

הרשות לניהול המאגר הביומטרי

דין וחשבון חצי שנתי לתקופה V

בהתאם לצו הכללת אמצעי זיהוי ביומטריים
ונתוני זיהוי ביומטריים במסמכי זיהוי
ובמאגר מידע, התשע"א-2011

לתקופה שבין 01/07/2015 עד 31/12/2015

ינואר 2016

תוכן עניינים

1. רקע 4
2. תמצית מנהלים 6
3. פעילות הרשות לניהול המאגר הביומטרי 8
 - 3.1 נתונים וכמויות במאגר הביומטרי 9
4. משימות לתקופת המבחן 12
5. הממשק בין רשות האוכלוסין לרשות לניהול המאגר הביומטרי 13
 - 5.1 התוצרים המועברים 13
 - 5.2 תוצאות זיהוי 14
 - 5.3 משך הזמן הדרוש לקבלת תוצאת הזיהוי והעברתה לידי עובד רשות האוכלוסין 15
 - 5.4 פעילות השוואת הביומטריות 16
6. מדדי ביומטריה (דיוק המערכת הביומטרית) 19
 - 6.1 מערכת השוואה הביומטרית 19
 - 6.2 הדרישה המוגדרת בצו בכל הנוגע לביצועי המערכת 19
 - 6.3 מדדי הדיוק של המערכת הביומטרית במאגר (בהתאם לפרוטוקול תקופת המבחן) 20
7. אבטחת מידע ופרטיות ברשות לניהול המאגר הביומטרי 26
 - 7.1 ניהול סיכונים 27
 - 7.2 אבטחת מידע – היבטי המבנה הארגוני 27
 - 7.3 אבטחה פיסית 28
 - 7.4 אבטחת מידע 28
 - 7.5 סקרי סיכונים ומבדקי חדירות 29
8. בדיקת אתר גיבוי 30
9. הסתייעות בגורמי חוץ 30
10. שמירת המידע 31
11. העברת המידע מהמאגר לגורמי חוץ 31
12. נגישות למידע במאגר 31
13. עלויות תקציביות 32
14. סיכום 33

לכבוד:
ראש הממשלה
שר הפנים
שר האוצר
שרת המשפטים
השר לבטחון פנים
ועדת הכנסת המשותפת
ועדת הכנסת המשותפת ליישומים ביומטריים
הממונה על היישומים הביומטריים
הוועדה המייעצת

הנדון: דו"ח תקופתי חמישי לתקופת המבחן 01/07/2015 - 31/12/2015

בהתאם לסעיף 41(1) לחוק הכללת אמצעי זיהוי ביומטריים ונתוני זהות ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע – 2009 (להלן החוק), יוחל החוק בהדרגה, באופן שיקבע בצו בתקופת מבחן בת שנתיים שבמהלכה יחולו הוראות החוק על תושבים שיתנו את הסכמתם לכך בכתב, במטרה לבחון את אופן היישום של הוראות החוק, את נחיצות קיומו של מאגר ביומטרי ומטרותיו, את המידע שיש לשמור במאגר ואת אופן השימוש בו.

בהתאם לכך, נקבע צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשע"א – 2011, (להלן- הצו) אשר מסדיר את תקופת המבחן.


לאחר תקופת היערכות משמעותית החלה בפועל תקופת המבחן ביום 30/06/2013 ובתהליך הדרגתי שנמשך כשלושה חודשים, החלו לשכות רשות האוכלוסין וההגירה לקבל בקשות להנפקת מסמכי זיהוי לפי הוראות החוק, בבד בבד עם תפעול המאגר הביומטרי במקביל על יד הרשות לניהול המאגר הביומטרי.

ביום 29/06/2015 בתום תקופת מבחן של שנתיים, הוארכה תקופת המבחן לתקופה של תשעה חודשים נוספים, עד ליום 31/03/2016.

בהתאם לסעיף 11(ב) לצו, מוגש בזאת דין וחשבון חמישי המתייחס לחצי השנה החמישית של תקופת המבחן.

31/01/2016

תאריך



גון קרמי

ראש הרשות לניהול המאגר הביומטרי

1. רקע

דין וחשבון חמישי זה מוגש לראש הממשלה, שר הפנים, שר האוצר, שרת המשפטים, השר לביטחון הפנים, ועדת הכנסת המשותפת, ועדת הכנסת המשותפת ליישומים ביומטריים, הממונה על היישומים הביומטריים במשרד ראש הממשלה והוועדה המייעצת במסגרת מילוי החובות הנדרשים בחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע - 2009¹ (להלן: החוק).

דיווח זה הינו דין וחשבון חמישי לתקופת המבחן, שבו מפורטות ומתוארות פעולות הערכה ומדידה אשר מבוצעות ברשות לניהול המאגר הביומטרי במסגרת פרויקט התיעוד הלאומי הביומטרי החדש. דיווח זה מספק תמונת מצב נכונה לתאריך 31 בדצמבר 2015.

ב- 30 ביוני 2013 החלה הנפקה של תיעוד לאומי חדש לתושבי מדינת ישראל. תיעוד זה כולל את תעודת הזהות הביומטרית ואת הדרכון הביומטרי. מסמכי זיהוי אלו נועדו להקשות על זיופם ולמעשה לשלול מעבריינים את היכולת הקלה לייצר בעצמם מסמכי זיהוי מזויפים. מעבר למניעת זיוף מסמכי הזיהוי, הוקם בסיס נתונים מרכזי הכולל מידע ביומטרי (להלן: מאגר ביומטרי), שמטרתו להקשות על זיופי זהות ובפרט להקשות על יכולת קבלת זהויות מרובות. תהליך הנפקה זה הינו חלק מיישום הוראות החוק.

סעיף 41 לחוק קבע תחולה הדרגתית ותקופת מבחן, שמטרתה "לבחון את אופן יישום החוק, את נחיצות קיומו של המאגר הביומטרי ומטרותיו, את המידע שיש לשמור במאגר ואת אופן השימוש בו". נושאים אלו מפורטים בתקנות הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע (תקופת מבחן) התשע"א - 2011 (להלן "התקנות"²), בצו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע התשע"א - 2011 (להלן "הצו"³), ובפרוטוקול תקופת המבחן⁴. בסיום תקופת המבחן תתקבל החלטה לגבי עתידו של המאגר הביומטרי המרכזי.

מתחילת תקופת המבחן ליישום החוק נבחנו נושאים אלו באופן שוטף בלשכות רשות האוכלוסין, ברשות לניהול המאגר הביומטרי, במרכזי הנפקה של תעודות הזהות והדרכונים ובמערך ביקורת הגבולות במעברי הגבול הבינלאומיים של מדינת ישראל.

¹ ראו נוסח החוק ב- http://smartid.gov.il/SiteCollectionDocuments/bio_law.pdf

² ראו נוסח התקנות ב- http://smartid.gov.il/SiteCollectionDocuments/bio_Takanot.pdf

³ ראו נוסח הצו ב- http://smartid.gov.il/SiteCollectionDocuments/bio_Tsav.pdf

⁴ ראו נוסח פרוטוקול תקופת המבחן ב- <http://www.piba.gov.il/Subject/BiometricPassports/Documents-%20פרוטוקול%20תקופת%20המבחן.pdf>

לשכות רשות האוכלוסין מבצעות תהליכים של וידוא ואימות זהות, נטילת אמצעי זיהוי ביומטריים (להלן: "הרכשה"), בדיקת איכות אמצעי הזיהוי, השוואת אמצעי זיהוי ביומטריים (אדם מול מסמך זיהוי) והעברת אמצעי זיהוי ביומטריים לרשות לניהול המאגר הביומטרי ולמערכי ההנפקה של מסמכי הזיהוי.

הרשות לניהול המאגר הביומטרי מבצעת תהליכים של השוואת אמצעי הזיהוי המתקבלים מלשכות רשות האוכלוסין לנתונים השמורים במאגר הביומטרי כדי לאתר כפילויות או ניסיונות התחזות. כמו כן מעבירה הרשות לניהול המאגר הביומטרי לרשות האוכלוסין אישור להנפיק מסמכי זיהוי (תעודות זהות חכמות ודרכונים ביומטריים) כאשר אמצעי הזיהוי הביומטריים נמצאים תקינים.

