אלו נבדקים ומושווים עם הנתונים הביומטריים של העובדים אשר נקלטים בכניסתם וביציאתם ממקום העבודה.

8. ככלל, קיימות מגוון של טכנולוגיות העשויות לאפשר זיהוי ביומטרי של עובדים בעת כניסה למקומות עבודה ויציאה מהם, כגון:

   א. סריקת טביעת אצבע;

   ב. זיהוי פנים של עובד;

   ג. זיהוי ביומטרי לפי קשתית העין (iris scanning);

   ד. סריקת כף יד, לרבות סריקת צורת ותווי כף היד של העובד, וסריקת כלי הדם מתחת לעור כף היד, לשם ניטור וזיהוי מבנה העורקים, הורידים והנימים בכף היד.[5]

חלק מהטכנולוגיות האמורות נמצאות כבר היום בשימוש ארגונים בארץ ובעולם. יצוין כי בעתיד קיימת סבירות שנהיה עדים לשימוש הולך וגובר של ארגונים גם בטכנולוגיות לזיהוי ביומטרי המבוססות על זיהוי תכונות התנהגותיות של עובדים, כגון דפוס וצורת הליכתם. כמו כן, בעתיד ייתכן ולא יהיה צורך במגע או בקרבה פיזית למכשירים לשם ביצוע הזיהוי.

<u>זיהוי ביומטרי – יתרונות וסיכונים לפרטיות</u>

9. ככלל, העובדה שמידע ביומטרי הוא קבוע ולא ניתן לשינוי, מהווה מצד אחד יתרון כאשר מדובר בצורך וביכולת לזהות אדם באופן ודאי. לתכונה זו יתרונות נוספים, לרבות בכל הנוגע לפרטיות ואבטחת מידע.

---

[4] חוק הגנת השכר, התשי"ח-1958 וחוק שעות עבודה ומנוחה, התשי"א-1951 יוצרים חובה לרישום שעות עבודה כבסיס לתשלום השכר וקיום חובות המעסיק כלפי עובדיו. להרחבה בנושא ראו: זרוע העבודה, "חובת רישום שעות עבודה ומנוחה שבועית" (18.1.2021).

[5] תחת רשימה זו מפורטות טכנולוגיות המשמשות כבר כיום למטרת דיווח ובקרת נוכחות עובדים במקום העבודה (כגון טכנולוגיות לזיהוי פנים וסריקת טביעות אצבע), וכאלו העשויות להיות בשימוש למטרה זו בעתיד.

10. כך לדוגמה, שימוש במערכות ביומטריות לאיסוף ושמירת מידע אישי עשוי להפחית את הסיכון למקרים של גישה לא מורשית או חדירה ללא הרשאה למאגרי המידע, ומכאן להפחית את האפשרות של זליגת מידע ודלף מידע ממאגרים אלו, ואת האפשרות לשימוש פסול במידע.

11. עם זאת, שימוש שכזה טומן בחובו גם סיכונים שונים לפרטיות, כגון: איסוף המידע שלא על יסוד הסכמה חופשית ומדעת של העובדים, וזאת בשל פערי כוחות בין עובדים למעסיקים;[6] הגברת תחושת המשטור והפגיעה בתחושת השליטה של עובדים על המידע האישי הנוגע אליהם;[7] גניבתו של המידע, זליגתו וחשיפתו ברבים; ושימוש במידע למטרות השונות מהמטרה שלשמה נאסף המידע מלכתחילה.[8]

12. בנוסף, החזקת נתונים ביומטריים של עובדים במאגר מידע מרכזי המוחזק אצל מעסיק (או אצל גורם חיצוני המחזיק בו עבור המעסיק), להבדיל משמירתו על גבי כרטיס חכם אישי בלבד הנתון לשליטתו הבלעדית של העובד, מעלה במידה משמעותית את סיכוני אבטחת המידע הנוגעים לו ואת הסיכון באובדן השליטה במידע הביומטרי הנוגע אליו.[9]

13. בכל הנוגע לזליגת המידע יצוין גם, שככל שהשימוש במידע ביומטרי כאמצעי לזיהוי ילך ויגבר (לדוגמה במסגרת רכישת מוצרים וקבלת שירותים, או במסגרת שימושים פרטיים כגון זיהוי ביומטרי בכניסה לבתי מגורים), כך סביר כי יגבר גם התמריץ של גורמים עבריינים לגניבתו של המידע הביומטרי ולשימוש בו לצרכים פסולים.

14. בשל כך שנושא מידע אינו יכול לשנות את מאפייניו הביומטריים, הרי שדלף מידע ביומטרי והגעתו לידי גורמים שאינו מורשים, חושפים את נושא המידע לשלל בעיות, כגון: גניבת זהותו וניסיונות גישה לנכסיו ושירותיו המקוונים השונים, שימוש במידע הביומטרי שלו בכדי להסיק מידע נוסף על אודותיו (כגון מחלות), כמו כן תתכן מניעת שירות מאדם עקב שגיאת המערכת באימות הזהות שלו.[10]

<u>פסיקות בתי הדין לעבודה ועמדות היועץ המשפטי לממשלה</u>

15. הזכות לפרטיות היא זכות יסוד בעלת מעמד על-חוקתי, וזאת בהתאם להוראות סעיף 7 לחוק יסוד: כבוד האדם וחירותו. ככלל, לעובד עומדת הזכות לפרטיות גם במקום העבודה. ואולם,

---

[6] לאור כך, הסכמת עובדים לפגיעה בפרטיותם במסגרת יחסי עבודה נתפסת כ'הסכמה חשודה'. להרחבה ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה** 253 (2010).

[7] ראו מיכאל בירנהק "מעקב בעבודה: טיילור, בנת'האם והזכות לפרטיות" **עבודה, חברה ומשפט** יב 8, 34 (2008). ראו גם טל גולן "העין הבוחנת והצופה: הסדרה ומשטור של התנהגות עובדים במקום העבודה" **משפט, חברה ותרבות - מסדירים רגולציה: משפט ומדיניות**, 515 (2016). סיכון זה צוין גם בחוות דעתו של היועץ המשפטי לממשלה בנוגע לשימוש במצלמות מעקב במקומות עבודה. ראו פס' 49-50 לחוות דעת היועץ בסע"ש (ת"א-יפו) 45564-12-17 **גליה כהן נ' אל על נתיבי אויר לישראל בע"מ** (פורסם בנבו, 27.7.2022), (להלן: 'עניין כהן').

[8] פרופ' לימור עציוני טענה בעניין זה כי " ... איסוף ואחסון של נתונים ביומטריים של עובדים מעלים חששות לגבי שימוש נאות במידע האישי המצטבר". לימור עציוני "השימוש בטכנולוגיות ביומטריות – היבטים נורמטיביים ומשפטיים" **סייבר, מודיעין וביטחון** 3 85, 87 (2012).

[9] סיכונים אלו חלים, גם אם במידה מעט פחותה, הן בשימוש במערכות השומרות רק נתונים חלקיים של מידע ביומטרי, והן במערכות שאינן שומרות את הנתון הביומטרי עצמו אלא רק מידע מקודד המיוחס לו.

[10] מצב זה מוגדר כמניעת שירות עקב דחיה שגויה של טענת הזדהות (FRR).

זכות זו אינה מוחלטת ויש לאזנה מול אינטרסים של המעסיק, לו עומדת הפררוגטיבה לנהל את עסקו. עם זאת, **פררוגטיבה זו כפופה לדרישות הסבירות, המידתיות תום הלב וההגינות**.[11]

16. ככלל, וכפי שנקבע בעניין **איסקוב**, מעסיק המבקש לנקוט בפעולה הפוגעת בפרטיות עובד נדרש לעמוד במספר עקרונות. עיקרון אחד הוא עיקרון **הלגיטימיות**, לפיו הפעולה תתבצע רק מטעמים שיש בהם עניין רלבנטי ישיר של המעסיק ומתוך אינטרס לגיטימי של צרכי העבודה. עיקרון שני הוא **המידתיות**, שבמסגרתו על המעסיק לוודא כי הפעולה היא חיונית לאינטרס לגיטימי של מקום העבודה. לפי עיקרון זה, על מעסיק לבחון, בין היתר, האם ישנן חלופות הפוגעות במידה פחותה בפרטיות העובדים, ולבחון האם תכלית הפעולה מצדיקה את הפגיעה בפרטיותם. כאמור בעמדת היועץ המשפטי לממשלה בעניין **כהן**,[12] אשר עסקה בסוגיית הצבת מצלמות מעקב במרחב הציבורי שבמקומות עבודה, מעסיק אינו רשאי לפגוע בפרטיות עובדיו שלא בהתאם למבחני התכלית הראויה והמידתיות.

17. עיקרון מרכזי נוסף הוא עיקרון **השקיפות**, לפיו על מעסיק להביא לידיעת עובדיו, בפירוט ובבירור, את מדיניותו בנוגע לפעולתו ואת אופן יישומה בפועל. כמו כן, על מעסיקים לאפשר לעובדים גישה למידע שנצבר עליהם, ולהודיע להם על משך הזמן בו ייאגר המידע שנצבר.[13]

18. מעבר לכך, בית הדין קבע כי פעולה הפוגעת בפרטיות עובד צריכה להיעשות **בהסכמתו**, הניתנת במפורש, בדעת ומתוך רצון חופשי. כמו כן, על פי עיקרון **צמידות המטרה**, מעסיק אינו רשאי להשתמש במידע שנאסף במסגרת פעולתו למטרות החורגות מהמטרה הראשונית לשמה נאסף, ועל מעסיקים להקפיד על דיוק המידע שנאסף, סודיותו, ואבטחתו.[14]