מערכי ההנפקה מייצרים כרטיסי תעודות זהות ביומטריות ודרכונים ביומטריים שמשולב בהם שבב המכיל נתונים ביומטריים, לאחר קבלת האישור להנפקה מהרשות לניהול המאגר הביומטרי. תעודות זהות נמסרות ישירות לתושב בלשכות רשות האוכלוסין בעוד שדרכונים נשלחים בדואר רשום. המעבר מהנפקה מבזרת של תיעוד לאומי בלשכות רשות האוכלוסין להנפקה מרכזית הינו נדבך חשוב מאד ומרכזי מאד באבטחת התיעוד הלאומי החדש, לפיכך הנפקת מסמכי הזיהוי החדשים נעשית במתקנים בהתאם לתקנים המודרניים ביותר שהוגרו במיוחד לצורך זה.

מערך ביקורת הגבולות מבצע נכון לעכשיו באופן ניסיוני השוואות בין אמצעי זיהוי ביומטריים (תמונת פנים וטביעות אצבע) הנלקחים מהנוסעים לבין המידע הנקרא מהדרכון כדי לאפשר למחזיקי הדרכון הביומטרי מעבר במסלול מקוצר בעת ביקורת הגבולות. מעבר זה מתבצע באמצעות עמדות ביקורת גבולות בשירות עצמי כחלק מהליך הזיהוי הנדרש במעבר גבול.

משטרת ישראל בוחנת את ערוץ הקשר אל הרשות לניהול המאגר הביומטרי באמצעות ביצוע הדמיה של בקשות לקבלת נתוני זיהוי מהמאגר. בכל מקרה לא יתקיים קישור בין המשטרה למערכות הרשות, אלא שאילתות ללא חיבור ישיר וללא מענה בזמן אמת.

כל התהליכים המתוארים לעיל מלווים באיסוף של נתונים רבים, כמתחייב בצו. תקופת המבחן כמצוין בחוק מלווה בתוכנית מבחן הנגזרת מהצו ומפרוטוקול תקופת המבחן. על מנת ליישם את תוכנית המבחן הוקם על ידי רשות האוכלוסין והרשות לניהול המאגר הביומטרי מערך מדידה והערכה הכולל איסוף נתונים מהמערכות הממוחשבות בכל חלקי המערכת הביומטרית, ביצוע סקרי שביעות רצון, מדידת ביצועים למערכת הביומטרית, בחינת חלופות למאגר המידע הביומטרי, ביצוע אירועים יזומים, בדיקות אבטחת מידע ובדיקת אתר גיבוי (ע"י הרשות לניהול המאגר הביומטרי בלבד).

נתונים רבים מועברים באופן שוטף גם ללשכה המרכזית לסטטיסטיקה לצורך חישוב מדדים וניתוחים של הנתונים.

2. תמצית מנהלים

דיווח זה הינו דין וחשבון חמישי לתקופת המבחן ומספק תמונת מצב נכונה לתאריך 31 בדצמבר 2015. בדו"ח מפורטות פעולות הערכה ומדידה אשר מבוצעות ברשות לניהול המאגר הביומטרי (להלן: הרשות). הדו"ח כולל מדידת ביצועים למערכת הביומטרית בצורה שוטפת והסברים לעמידה בדרישות החקיקה, תאור בדיקות אבטחת מידע, סקרי סיכונים והגנת הפרטיות, וכן בדיקת מעבר לעבודה באתר גיבוי בתרחיש המדמה התרחשות אסון.

דו"ח זה אינו מפרט את כל מבדקי הנחיצות, מבחני החלופות ומבחנים דומים אשר נערכו במסגרת תקופת המבחן ופורסמו במסמכים קודמים אשר הגישה הרשות. דו"ח זה מפנה את הקורא לדו"ח המסכם המעודכן אשר הוגש על ידי הרשות בדצמבר 2015 לשר הפנים ולראש הממשלה. הדו"ח המסכם מפרט בין היתר את בחינת החלופות למאגר הביומטרי, את תוצאות בחינתן ואת סיכום והמלצת הרשות לניהול המאגר הביומטרי. יחד עם הדו"ח אשר סיכם את תקופת המבחן הראשונה בת השנתיים, הוגש לשר הפנים הדו"ח המסכם של הוועדה המייעצת אשר פיקחה על התנהלות התקופה.

בנוסף מפנה דו"ח זה לעיקרי הממצאים והמשמעויות של עבודות מחקר אשר נערכו לבחינת נחיצות המאגר ומטרותיו, בין השאר בנושא תופעת ההרכשות הכפולות וגניבת הזהויות, שימוש במאגרי ביומטריים במדינות העולם, בחינת חלופות מפורטת וכן שימוש בתעוד חכם ובמאגר ביומטרי ככלי למניעת פשיעה וטרור ועוד.

הנתונים ותוצאות הבדיקות אשר מפורטים בדו"חות הרשות אשר צוינו לעיל מבוססים על מערך המדידה וההערכה ברשות אשר כולל איסוף נתונים מהמערכות הממוחשבות וניתוחם על ידי מומחים בתחום הביומטריה וכן על ידי מומחי חברת מחצ"ב רפא"ל. בנוסף, מועברים הנתונים ללשכה המרכזית לסטטיסטיקה, (למ"ס).

בתקופת דיווח חמישית זו, המשיכה הרשות לשפר ולשדרג את היכולות הטכנולוגיות במטרה להבטיח את ההגנה הטובה ביותר על זהותם של תושבי מדינת ישראל. הרשות נמצאת בעיצומה של הטמעת מערכת השוואת ביומטרית חדשה, שלאחר הטמעתה תפעל במקביל למערכת הקיימת. זאת במטרה להבטיח את רמות הדיוק הגבוהות ביותר של השוואות הביומטריות על ידי שימוש במגוון מנועים ביומטריים לביצוע תהליכי השוואות. תצורת פעולה זו מקובלת בפרויקטים דומים בעולם.

הרשות מבצעת תהליכים של השוואת אמצעי הזיהוי המתקבלים מהלשכות (תמונת פנים ושתי טביעות אצבע בלבד), לנתונים השמורים במאגר הביומטרי לצורך מניעת כפילויות או ניסיונות התחזות. כמו כן מעבירה הרשות לרשות האוכלוסין אישור להנפיק מסמכי זיהוי (תעודות זהות חכמות ודרכונים אלקטרוניים) בהתאם

לתוצאות ההשוואה. תופעת ההרכשות הכפולות, קרי גניבת זהות והשגת מסמך מזהה תוך התחזות הנה תופעה נרחבת. משמעויותיה של התופעה הינן חמורות ביותר, בפרט בעידן אליו המדינה נכנסת כעת, עידן בו התעוד הביומטרי החכם ישמש למגוון יישומים ופעילויות של תושבים במסגרת צריכת שירותי ממשלה ושירותים נוספים. **המאגר הביומטרי אשר הוקם במסגרת הפרויקט מאפשר לוודא כי לכל תושב תהא תעודה מזהה אחת בזהותו המקורית בלבד** ומונע מצב בו יונפק תעוד ביומטרי חדש תוך גניבת זהות והשגת מספר תעודות חדשות בזהויות בדויות על ידי עבריינים.

כפי שמוצג בדו"ח זה, בתום כשנתיים וחצי של פעילות במסגרת הפרויקט, ניתן לקבוע כי המדינה ממלאת את האחריות המוטלת עליה **ומאפשרת רמה גבוהה של ביטחון אישי והגנה על פרטיות התושבים על ידי הנפקת תעוד ביומטרי חכם המבוסס על פעילות המאגר הביומטרי. שילוב השניים מאפשר עמידה ביעד כפי שנקבע בחוק: "תעוד אחד לאדם אחד".**

לאור הנתונים אשר מוצגים בדו"ח שלהלן **ולאור הצטרפותם של 856,024 תושבים מתחילת הפרויקט**, (נכון לסוף דצמבר 2015), אשר קיבלו תעודות זהות ודרכונים ביומטריים חכמים, ניתן לומר שהתהליך מתבצע בצורה משביעת רצון ואף מעבר לכך. תהליכי ההרכשה וההנפקה מבוצעים בצורה טובה, תהליכי ההשוואה הביומטרית במערכות הרשות לניהול המאגר הביומטרי מאתרים ומונעים הרכשות כפולות והתקופה מתאפיינת במינימום תקלות. רמת האבטחה וההגנה על הפרטיות הנן גבוהות ביותר כפי שנדרש בחוק וכפי שמוגדר ומפוקח על ידי הגורמים הרלוונטיים.

הערה: לדו"ח זה מצורף כנספח דו"ח הלשכה המרכזית לסטטיסטיקה המתייחס לתקופת הדיווח הנוכחית.

3. פעילות הרשות לניהול המאגר הביומטרי

בהתאם לאמור בחוק, סעיף 10א': "השר יקים, במשרד הפנים, רשות לניהול המאגר הביומטרי שתהא אחראית לניהול המאגר הביומטרי ובכלל זה להפקת נתוני זיהוי ביומטריים מאמצעי זיהוי ביומטריים שהועברו אליה, לעיבודם, להעברת מידע מהמאגר הביומטרי וכן לאבטחת המאגר, לאחזקתו ולטיפול השוטף בו, הכל בהתאם להוראות לפי חוק זה".

בחודש אוגוסט 2011 הוקמה על פי החוק הרשות לניהול המאגר הביומטרי. ייעודה העיקרי של הרשות לניהול המאגר הביומטרי הנו הקמה, אבטחה וניהול של בסיס הנתונים הביומטריים (המאגר), אשר מהווים נתונים מזדהים ומשולבים בתעודות הזהות הביומטריות ובמסמכי הנסיעה.

בנוסף, נקבעה בחוק תקופת מבחן בת שנתיים אשר החלה בתאריך 30 ביוני 2013. בסיום התקופה ובהתאם למדדים ולתוצאות שידווחו יוחלט בין החלופות האפשריות הבאות:

1. מעבר לפעילות מלאה והחלת החוק כמנדטורי על כלל התושבים.
2. החלה הדרגתית של החוק.
3. המשך תקופת המבחן ב- עד שנתיים נוספות.

בתאריך 29/6/2015 אישרה הכנסת את קביעתו של שר הפנים בצו להארכתה של תקופת המבחן בתשעה חודשים נוספים, עד לתאריך ה- 31/3/2016.

בסעיף 10 ה' לחוק מוגדר שבמידה ולא תתקבל החלטה לאחר ארבע שנים יימחק המאגר הביומטרי.

הייעוד העיקרי של בסיס הנתונים הביומטריים המרכזי הנו **מניעה וסיכול של ניסיונות קבלת תיעוד במרמה**. המערכות המותקנות ברשות מאפשרות השוואת פרטים ביומטריים של מבקש התיעוד מול פרטים ביומטריים המאוחסנים בבסיס הנתונים ועל ידי כך מאותרים ונמנעים ניסיונות הרכשה כפולה והתחזות. פעילות זו מאפשרת מתן תיקוף לאמיתות התיעוד ובנוסף להיותו תיעוד מאובטח מאוד הוא גם תיעוד אמין.

כפי שבוצע טרם תחילת תקופת המבחן ובמהלך כל תקופת הדיווח, ממשיכה הרשות לניהול המאגר הביומטרי ביישום המוטל עליה על פי חוק ובכלל זה אבטחתו הלוגית והפיסית של מאגר הנתונים הביומטריים והגנת הפרטיות, ניהולו השוטף של המאגר והעברת תוצאות זיהוי לרשות האוכלוסין לצורך ניפוק מסמכי זיהוי. בנוסף לכך, משקיעה הרשות משאבים בהכשרת עובדים והתמקצעותם וכן בשיפור יכולות טכנולוגיות. כדוגמא לכך נערכת הרשות להטמעתה של מערכת השוואה ביומטרית חדישה. כמו כן, הרשות נערכה טכנולוגית ותפעולית לתהליך החלפתם של סורקי טביעות האצבע אשר בוצע בלשכות רשות האוכלוסין.

3.1 נתונים וכמויות במאגר הביومتر

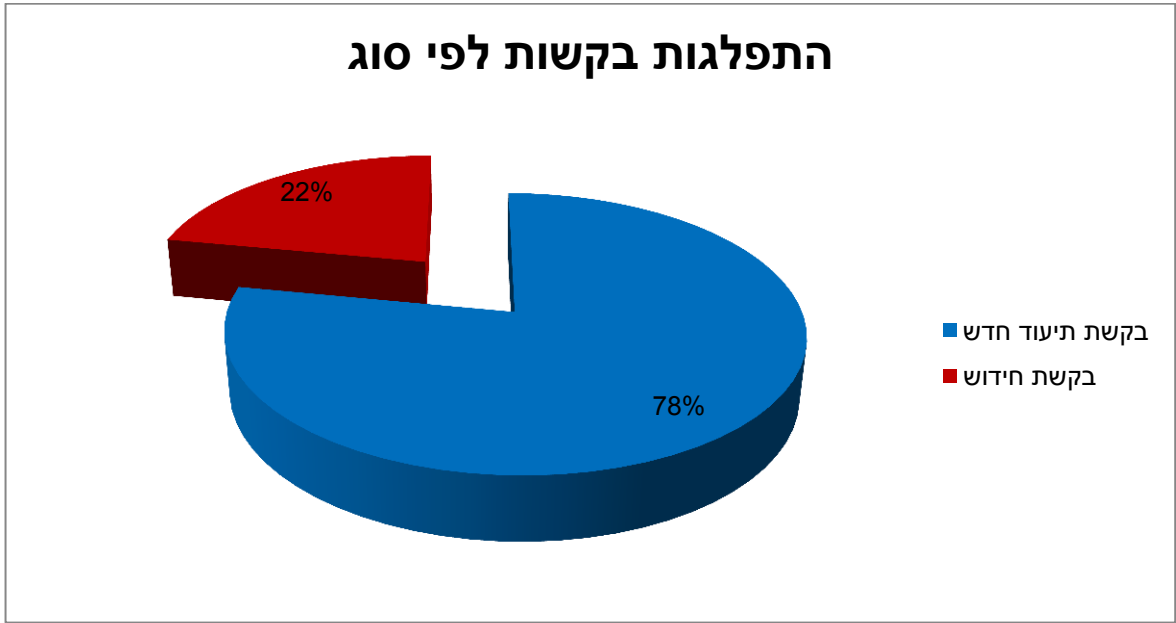
להלן כמות המצטרפים למאגר הביومتر בתקופה אליה מתייחס דין וחשבון זה.

3.1.1 המאגר הביومتر

מספר התושבים אשר בחרו במסמכי הזיהוי הביומטריים ואשר פרטיהם מצויים בבסיס הנתונים הביומטריים המרכזי נכון ליום 31 בדצמבר 2015 הוא **856,024 תושבים**. חלקם בחרו בדרכון הביومتر החדש, חלקם בתעודת הזהות הביומטרית וחלקם ביקשו לקבל את שני סוגי המסמכים גם יחד. (מספר זה כולל את מספר התושבים שבחרו תיעוד חכם ביומטרי, כייחודיים, כלומר, כל מבקש תיעוד נספר פעם אחת ויחידה – Unique).

בסוף דצמבר המאגר כולל את פרטיהם הביומטריים של 856,024 תושבים

בתקופת הדיווח החמישית הוגשו ⁵156,875 בקשות מתוכם הצטרפו 123,042 תושבים חדשים ונכללו במאגר. ניתן לראות כי ככל שמספר הבקשות במאגר גדל, כך גדל מספר בקשות החידוש.



⁵ פער של 18 רשומות נובע מהשלמת רשומות FTE מתקופות קודמות ואשר בוצע בתקופת הדיווח ה-5.