19. פסק דין משמעותי שעסק ספציפית בסוגיית איסוף מידע ביומטרי לצרכי בקרת נוכחות במקומות עבודה הוא פסק הדין של בית הדין הארצי לעבודה בפרשת **קלנסווה**.[15] בפסק דין זה נקבע כי **טביעת אצבע היא מידע פרטי-אישי של אדם, ומסירתה לאחר פוגעת, כבר בעצם המסירה, בפרטיות ובאוטונומיה של המוסר. פגיעה נוספת ונפרדת בפרטיות ובאוטונומיה נגרמת כתוצאה מהסיכון הכבד לשימוש לרעה בטביעת האצבע או לשימוש בה שלא למטרה שלשמה נמסרה**.[16]

---

[11] ע"ע (ארצי) 90/08 **טלי איסקוב ענבר נ' מדינת ישראל - הממונה על חוק עבודת נשים** (פורסם בנבו, 8.2.2011) (להלן: 'עניין איסקוב'), פסקה 10 לפסק דינה של השופטת ארד.

[12] עניין כהן, לעיל ה"ש 7. בחוות דעתו הבהיר היועץ כי ככלל, למעסיק עומדת הזכות והחובה לקיים רישום מהימן של שעות העבודה של עובדים, וכי הוא רשאי אף לפקח על רישום כאמור, והכל מכוח הפררוגטיבה שלו לנהל את עסקו בדרך הטובה ביותר ולהקפיד על דיווחי אמת. נטען כי זכות זו נגזרת מזכותו הקניינית של המעסיק, הכוללת את זכותו למידע אמין בדבר שעות עבודתו של העובד. הובהר כי דיווחי שקר הם תופעה פסולה וחמורה אשר טמונה בה פגיעה פוטנציאלית בקניין המעסיק. ראו פס' 97-99 לעמדת היועץ.

[13] עניין איסקוב, לעיל ה"ש 11, פסקה 26ה לפסק דינה של השופטת ארד.

[14] שם.

[15] עס"ק (ארצי) 7541-04-14 **הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי - עיריית קלנסווה** (פורסם בנבו, 15.3.2017), (להלן: 'עניין קלנסווה').

[16] שם, בפס' 89 לפסק דינו של השופט איטח.

לאור האמור קבע בית הדין הארצי לעבודה כי למרות שאין פסול בשימוש מעסיקים במערכות לדיווח נוכחות עובדים המבוססות על טביעות אצבע, הרי שאין למעסיקים סמכות בדין לחייב עובדים למסור מידע ביומטרי לצרכי דיווח נוכחות, וכי ניתן להכשיר פגיעה שכזו בפרטיותם של עובדים רק בחוק או מכוח הסכמה שניתנה כדין.

20. בית הדין עסק בהרחבה גם בסוג המידע שעל מעסיק להציג לעובדיו כאשר הוא מבקש את הסכמתם לאיסוף מידע ביומטרי שלהם:

> "קודם לבקשת הסכמתן של עובדות החינוך היה על העירייה להציג להן מידע מקיף ומפורט, ובכלל זה (ולא כרשימה ממצה): הסבר מפורט מה 'ניטל' מהן; מי הם ה'טכנאים' שייטלו מהן את טביעות האצבע ומה הכשרתם; האם טביעות האצבע נשמרות ב'מאגר'; מי אחראי על המאגר ולמי יש גישה אליו ואל המידע האצור בו; האם המידע שנשמר, נשמר בצמידות לפרטי זיהוי אישיים אחרים; מהן דרכי האבטחה של אותו מידע; מהן הסכנות האפשריות; האם לגורמים חיצוניים יש אפשרות להתחבר ל"מערכת" מבחוץ או שמא מדובר במערכת 'מבודדת'; האם ניתן להעתיק את טביעת האצבע מיחידות הקצה (הסורקים) – בין בצורה דיגיטאלית ובין בצורה אחרת; מי בודק ומתי האם מידע זה נשמר או שמא נעשה ניסיון שלא כדין לגשת אליו; כיצד ומתי מוחקים מידע מאותו מאגר; מי הממונה בעירייה על כל אלה ומי אמון על מתן תשובות לשאלות, תהיות וכיוצ"ב בקשות לקבלת מידע".[17]

<u>הבהרות והמלצות הרשות להגנת הפרטיות</u>

21. מידע ביומטרי הוא מידע ייחודי. לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות'), מידע אישי שהוא מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב, מהווה "מידע בעל רגישות מיוחדת".[18] ככלל, למעסיקים עומדת הפררוגטיבה לאסוף ולהשתמש במידע ביומטרי לדיווח ולבקרת נוכחות עובדים במקום העבודה. עם זאת, **איסוף המידע והשימוש בו חייבים להיעשות באופן סביר ומידתי, תוך יידוע העובדים וקבלת הסכמתם לכך, תוך יישום כללי אבטחת המידע, ותוך הקפדה על עיקרון צמידות המטרה**.

22. להלן יפורטו מספר כללי אצבע והמלצות מרכזיות ליישום עקרונות אלו. יודגש כי הכללים והעקרונות שיפורטו להלן רלוונטיים לכל סוגי המידע הביומטרי, לרבות טביעות אצבע, זיהוי פנים, זיהוי קשתית העין, וזיהוי תכונות התנהגותיות של עובדים, כגון דפוס וצורת הליכתם.

---

[17] שם, בפס' 144 לפסק דינו של השופט איטח.

[18] סעיף קטן (4) להגדרת "מידע בעל רגישות מיוחדת" בסעיף 3 לחוק הגנת הפרטיות. מזהה ביומטרי, כהגדרתו בחוק, מהווה "נתון ביומטרי המשמש לזיהוי אדם או לאימות זהותו, או אמצעי ביומטרי שניתן להפיק ממנו נתון כאמור; לעניין הגדרה זו, 'ביומטרי – מאפיין אנושי, פיזיולוגי או התנהגותי, ייחודי, הניתן למדידה ממוחשבת'". עוד יצוין כי על-פי הקבוע בתוספת השלישית לחוק הגנת הפרטיות, מאגר מידע שיש בו מזהים ביומטריים של 100,000 בני אדם ומעלה, מהווה מאגר מידע שחלה עליו רמת האבטחה הגבוהה.

כמו כן יובהר כי הכללים והעקרונות האמורים נכונים, בשינויים המחויבים, גם כאשר מעסיקים נעזרים בגורם חיצוני לאיסוף ולשימוש במידע הביומטרי לצרכי בקרת נוכחות עובדים במקום העבודה.

<u>מידתיות, הצדקה לאיסוף ושימוש במידע ביומטרי ובחינת חלופות</u>

23. איסוף מידע ביומטרי טומן בחובו פגיעה קשה בפרטיות, בפרט במסגרת יחסי עבודה. לפיכך, על מעסיקים המבקשים להשתמש במערכות ביומטריות לדיווח ובקרה על נוכחות עובדים ולפיקוח על שעות העבודה, להבטיח כי שימושם במערכות אלו נעשה באופן מידתי. בהקשר זה מוטלת על מעסיקים **החובה להצדיק את הבחירה בשימוש במערכות אלו, על יסוד אינטרסים לגיטימיים שלהם חרף הפגיעה בפרטיות** (כגון קשיים בפיקוח על נוכחות עובדים במקום העבודה), וזאת בין היתר נוכח קיומן של **חלופות** אפשריות אחרות הפוגעות במידה פחותה בפרטיות העובדים.[19]

24. במסגרת זו על מעסיקים לבחון את אפשרות השימוש בחלופות הפוגעות במידה פחותה בפרטיות העובדים. להלן מוצעות מספר חלופות אפשרויות לבחינה:

א. חלופה רצויה אחת היא שימוש מעסיקים באמצעים לדיווח ומעקב אחר שעות עבודה שפגיעתם בפרטיות היא הפחותה ביותר, כגון כרטיסי עובד שאינם כוללים מידע ביומטרי.

ב. אם נמצא כי שימוש בכרטיסי עובדים לבדם אינו מספק, מעסיקים יכולים לשקול התקנת מצלמות שאינן ביומטריות המצלמות את אזור שעון הנוכחות בלבד, אשר צילומיהן ייבחנו רק כשיעלה חשש כי עובד מסוים אינו מדווח בצורה אמינה על שעות עבודתו. שימוש ספציפי, ממוקד ונקודתי שכזה במצלמות שאינן ביומטריות, במקביל לשימוש בכרטיסי עובדים, עשוי לאפשר למעסיקים לפקח בצורה נאותה ומידתית על שעות העבודה, וזאת ללא צורך באיסוף ושימוש במידע ביומטרי.[20]

ג. חלופה נוספת עשויה להיות שימוש במידע ביומטרי במקום העבודה באופן שבו המידע כלל אינו נאסף למאגר מידע, אלא נשמר על גבי כרטיסים חכמים בלבד. לפי שיטה זו, המאפיינים הביומטריים של העובד אינם מושווים עם מאגר מרכזי, אלא עם הנתונים הדיגיטליים שלו (כגון התבנית הדיגיטלית של טביעת אצבע) השמורים על הכרטיס

[19] סעיף 5.1.4 למסמך מדיניות לאומית ליישומים ביומטריים', לעיל ה"ש 3, קובע לעניין זה כי "ההחלטה על שימוש במערכת ביומטרית נדרשת להישען על ניתוח מקדים שייעשה בגוף ויתועד על ידו. הניתוח המקדים יתועד ויכלול שקילת חלופות לעצם השימוש ביישומים ביומטריים, כולל ניתוח היתרונות אל מול הסיכונים הכרוכים בכך ... התיעוד נועד לוודא שהחלטות בעניין זה אינן מתקבלות כלאחר יד, אלא רק לאחר שנבדקו השיקולים השונים".