סוג הבקשה	תקופת הדיווח הנוכחית	כל תקופת המבחן
בקשת תיעוד חדש	78%	88%
בקשת חידוש ⁶	22%	12%

חלוקה לסוגי הרכשות בהתאם לנתונים המופיעים במערכות הרשות לניהול המאגר הביومتر (כמות הבקשות בתקופת הדיווח החמישית) :

הנתון	כמות הבקשות
הרכשות מלאות (תמונת פנים ושתי אצבעות מורות)	131,255
הרכשות חלקיות (תמונת פנים ואצבעות אחרות, אגודלים או אמות)	5,049
הרכשות חסרות (ללא טביעות אצבע כלל) של ילדים	17,694
הרכשות חסרות (ללא טביעות אצבע כלל) של מבוגרים	28
הרכשות מלאות עם FTE (1 או יותר)	921
הרכשה חלקית עם FTE	1928
סה"כ הרכשות	156,875

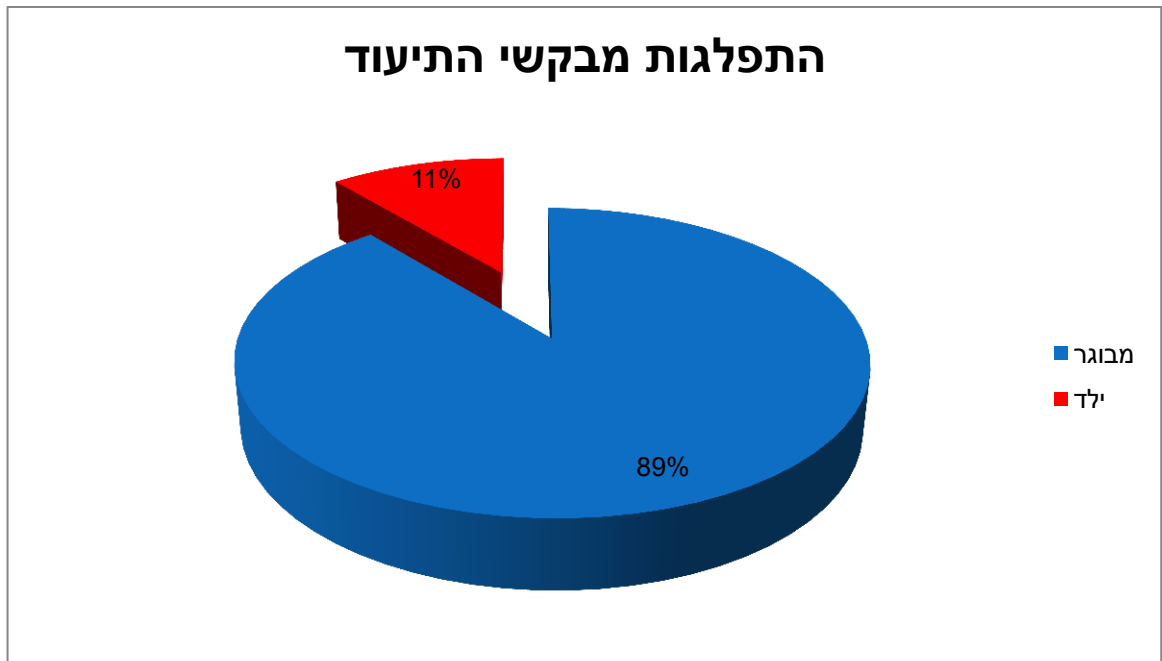
הסבר:

הרכשה משמעותה, בקשת תיעוד ביومتر של תושב ישראלי הכוללת טביעות אצבע וצילום פנים. **חידוש** משמעו הרכשה נוספת של מבקש התיעוד, אם בשל בקשת תיעוד נוסף, כדוגמת בקשת הנפקת דרכון לאחר שבביקור קודם התבקשה רק ת"ז, או אם בשל דיווח אובדן/גניבה של תיעוד ביومتر חדש.

⁶ **חידוש** משמעו הרכשה נוספת של מבקש התיעוד, אם בשל בקשת תיעוד נוסף, כדוגמת בקשת הנפקת דרכון לאחר שבביקור קודם התבקשה רק ת"ז, או אם בשל דיווח אובדן/גניבה של תיעוד ביومتر חדש.

התפלגות מבקשי התיעוד בחלוקה למבוגרים וילדים

מבקש התיעוד	תקופת הדיווח הנוכחית	כלל תקופת המבחן
מבוגר	89%	92%
ילד	11%	8%



4. משימות לתקופת המבחן

בהתאם לדרישות החוק, הצו ופרוטוקול תקופת המבחן, התקיימו מבדקים רבים בנוסף למספר עבודות מחקר מקיפות במהלך תקופת המבחן בת השנתיים וחצי. תוצאות המבדקים והבחינות מפורטים במסמכים אשר הועברו לעיון הגורמים הרלוונטיים אשר שותפים לפרויקט. בנוסף, ניתן לעיין במסמכים הבלתי מסווגים באתר האינטרנט⁷ של הרשות לניהול המאגר הביومتر. כמו כן, הועברו מסמכים אלה לוועדת הכנסת המשותפת ליישומים ביומטריים לשם פרסומם באתר הוועדה. להלן הנושאים אשר נבחנו במסגרת תקופת המבחן:

1. בחינת היקף תופעת ההרכשות הכפולות וגניבת הזהות במדינת ישראל ודוגמאות מהעולם.
2. עבודת מחקר המציגה מאגרים ביומטריים ומגמות עולמיות בתחום הביומטריה ויישומיה.
3. בחינת חלופות שונות המאפשרות מתן מענה לדרישות החוק, ובכללן חלופות הכוללות כמות שונה של נתונים ביומטריים, חלופה של אימות באמצעות תשאול (ללא שימוש בנתונים ביומטריים), ואימות באמצעות שימוש בנתונים ביומטריים חלקיים. כמו כן נבחנה חלופה של מימוש מאגר ביומטרי בשיטת ההקבצים.
4. עבודת מחקר הבוחנת את יכולות התייעוד החכם והמאגר הביומטרי לשמש ככלי למניעת פשיעה וטרור, שבוצעה על ידי המכון למדיניות נגד טרור במרכז הבינתחומי.
5. אומדן היקף הנזקים הנגרמים למדינת ישראל כתוצאה מהתחזות וגניבת זהות.
6. מבדקי אבטחה, סקרי סיכונים ובחינת תצורת ההגנה על הפרטיות ברשות.
7. מבדקי ביצועים למערכות הרשות וליכולות המאגר לתת מענה לדרישות החוק.
8. אופן יישום הוראות החוק

⁷ אתר הרשות לניהול המאגר הביומטרי : www.biodb.gov.il

5. הממשק בין רשות האוכלוסין לרשות לניהול המאגר הביומטרי

5.1 התוצרים המועברים

תושב מדינת ישראל המגיע ללשכת רשות האוכלוסין לצורך הוצאת תיעוד ביומטרי מאשר את צילום תמונת הפנים שלו וסריקת שתי טביעות האצבע. תהליך הצילום והסריקה של הנתונים הביומטריים נקרא – **הרכשה**.

בסיום תהליך ההרכשה מועברים מרשות האוכלוסין בצורה מאובטחת ומוצפנת (ללא חיבור ישיר, חוטי או אלחוטי או אחר), לרשות הביומטרית, הנתונים הביומטריים בתוספת מספר נתונים תפעוליים (לא דמוגרפיים) כדוגמת, מספר מזהה מוצפן, או סימון אם התמונה סרוקה. כלל נתונים אלו של תושב בודד נקראים – **בקשה**.

- לתושב אחד יכולות להיות מספר בקשות – אם בשל הגשת בקשת ת"ז ודרכון במועדים שונים ואם בשל אובדן או גניבה. לאחר שליחת הבקשה, נמחקים כלל הנתונים הביומטריים של התושב מהמחשב בלשכה. תושב המבקש תיעוד נוסף (לדוגמא ביקש דרכון ואח"כ מבקש ת.ז.) מתבקש לבצע הרכשה נוספת. היות ואין נתונים ביומטריים בלשכת רשות האוכלוסין מופקת בקשה נוספת. כך שלתושב יכולות להיות מספר בקשות.

הנתונים הביומטריים, (ללא נתונים דמוגרפיים כלשהם) מתוך הבקשות לקבלת התיעוד, אשר מתקבלים מן התושבים בתהליך ההרכשה בלשכות רשות האוכלוסין, מועברים בצורה מאובטחת ומוצפנת למערכות הרשות לניהול המאגר הביומטרי. תהליך ההעברה כולל העברה ידנית מאובטחת בשל ה**נתק המוחלט הקיים בין המערכות ("Air Gap")**.