[20] גישה ברוח דברים אלו הוצגה על-ידי הסתדרות העובדים החדשה בעניין קלנסווה. כך, בפס' 42 לפסק דינו של השופט איטח צוין כי לגישת ההסתדרות, "ניתן לוודא אמינות דיווח באמצעים שאינם מצריכים חדירה למתחם הפיזי של העובד, דוגמת מצלמה המצלמת את שעון הנוכחות ואת העובדים המחתימים בו את כרטיסם, ולכן חיוב עובד ליתן טביעת אצבע מהווה דרישה שאינה סבירה ואינה מידתית".

החכם בלבד. לגישת הרשות, חלופה זו מאפשרת ניצול של יתרונות הטכנולוגיה הביומטרית שמאפשרת זיהוי וודאי של העובד מחד, אך אינה יוצרת סיכונים עודפים לפרטיות של העובדים, מאידך.[21]

ד. חלופה מידתית נוספת עשויה להיות העמדת המערכות הביומטריות רק לשימושם של עובדים המסכימים לכך, תוך העמדת חלופה סבירה לעובדים המסרבים לעשות כן.

25. יובהר כי לגישת הרשות, איסוף מידע ביומטרי למאגר מידע ושימוש בו במסגרת מקום העבודה עשוי להיחשב צעד בלתי מידתי, אלא אם קיימת הצדקה לדברים (כגון קושי ספציפי של מעסיקים לפקח על נוכחות עובדים במקום העבודה) ואין בנמצא חלופה סבירה אחרת.

<u>יידוע עובדים</u>

26. על מעסיקים המבקשים לאסוף ולהשתמש במידע ביומטרי של עובדיהם לצרכי בקרת נוכחות **ליידע אותם באופן נרחב** בכל הנוגע לאופן איסוף המידע והשימוש בו.

27. כך, על מעסיקים לספק מידע, בין היתר, בדבר מטרות איסוף המידע; זהות הגורם האחראי על המאגר בו נשמר המידע ומורשי הגישה אליו; אופן אבטחת המידע; הסכנות האפשריות של איסוף ושמירת המידע; השלכות אי-מתן הסכמת העובד לאיסוף המידע והשימוש בו; זכויות העובד בדבר העיון ותיקון המידע, וכן הלאה. הסברים אלו צריכים להינתן בשפה ברורה ומובנת. יובהר כי חובת היידוע המוטלת על מעסיקים בהקשר זה היא ככלל רחבה יותר מהקבוע בסעיף 11 לחוק הגנת הפרטיות.[22]

28. יצוין כי על-פי מסמך המדיניות הלאומית ליישומים ביומטריים, פניה לקבלת מידע ביומטרי מאדם צריכה לכלול התייחסות גם לתכלית שלשמה מבוקש המידע הביומטרי; לאילו גורמים עשוי להימסר המידע הביומטרי ומהם השימושים שהם יכולים לעשות בו; כיצד נשמר המידע והשימוש בו.[23]

<u>הסכמת עובדים</u>

29. **בהיעדר הסמכה בחוק, למעסיקים <u>אסור לחייב</u> עובדים במסירת מידע ביומטרי לצרכי דיווח ובקרת נוכחות או פיקוח על שעות עבודתם, אם לא ניתנה לכך הסכמת העובד**. לפיכך, בהיעדר הסמכה בחוק הקובעת אחרת, איסוף ושימוש מעסיק במידע ביומטרי של עובד לבקרת נוכחות חייבים להיעשות בהסכמת העובד, אשר צריכה להיות **הסכמה מדעת, המתקבלת בצורה**

[21] חלופה זו רלוונטית במיוחד בנוגע למערכות לזיהוי טביעת אצבע של עובדים.
[22] לעמדת הרשות להגנת הפרטיות בנושא חובת היידוע ראו: "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (31.7.2022).
[23] סעיף 4.5 למסמך המדיניות הלאומית ליישומים ביומטריים, לעיל ה"ש 3.

מפורשת או מכללא (קרי, באופן המשתמע מהתנהגות העובד עצמו).[24] עם זאת, בנסיבות בהן השימוש במערכות ביומטריות לבקרת נוכחות נעשה באופן מידתי כפי שפורט לעיל, רשאי מעסיק לדרוש מעובד כי ייתן הסכמתו לאיסוף המידע, וסירוב העובד עלול להיות בעל השלכות מבחינת יחסי העבודה בין הצדדים.[25]

30. **היה ולא ניתנה הסכמת העובד, במפורש או מכללא, לכך שמידע אישי על אודותיו ייאסף לצרכי שימוש במערכות ביומטריות לדיווח ובקרת נוכחות, יימנע מעסיקו מלאסוף עליו מידע אישי באמצעות מערכות אלו.**

31. לגישת הרשות, ראוי ככלל שמעסיקים המבקשים להשתמש במערכות ביומטריות לדיווח ובקרת נוכחות עובדים יעמידו אפשרות זו לבחירת עובדיהם, כלומר יאפשרו להם לבחור בין שימוש במערכות בקרת נוכחות ביומטריות לבין שימוש במערכות שאינן כאלו. במצב שכזה, בחירת עובדים להשתמש במערכות ביומטריות, במקביל למתן הסכמתם המפורשת לכך, תהווה עדות טובה לכך שהסכמה זו אכן ניתנה מתוך רצון חופשי.

32. יודגש: **הסכמת עובדים לאיסוף ולשימוש במידע ביומטרי היא הכרחית אך לא מספיקה**. גם אם מתקבלת הסכמת העובד, אין בכך כדי להכשיר את איסוף המידע הביומטרי והשימוש בו בנסיבות בהן יימצא כי איסוף זה אינו עומד בתנאי המידתיות שפורטו קודם לכן.

<u>עיקרון צמידות המטרה</u>

33. על מעסיקים המשתמשים במערכות ביומטריות לדיווח ובקרה על שעות העבודה להקפיד להשתמש במידע הנאסף אך ורק למטרות אלו. שימוש במידע למטרות אחרות עלול להוות פגיעה בפרטיות והפרה של הוראות סעיפים 2(9) ו- 8(ב) לחוק הגנת הפרטיות.

34. לאור האמור רצוי שמעסיקים יימנעו מלכתחילה מלאסוף על עובדיהם מידע ביומטרי שאינו נדרש. במובן זה, **על מעסיקים לוודא כי הכמות והאיכות של הנתונים הביומטריים הנאספים (כגון טביעות אצבע ותמונות פנים) הן בהתאם לרמת הזיהוי הנדרשת, ולא מעבר לכך**.

<u>אבטחת מידע</u>

35. על-פי סעיפים 1(3)(ז) ו-2(1) לתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'תקנות אבטחת מידע'), מאגר מידע בו מוחזק מידע ביומטרי מכל סוג, לרבות טביעות אצבע, מהווה מאגר מידע שחלה עליו לכל הפחות רמת האבטחה הבינונית לפי

[24] לדוגמה, הגעת עובד למקום העבודה ושימושו במערכות ביומטריות למעקב אחר נוכחות עובדים, לאחר שנמסר לו כלל המידע על כך ששימוש זה כרוך באיסוף מידע ביומטרי וכו', עשוי להיחשב כהסכמה מכללא לאיסוף המידע ולשימוש בו למטרה זו.

[25] מסמך זה מתמקד בסוגיית הפגיעה בפרטיות ואין הוא עוסק בשאלת סבירות סירובו של עובד לבקשה מידתית ולגיטימית של מעסיק לשימוש במערכות ביומטריות לבקרת נוכחות, או במשמעותו של סירוב לבקשה שכזו במישור יחסי העבודה.

התקנות, אלא אם מדובר אך ורק במאגר תמונות הפנים של העובדים, המוחזק לשם ניהול העסק ולא לצרכי זיהוי דיגיטלי של העובד, שאז תחול על מאגר רמת אבטחה בסיסית בלבד.

36. יתר על כן, מאגר מידע המכיל מידע ביומטרי של עובדים, שיש בו מידע על אודות 100,000 איש ומעלה, או שמספר בעלי ההרשאה בו עולה על 100, ייחשב מאגר מידע שחלה עליו רמת האבטחה הגבוהה לפי תקנות אבטחת מידע, על כל המשתמע מבחינת החובות המוגברות בהן חבים מאגרים אלו לפי התקנות.

37. הרשות ממליצה לארגונים לנקוט באמצעים מתקדמים לאבטחת המידע הביומטרי השמור במאגריהם, כגון שימוש במנגנוני הצפנה וקידוד ייחודיים למידע הביומטרי, והפרדת הנתונים הביומטריים במאגר ממידע אישי אחר, כך שנתונים אלו ישמרו באופן נפרד. עוד רצוי לקבוע כי כל פעולה במאגר של ארגון המחזיק מידע ביומטרי, תתועד באופן ממוכן יחד עם פרטיו של הגורם שביצע את הפעולה.[26]

38. לגישת הרשות, ראוי שמעסיקים יגבשו נהלים לצמצום הסיכונים לפגיעה בפרטיות הכרוכים באיסוף ובשימוש במידע ביומטרי, לרבות בכל הנוגע להרשאות הגישה למאגרים וסיסמאות הכניסה אליהם. נוכח אופיו הרגיש של מאגר שמכיל מידע ביומטרי, רצוי כי מעסיקים ייקבעו הסדרי אבטחת מידע מחמירים למאגרים אלו ביחס למאגרים אחרים. כך לדוגמה רצוי כי המידע הביומטרי הנדרש לצורך זיהוי העובד, לא יישמר במאגר מידע המנוהל על ידי החברה או ספקיה, אלא יישמר על גבי התקן חכם שבחזקת העובד (כגון כרטיס עובד), באופן שיאפשר את זיהויו, תוך ביטול הסיכון לדליפה של המידע הביומטרי של כלל העובדים.