מערכות הרשות מנותקות מהעולם החיצון ואינן מחוברות בשום אופן, חוטי או אלחוטי למערכות או לרשתות אחרות

5.2 תוצאות זיהוי

ברשות לניהול המאגר הביומטרי מבוצע תהליך השוואת נתונים ביומטריים, כאשר תוצאות ההשוואה מועברות לרשות האוכלוסין ללא הנתונים הביומטריים. תוצאות ההשוואה כוללות את מספר הבקשה ומידע אם הבקשה נדחתה, אושרה או שנדרש בירור.

ברשות לניהול המאגר הביומטרי אין נתונים דמוגרפיים כלשהם של תושבי המדינה אלא אך ורק הנתונים הביומטריים ולכן יכולים להתרחש מקרים בהם הנתונים הביומטריים אינם מספיקים לקבלת החלטה על אישור או דחיית בקשה, לדוגמא: דמיון בין שתי תמונות פנים של אנשים בעלי זהויות שונות. הדמיון יכול לנבוע מהתחזות, או בגלל שמדובר בתאומים. היות וברשות לניהול המאגר הביומטרי אין נתונים דמוגרפיים, אין לרשות לניהול המאגר הביומטרי את היכולת לקבוע כי מדובר בתאומים והמקרה מועבר **לבירור** רשות האוכלוסין ללא הנתונים הביומטריים תוך ציון כי קיים דמיון בין שתי תמונות פנים של אנשים שונים. רשות האוכלוסין לאחר בירור המקרה יכולה להחזיר תשובה לרשות לניהול המאגר הביומטרי אם לאשר או לדחות את הבקשה.

מספר הפעמים שבהן העבירה הרשות לניהול המאגר הביומטרי תוצאות זיהוי אל רשות האוכלוסין:

סוג התשובה	כמות
הבקשה אושרה	156,630
הבקשה בבירור	1
הבקשה נמצאת בבירור ברשות האוכלוסין	14
הבקשה נדחתה	230
סה"כ בקשות	156,875

אישור – אישור הבקשה וכפועל יוצא אישור להנפיק תיעוד לבעל הרשומה.

דחיה – דחית הבקשה להנפקת תיעוד מסיבות שונות המפורטות בהמשך. הטיפול בבקשה חוזר לרשות האוכלוסין שלעיתים נדרשת לזמן את התושב להרכשה נוספת, לדוגמא.

בירור - מצב ביניים הדורש בחינה מעמיקה של תוצאת ההשוואה טרם העברת תשובה סופית בדבר אישור או דחיה של הבקשה. אם על ידי הרשות לניהול המאגר הביומטרי ואם על ידי רשות האוכלוסין.

- נתוני הטבלה משקפים מצב נתון בתאריך 31 בדצמבר 2015 בשעה 19:00

- במהלך התקופה המדווחת הועברו לבירור רשות האוכלוסין 242 בקשות אשר בגמר תהליך הבירור אושרו או נדחו בהתאם לתוצאת הבדיקה

התפלגות הבקשות המצויות במאגר

במאגר הביומטרי מצויות כלל הבקשות לתיעוד המגיעות ממערך ההרכשה, ללא קשר לסוג מסמך הזיהוי שביקש התושב להנפיק. לדוגמה אדם אשר ביקש בשתי פעמים שונות תיעוד ביומטרי, פעם אחת תעודת זהות ופעם שניה דרכון, מופיע במאגר כשתי בקשות נפרדות, **המשויכות לאותו אדם** (הכמות המצוינת בתחילת הפרק כוללת את כלל הבקשות מאותו אדם **פעם אחת בלבד**. כאמור, Unique). מסיבה זו מספר הבקשות במאגר גבוה ממספר התושבים. מצב זה, של יותר מרשומה אחת לכל תושב, יכול להצביע על מי שביקש במועדים שונים דרכון ותעודות זהות או מצב של בקשה נוספת לאחד ממסמכי הזיהוי, עקב אובדן, גניבה או השחתה.

להלן הנתונים של התפלגות הבקשות במאגר לתקופת הדיווח על פי מספר רשומות לתושב:

מס' רשומות	הערך	סה"כ רשומות
רשומה יחידה לתושב	146,794	146,794
2 רשומות לתושב	4,896	9,792
3 רשומות לתושב	91	273
4 רשומות לתושב	4	16
סה"כ	151,785	156,875

5.3. משך הזמן הדרוש לקבלת תוצאת הזיהוי והעברתה לידי עובד רשות האוכלוסין

להלן נתונים על משך הזמן הדרוש לקבלת תוצאת זיהוי מהרשות לניהול המאגר הביומטרי והעברתה לידי רשות האוכלוסין, על פי מספר הבקשות בכל קטגוריה (משך זמן הטיפול בימי עבודה):

משך הזמן	הערך	%
אותו יום	55	0%
יום אחד	152,027	97%
יומיים	4,793	3%
שלושה ימים	0	0%
מעל שלושה ימים	0	0%
סה"כ	156,875	100%

השאיפה היא כמובן לזמני תגובה קצרים ככל האפשר, מבלי לפגוע באמינות התשובות המגיעות מהרשות לניהול המאגר הביומטרי.

5.4 פעילות השוואות הביומטריות

נכון לתאריך 31 בדצמבר 2015 המאגר כולל 974,680 בקשות (סך הרשומות אשר התקבלו במערכות הרשות הביומטרית הכוללות בקשות חדשות וכן בקשות חידוש), של 856,024 תושבים. בממוצע מצטרפים כ- 1,200 תושבים ביום עבודה. בכל יום מבצעות מערכות הרשות הביומטרית השוואות בצורה ממוכנת של פרטי אותם מצטרפים חדשים מול מאגר הנתונים הקיים. לדוגמא, ביום עבודה ממוצע מבוצעת השוואת נתונים ביומטריים של 1,398 רשומות ביומטריות חדשות מול 974,680 רשומות ביומטריות במאגר. כל תמונת פנים מושווית לתמונות הפנים במאגר וכל אצבע מושווית הן לאצבע ימין והן לאצבע שמאל, סה"כ 5 השוואות לכל בקשה (אחת פנים וארבע אצבעות). המשמעות הנה שבפועל מבוצעות כיום כ - 7,000,000,000 (7 מיליארד) השוואות כל יום על ידי מערכת השוואות הביומטריות.

5.4.1 עצירת הנפקה והסיבות לעצירה

במקרים בהם תוצאת השוואה במערכות הרשות לניהול המאגר הביומטרי הנה "אי התאמה", לא מתקיים תהליך הנפקת תיעוד עבור אותן בקשות. מקרים אלו נובעים ממספר גורמים המפורטים להלן. בכל המקרים מדובר בהתראות אשר מתקבלות על ידי מערכת השוואות הביומטריות ומטופלות בנוסף בצורה ידנית על ידי העובדים המקצועיים ברשות לצורך אימות ווידוא הנתונים. יש לציין כדוגמא את נושא התאומים הזחים אשר לגביהם מתריעה המערכת וכתוצאה מכך יש צורך בטיפול ידני על ידי מפעילי המערכת.

מספר הפעמים שבהן נעצרה (לא התקיימה) הנפקה בתקופת הדיווח הנוכחית והסיבות לעצירה הם כדלהלן:

ערכים	הסיבה לעצירת הנפקה
56	תפעולי - נתונים מנהלתיים שאינם תקינים לדוגמה: טביעת אצבע המתקבלת בצורה אשר מערכת ההשוואות אינה מסוגלת לעבד
83	נתונים ביומטריים של אדם כפי שהתקבלו בבקשת חידוש אינם דומים לנתונים ביומטריים שהתקבלו בבקשות קודמות של אותו אדם.
1	נתונים ביומטריים של אדם דומים לנתונים ביומטריים של אדם אחר במאגר
90	הרכשה של אותה טביעת אצבע הן בימין והן בשמאל לאותו אדם
0	התרעת שווא תפעולית
230	סה"כ

להלן מספר הפעמים שבהן נעצרה (לא התקיימה) הנפקה בכל תקופת המבחן עד 31 בדצמבר 2015 והסיבות לעצירה הם כדלהלן:

סה"כ	H5	H4	H3	H2	H1	הסיבה לעצירת הנפקה
341	56	7	163	42	73	תפעולי - נתונים מנהלתיים שאינם תקינים לדוגמה: טביעת אצבע המתקבלת בצורה אשר מערכת ההשוואות אינה מסוגלת לעבד
232	83	66	41	20	22	נתונים ביומטריים של אדם כפי שהתקבלו בבקשת חידוש אינם דומים לנתונים ביומטריים שהתקבלו בבקשות קודמות של אותו אדם.
21	1	2	0	6	12	נתונים ביומטריים של אדם דומים לנתונים ביומטריים של אדם אחר במאגר
656	90	136	136	130	164	הרכשה של אותה טביעת אצבע הן בימין והן בשמאל לאותו אדם
3	0	2	1	0	0	התרעת שווא תפעולית
1,253	230	213	341	198	271	סה"כ

(*) הנתונים בטבלה לעיל מעודכנים ל-31.12.15. בדוחות הקודמים בוצע חיתוך דומה אך מאז התבצע עידכון לגבי בקשות בסטטוס בירור ולכן המספרים לגבי החציונים הללו מעט שונים מהדוחות הקודמים.

ייעודה המרכזי של מערכת ההשוואה הביومترית ותהליכי העבודה אשר נבנו סביבה הנו איתור הרכשות כפולות ומניעת התחזות. פעילותה השוטפת של הרשות לניהול המאגר הביומטרי כוללת ביצוע השוואת הנתונים הביומטריים של מבקשי התיעוד מול כלל הנתונים אשר מאוחסנים במאגר. מדובר בתהליך הכולל פעילות מערכת ממוכנת וטיפול מקצועי פרטני של עובדים מקצועיים ומומחים בתחום.

בטבלה לעיל מפורטים המקרים שאותם איתרה מערכת ההשוואה בפועל כאירועי הרכשה כפולה וחשד להתחזות, מתוך כלל האירועים האפשריים שלהלן:

- 1) שני אנשים שונים שהורכשו בטעות באותה זהות.
- 2) תאומים שהורכשו בטעות באותה זהות.
- 3) הרכשה של אותו אדם, בטעות בשתי זהויות שונות.
- 4) הרכשה מוטעית של אותה אצבע הן בימין והן בשמאל.
- 5) ניסיונות התחזות לצורך קבלת תיעוד במרמה.
- 6) חלק מהנתונים הביומטריים שייכים לאדם אחר.
- 7) אי-התאמה לרשומות קודמות של אותו אדם.

המשמעות של עצירת מעל 1,250 הנפקות אלו בזכות פעילות ההשוואה במערכות המאגר, הנה כי נמנעה הנפקת מסמכי זיהוי אשר היו כוללים נתונים ביומטריים שגויים. בחלקם מקרים אשר בוודאות הינם ניסיונות להרכשה כפולה, בחלקם ניסיונות החשודים ככאלו ובחלקם נוגעים לבעיות תפעוליות כפי שמוסבר לעיל.

6. מדדי ביומטריה (דיוק המערכת הביומטרית)

סעיף זה דן בביצועי המערכת הביומטרית מבחינת דיוק. ניתן למצוא פירוט של מדדי הדיוק והמושגים שלהלן בפרוטוקול תקופת המבחן.

6.1 מערכת ההשוואה הביומטרית

- מערכת ההשוואות הביומטריות הפעילה ברשות ממועד תחילת הפרויקט, הנה מערכת המבוססת על מנועי השוואה ביומטריים (מנוע השוואת תמונות פנים ומנוע השוואת טביעות אצבע) אשר נרכשו מהספקים מהמובילים בתחום זה בעולם.
- מנועי ההשוואה הללו פעילים בשימוש בפרויקטים במדינות שונות ומעורבים בהשוואות של מיליוני פרטים ביומטריים בפרויקטים אלו.
- על בסיס מנועי ההשוואה הללו פותחו ברשות ממשקי משתמש, מערכת קבלת החלטות ותהליכי עבודה המותאמים לצרכי הרשות במסגרת הפרויקט.
- **מערכת ההשוואות הביומטריות הפעילה ברשות הנה מערכת אמינה העומדת בסטנדרטים המקובלים ובמדדי הדיוק והביצועים הנדרשים בחקיקה.**
- **בדיקות שוטפות, הן לביצועי המערכת והן לרמות הדיוק של פעילות ההשוואות, מבוצעות ברשות על ידי גורמים מקצועיים בלתי תלויים.**
- כאמור לעיל, ביום עבודה ממוצע מבוצעת השוואת נתונים ביומטריים של כ- 1,400 רשומות ביומטריות חדשות מול למעלה מ- 970 אלף רשומות ביומטריות במאגר. המשמעות הנה השוואת טביעות אצבע חדשות מול קיימות וכן השוואת תמונות פנים חדשות מול קיימות. בפועל מבוצעות כיום כ – **7,000,000,000 (7 מיליארד) השוואות ביום על ידי מערכת ההשוואות הביומטרית.**
- **בנוסף לכך, הרשות ממשיכה בתהליכי הטמעת מערכת ההשוואות ביומטריות אשר בשילוב עם המערכת הנוכחית תאפשר יעול תהליכי העבודה ושיפור הביצועים.**
- המערכת הנרכשת מהווה שדרוג טכנולוגי של המערכת הקיימת כאשר לאחר הטמעתה יפעלו שתי המערכות במקביל. תצורת פעולה זו מקובלת בפרויקטים דומים בעולם ומאפשרת שיפור רמות דיוק ההשוואה על ידי שימוש במגוון מנועים ביומטריים לביצוע תהליכי ההשוואות.

6.2 הדרישה המוגדרת בצו בכל הנוגע לביצועי המערכת

- לגבי השוואה של אמצעים ונתונים ביומטריים של תושב מול האמצעים והנתונים הביומטריים הכלולים במאגר לגבי אותו תושב, מדד להצלחה יהיה קצב שגיאות של לא יותר מקבלה מוטעית אחת לכל 10,000 נטילות, וקצב שגיאות של לא יותר מדחייה מוטעית אחת לכל 100 נטילות.

- לגבי השוואה של אמצעים ונתונים ביומטריים של תושב מול כל האמצעים והנתונים במאגר, מדד להצלחה יהיה קצב שגיאות של לא יותר מאי התאמה מוטעית אחת לכל 20 נטילות, וקצב שגיאות של התאמה מוטעית אחת, לפי המתואר בטבלה הבאה, לפי גודל המאגר:

<u>גודל המאגר</u>	<u>קצב שגיאות של</u>
עשר מיליון רשומות	לא יותר מהתאמה מוטעית אחת לכל 100 נטילות
מיליון רשומות	לא יותר מהתאמה מוטעית אחת לכל 1000 נטילות
מאה אלף רשומות	לא יותר מהתאמה מוטעית אחת לכל 10,000 נטילות

- לגבי מספר הפעמים שבהם נעצרה הנפקה בשל חשד להרכשה כפולה שאותר ברשות, מדד להצלחה הוא עצירת הנפקה ביותר מ- 95% מהמקרים שבהם התבצעה הרכשה כפולה, וכן זיהוי של 95% מהניסיונות היזומים להתחזות בזהות כפולה.

6.3. מדדי הדיוק של המערכת הביومترית במאגר (בהתאם לפרוטוקול תקופת המבחן)

את בדיקות הביצועים, עמידה במדדים ובחינת החלופות הביומריות מלווים המרכז למחקרים צבאיים (מחצ"ב) רפא"ל וכן יועץ חיצוני מקצועי בתחום הביומרית.

1. במסמכי מחצ"ב רפא"ל אשר ציטוטים מהם מובאים להלן, מושוים ביצועי המאגר ליעדי הביצועים שהוגדרו בחוק. הניתוח מבוסס על שני מדגמים:

א. **טביעות אצבע:** מדגם של כ-6,000 השוואות נכונות (רישום נוסף של נבדק במאגר (חידוש)) וכ-24 מיליארד השוואות לא נכונות

ב. **תמונת פנים:** כ-40 אלף השוואות נכונות (חידושים) וכ-25 מיליארד השוואות לא נכונות.