39. הרשות מבקשת להדגיש את החשיבות שבעריכת תסקיר השפעה על פרטיות, עבור כל ארגון המחליט לאסוף מידע ביומטרי על עובדיו, טרם תחילת האיסוף. תסקיר הוא תהליך אשר נועד לסייע לארגון באיתור, הערכה וניהול של סיכונים לפרטיות בפרויקטים או פעילויות עסקיות וארגוניות אחרות הכוללות עיבוד של מידע אישי, כמפורט במדריך לעריכת תסקיר שפרסמה הרשות.[27] לגישת הרשות, עריכת התסקיר בשלב מוקדם היא הדרך היעילה והאפקטיבית למזער את הסיכון לפגיעה בפרטיות, ורצוי כי ארגונים המבקשים לאסוף ולהשתמש במידע ביומטרי של עובדים (בכלל ובקשר של שימוש במערכות ביומטריות לבקרת נוכחות בפרט), יערכו תסקיר טרם תחילת איסוף המידע.[28]

---

[26] השוו לדוגמה, הוראות תקנה 14 לתקנות הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשע"א-2011.

[27] ראו מדריך עזר לביצוע תסקיר השפעה על הפרטיות שפרסמה הרשות להגנת הפרטיות (נובמבר 2022). לאזכור ביחס למידע ביומטרי – ראו סעיף 2.1 למדריך.

[28] סעיף 5.2.4 למסמך מדיניות לאומית ליישומים ביומטריים', לעיל ה"ש 3, העוסק בתכנון לפרטיות (Privacy by design), כי "מערכת ביומטרית צריכה להיות מתוכננת תוך שילוב ותכנון מראש של היבטי הגנת הפרטיות. האם מערכת שאינה כוללת מאגר ביומטרי נותנת מענה לצרכים ולמטרות היישום, בהתחשב בכל השיקולים הרלוונטיים".

40. הרשות מבקשת להדגיש בהקשר זה גם את התועלת הרבה שבמינוי ממונה הגנת פרטיות בארגון, שבין יתר תפקידיו, הוא גם הגורם המתאים והיעיל לתכנון ולבחינת הצעדים הננקטים בארגון למזעור הסיכון לפגיעה בפרטיות עובדים. יצוין כי חוק הגנת הפרטיות קובע חובה למנות ממונה על הגנת פרטיות בגופים הבאים:

- גוף ציבורי כהגדרתו בסעיף 23 לחוק או מחזיק במאגר מידע כאמור, למעט גוף ביטחוני כהגדרתו בסעיף 23 כ;
- ארגונים שמטרתם העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, ויש במאגר מידע אישי על יותר מ-10,000 נושאי מידע;
- בעל שליטה במאגר מידע או מחזיק במאגר מידע שעיסוקיו העיקריים כוללים פעולות עיבוד מידע או כרוכים בפעולות כאמור, אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר;
- בעל שליטה במאגר מידע או מחזיק במאגר מידע שעיסוקו העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר, ובכלל זה תאגידים בנקאיים, חברות ביטוח, בתי חולים, וקופות חולים.

<u>צמצום ומחיקת מידע</u>

41. תקנה 2(ג) לתקנות אבטחת המידע מחייבת מעסיקים, בכובעם כבעלי שליטה במאגרי מידע, לבחון, אחת לשנה, אם המידע שהם שומרים במאגר אינו חורג מן הנדרש ביחס למטרותיו. לגישת הרשות, בנסיבות בהן מגיע בעל שליטה למסקנה כי מידע מסוים השמור במאגר הוא עודף, ואינו פועל לצמצום מידע זה, התנהלות זו עשויה בנסיבות מסוימות להוות הפרה של הוראות הדין.

42. לאור האמור, נוכח רגישותו של המידע הביומטרי, ולאור חובות תום הלב החלות על מעסיקים ביחסי עבודה, **רצוי כי מעסיקים יבחנו את נחיצות שמירתו של מידע ביומטרי המוחזק על-ידם, ויצמצמו מידע זה (לרבות באמצעות מחיקתו) כאשר אין עוד צורך בהמשך שמירתו**. כך למשל, מידע שאינו נחוץ עוד לארגון עשוי להיות מידע ביומטרי על עובדים שפרשו, או על עובדים שכבר אינם עושים שימוש במערכת הביומטרית.

43. ככלל, שמירת מידע אישי לאורך זמן מגבירה את הסיכון לפגיעה בפרטיות. לפיכך, ככל שמידע ביומטרי הנאסף לשם בקרת נוכחות נשמר על ידי המעסיק לתקופה ארוכה יותר – כך גובר הסיכון כי מידע זה ידלוף או ייחשף, ויפגע קשות בפרטיות העובד.

44. לאור האמור, עמדת הרשות היא שעל ארגונים לשמור מידע אישי על אודות עובדיהם אך ורק לתקופה התואמת את מטרת איסוף המידע או את מטרת המאגר בו שמור המידע. עמדה זו נכונה ביתר שאת ביחס למידע בעל רגישות מיוחדת כדוגמת מידע ביומטרי.

45. לפיכך, **עם סיום העסקתו של עובד יש להניח כי אין עוד הצדקה לשמירת מידע ביומטרי הנוגע אליו, ככל שהמידע נאסף לצרכי בקרת נוכחות, ועל המעסיק לפעול לצמצום מידע זה, לרבות באמצעות מחיקתו**. למען הסר ספק, מחיקת המידע צריכה להיעשות בכל סביבות העבודה הקיימות של הארגון, לרבות במערכות גיבוי המידע.[29]

<u>רישום מאגר ביומטרי</u>

46. על ארגונים החייבים ברישום מאגרים בהתאם להוראות סעיף 8א(א)(1) לחוק הגנת הפרטיות, ואוספים מידע ביומטרי לשם שימוש במערכות לבקרת נוכחות עובדים, להגיש בקשה לרישום המאגר, בהתאם להוראות פרק ב' לחוק הגנת הפרטיות. יובהר כי לפי הנחיות הרשות, בעת הגשת בקשה לרישום מאגר מידע ביומטרי, על המבקש לצרף התייחסות בכתב לשאלות הבאות:[30]

- אילו חלופות לאיסוף מידע ביומטרי נשקלו?
- איזו מערכת מופעלת לבקרת הכניסה?
- איזה מידע ביומטרי נאסף?
- האם המידע נאסף לכרטיס או למאגר, ולמה בחרתם בשיטה זו?
- במידה ומדובר במאגר, מי מחזיק במאגר ואיפה?
- האם ניתנה לעובדים חלופה מראש שאינה כוללת ביומטריה?
- האם העובדים מודעים לכך, שכאשר יש צו, המידע הביומטרי עשוי להגיע לגורמים אחרים מלבד בעל המאגר?

47. הרשות מדגישה כי על-פי הוראות סעיף 10(א)(1) לחוק הגנת הפרטיות, היא רשאית לסרב לרשום מאגר אם קיים יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע האישי הכלול בו נוצר, נתקבל, נצבר או נאסף בניגוד לחוק הגנת הפרטיות או בניגוד להוראות כל דין.

48. עוד יצוין כי על-פי הוראות סעיף 8א(ב)(1) לחוק, בעלי שליטה במאגרים שאינם חייבים ברישום אך שיש בהם מידע בעל רגישות מיוחדת (**ולענייננו מידע ביומטרי**) על אודות למעלה מ-100,000 איש, חייבים למסור הודעה לרשות על זהות בעל השליטה במאגר, מענו ודרכי ההתקשרות עימו, על זהות הממונה על הגנת הפרטיות (אם נדרש מינויו לפי סעיף 17ב1 לחוק), ועל דרכי ההתקשרות עימו, ולצרף העתק ממסמך הגדרות המאגר הנדרש לפי תקנה 2 לתקנות אבטחת מידע.

[29] יובהר, כי פסקה זו נוגעת אך ורק לשמירת מידע ביומטרי על עובדים שנאסף לצרכי בקרת נוכחות. אין היא מתייחסת לאפשרות שמירת מידע שאינו ביומטרי על עובדים, אשר במקרים מסוימים עשוי להיות נדרש למעסיק גם לאחר סיום ההעסקה.

סיכום

49. מידע ביומטרי הוא מידע ייחודי. ככלל, למעסיקים עומדת הפררוגטיבה לאסוף ולהשתמש במידע ביומטרי לדיווח ובקרת נוכחות עובדים במקום העבודה. עם זאת, איסוף המידע הביומטרי והשימוש בו חייבים להיעשות באופן סביר ומידתי, תוך יידוע העובדים וקבלת הסכמתם המפורשת לכך, תוך יישום חובות אבטחת המידע הקבועות בדין, ותוך הקפדה על עיקרון צמידות המטרה.

50. לגישת הרשות, על ארגונים לשמור מידע על אודות עובדיהם אך ורק לתקופה התואמת את מטרת איסוף המידע או את מטרת המאגר בו שמור המידע. לאור רגישותו המובנית של מידע ביומטרי, על מעסיקים להקפיד ביתר שאת על יישום עיקרון זה. לאור כך, ולנוכח רגישותו של המידע הביומטרי, על מעסיקים לבחון את נחיצות שמירתו של מידע ביומטרי המוחזק על-ידם, ולצמצם מידע זה (לרבות באמצעות מחיקתו) כאשר לא קיים צורך בהמשך שמירתו.