ג. נתוני אמת עם חידוש לאחר שנה וחצי עד שנתיים – כ-4,000 השוואות נכונות וכ-25 מיליארד השוואות לא נכונות .

ד. נתוני יצרן

2. הניתוח אינו מתייחס למערך האנושי שתומך ומגבה את המערכת הטכנית. המערך האנושי מבצע טיפול בכל התרעות המערכת ומהווה גורם מקצועי נוסף אשר מקבל החלטות על בסיס הנתונים הביומטריים ובטרם קבלת החלטה סופית לגבי הנפקת תיעוד לתושב.

הערה: דו"חות מחצ"ב רפא"ל הינם מסווגים ומועברים לגורמים הרלוונטיים בתפוצה מוגבלת.

6.3.1. השוואה לצורך אימות 1:1 (One to One)

השוואות אלו הן למעשה תהליך אימות זהות, להבדיל מתהליך זיהוי. במצב זה קיים מידע מראש על הזהות הצפויה שאמורה להיות מיוצגת על ידי אותה רשומה ביומטרית. תהליך ההשוואה הוא בין המידע הנבדק לדגימת ייחוס יחידה, שידועה כבר לגבי אותה זהות, השוואת 1:1.

להלן ציטוטים מדו"ח רפאל "ניתוח ביצועי המאגר הביומטרי - נובמבר 2015 V1" על משימת אימות במאגר בעל היתוך של 3 מנועים, שתי טביעות אצבע ותמונת פנים:

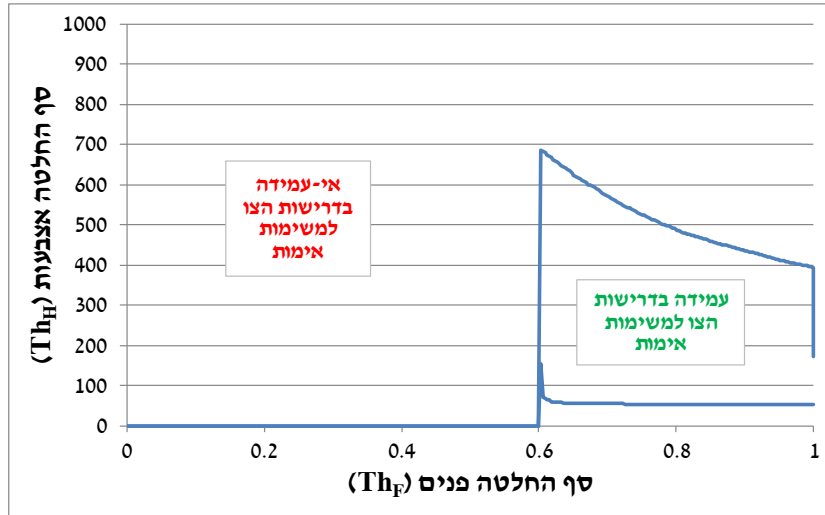
משימת אימות

1. היתוך טביעת אצבע ימין, טביעת אצבע שמאל ותמונת פנים (אמת ויצרן):
2. באיור 1,2 מוצגים מיפוי של אוסף זוגות הספים שעומדים בדרישות הצו למשימות אימות, עבור היתוך שתי טביעות אצבע עם נתוני אמת ונתוני יצרן של זיהוי פנים.



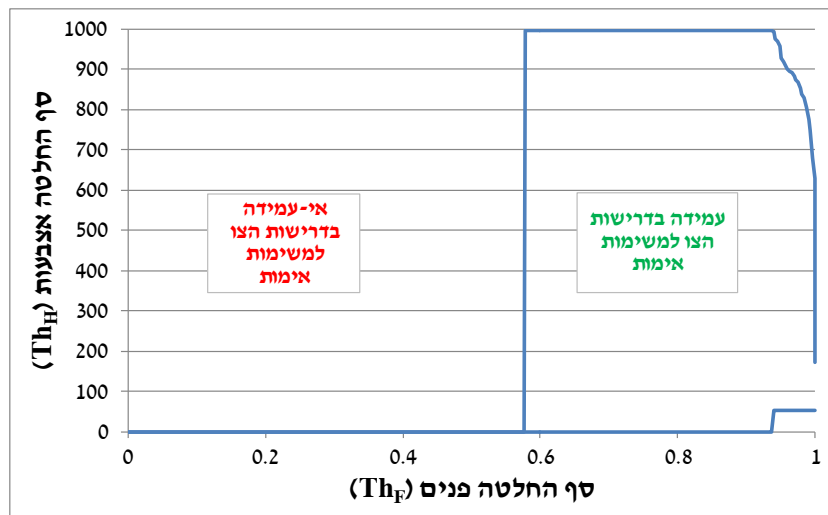
איור 1: אוסף זוגות ספי החלטה שעומדים בדרישות הצו למשימות אימות – שתי טביעות אצבע ונתוני אמת של זיהוי פנים

3.



איור 2: אוסף זוגות ספי החלטה שעומדים בדרישות הצו למשימות אימות – שתי טביעות אצבע ונתוני יצרן של זיהוי פנים

4. מניתוח של התוצאות עולה כי קיים אוסף רחב של זוגות ספי החלטה – (Th_H, Th_F) , שעבורם $FAR(Th_H, Th_F) < 1/10,000$ וגם $FRR(Th_H, Th_F) < 1/100$. המשמעות היא שלפי היתוך מנועי שתי טביעות אצבע ופנים, המתייחס לכלל ההחלטה שנבדק, המאגר עומד בדרישות הצו לגבי משימות אימות.



סיכום - ביצועי המאגר במשימות אימות

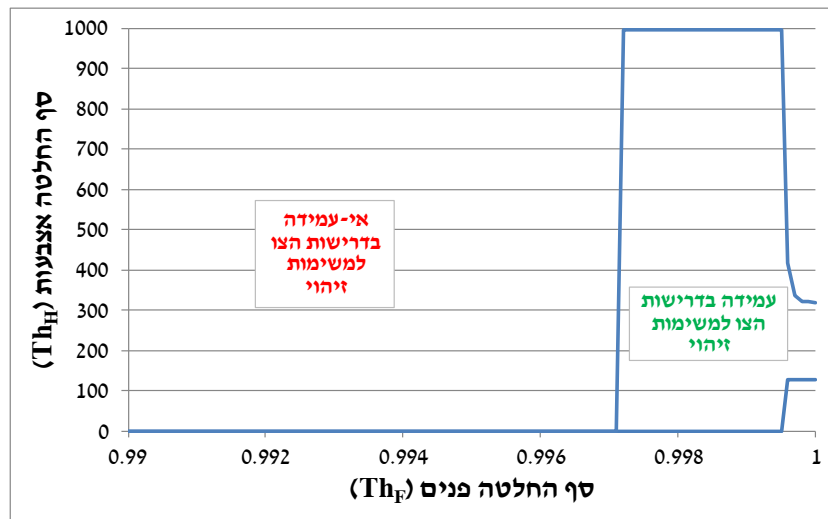
5. לאור האמור לעיל, היות שמנוע זיהוי פנים (לפי נתוני אמת) וכן היתוכים מסוג ציון מרבי אשר כוללים מנוע זה (הן לפי נתוני אמת והן לפי הצהרות יצרן), נסיק שהמאגר עומד בדרישות הצו למשימות אימות.

6.3.2. השוואה לצורך זיהוי N:1 (One to Many)

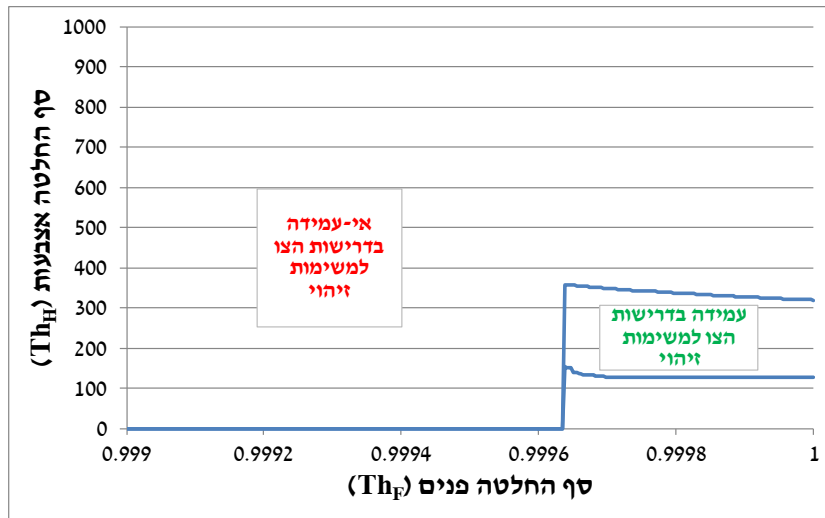
ההשוואות שלהלן הן תהליך של זיהוי, כלומר ההשוואה מתבצעת בין המידע הנבדק לכלל דגימות הייחוס שבמאגר, השוואת 1:N

משימת זיהוי

1. היתוך טביעת אצבע ימין, טביעת אצבע שמאל ותמונת פנים. באיורים 3 ו-4 מוצג מיפוי של אוסף זוגות הספים שעומדים בדרישות הצו למשימות זיהוי עבור היתוך של שתי טביעות אצבע ונתוני אמת של זיהוי פנים ועבור היתוך שתי טביעות אצבע ונתוני היצרן של זיהוי פנים, בהתאמה.



איור 3: אוסף זוגות ספי החלטה שעומדים בדרישות הצו למשימות זיהוי – שתי טביעות אצבע ונתוני אמת של זיהוי פנים



איור 4: אוסף זוגות ספי החלטה שעומדים בדרישות הצו למשימות זיהוי – שתי טביעות אצבע ונתוני יצרן של זיהוי פנים

2. מניתוח של התוצאות עולה כי קיים אוסף רחב של זוגות ספי החלטה – (Th_H, Th_F) , שעבורם $FMR(Th_H, Th_F) < 1/10,000$ וגם $FNMR(Th_H, Th_F) < 1/20$. המשמעות היא שלפי היתוך שני מנועי טביעות אצבע ומנוע זיהוי פנים, המתייחס לציון מרבי לרשומה, המאגר עומד בדרישות הצו לגבי משימות זיהוי.

סיכום – ביצועי המאגר במשימות זיהוי

3. לאור האמור לעיל, היות והיתוכים מסוג ציון מרבי אשר כוללים מנוע פנים (הן לפי נתוני אמת והן לפי הצהרות יצרן), נסיק שהמאגר עומד בדרישות הצו למשימות זיהוי.

6.3.3. איתור אירועי הרכשה כפולה ואירועים חריגים

ייעודה המרכזי של מערכת ההשוואה הביومترית ותהליכי העבודה אשר נבנו סביבה הנו **איתור הרכשות כפולות ומניעת התחזות**. פעילותה השוטפת של הרשות לניהול המאגר הביומטרי כוללת ביצוע השוואת הנתונים הביומטריים של מבקשי התיעוד מול הנתונים אשר מאוחסנים במאגר. מדובר בתהליך הכולל פעילות מערכת ממוכנת וטיפול מקצועי פרטני של עובדים מקצועיים ומומחים בתחום.

בטבלה מפורטים המקרים שאותם איתרה מערכת ההשוואה בפועל כאירועי הרכשה כפולה וחשד להתחזות, מתוך כלל האירועים האפשריים שלהלן:

- שני אנשים שונים שהורכשו בטעות באותה זהות.
- תאומים שהורכשו בטעות באותה זהות.
- הרכשה של אותו אדם, בטעות בשתי זהויות שונות.
- הרכשה מוטעית של אותה אצבע הן בימין והן בשמאל.
- ניסיונות התחזות לצורך קבלת תיעוד במרמה (מקרה אחד).
- חלק מהנתונים הביומטריים שייכים לאדם אחר.
- אי-התאמה לרשומות קודמות של אותו אדם.

הערך	תיאור האירוע
83	נתונים ביומטריים של אדם כפי שהתקבלו בבקשת חידוש אינם דומים לנתונים ביומטריים שהתקבלו בבקשות קודמות של אותו אדם. המשמעות: ישנן שתי בקשות לתיעוד של אותו אדם עם נתונים ביומטריים שונים
1	נתונים ביומטריים של אדם דומים לנתונים ביומטריים של אדם אחר במאגר. המשמעות: ישנן שתי בקשות לתיעוד עם אותם נתונים ביומטריים של אנשים שונים
90	הרכשה של אותה טביעת אצבע הן בימין והן בשמאל
174	סה"כ

• חשד לניסיונות התחזות:

- ארוע בו נתונים של אדם בבקשת החידוש אינם דומים לנתונים ביומטריים קודמים שהתקבלו בבקשה לאותה זהות, עשויים להעיד על ניסיון להתחזות ולגניבת הזהות על ידי אדם אחר.
- ארוע בו מורכשת אותה טביעת אצבע הן בימין והן בשמאל עשוי להעיד על כוונה לניסיון התחזות עתידי.

7. אבטחת מידע ופרטיות ברשות לניהול המאגר הביومتر

מראשית הקמתה עוסקת הרשות לניהול המאגר הביومتر בצורה אינטנסיבית בפעילות לאבטחת מערכות המידע ולהגדרת תהליכי עבודה מתאימים ומאובטחים. הרשות הקימה במהלך תקופה זו מערך מחשוב מאובטח בהתאם לסטנדרטים המחמירים ביותר, תוך מתן מענה לסיכוני אבטחת מידע והגנה על פרטיות בהתאם לאיום הייחוס וניהול הסיכונים.

אבטחת המידע ואבטחת הפרטיות של נתוניהם הביומטריים של אזרחי המדינה מבוססות על מספר מעגלי אבטחה נפרדים כאשר בכל מעגל מושקעים משאבים רבים - אנושיים, טכנולוגיים, פיזיים ונוהליים. בנוסף קיים תהליך שוטף של בקרה וביקורת על נושאים אלו על ידי עובדי הרשות בתפקידי אבטחת מידע והגנת הפרטיות העוסקים בתחום באופן שוטף.

תצורת האבטחה הפיזית, מערך הצופן ואבטחת מערכות המידע נבדקו ואושרו על ידי החטיבה לסיכול איומי סייבר בשב"כ בהתאם לדרישת החוק.

בראש צוות האבטחה אשר פועל ברשות מיום הקמתה, עומד כיום מנהל אשר מונה בספטמבר 2014, לאחר כחצי שנה של הליכי גיוס, וממשיך את ביצוע הפעולות כנדרש בחוק. במהלך כל תקופת המבחן ממלא מנהל הגנת הפרטיות ברשות את תפקידו כנדרש.

כלל הפעולות המבוצעות ברשות בנושאי אבטחת מידע מאושרות ומפוקחות על ידי הגורם המנחה – החטיבה לסיכול איומי סייבר בשב"כ

אבטחת המידע והגנת הפרטיות מבוססים כאמור על מספר מעגלי אבטחה, כאשר העיקרון המנחה הוא שכל מעגל אבטחה עונה על סך תרחישים וסיכונים מוגדרים ואילו סך המעגלים יחד, עונה על סך התרחישים והסיכונים עמם אנו מתמודדים. מעגלי האבטחה השונים כוללים בין היתר:

7.1. ניהול סיכונים

המאגר הביומטרי הינו נכס חשוב של מדינת ישראל ויתכן שיהיה יעד מועדף לתקיפה על ידי גורמים עוינים. עבודות אשר כללו הערכת סיכונים הן בהיבטי אבטחת מידע והן בהיבטי הגנת הפרטיות, מאוגדות וכלולות במספר מסמכים מסווגים. מיפוי האיומים והסיכונים הפוטנציאליים למאגר הביומטרי וכן בחינת איום הייחוס בוצעו טרם תחילת תקופת המבחן בהובלת הממונה על היישומים הביומטריים במשרד רה"מ ובשיתוף גורמי הביטחון. מיפוי האיומים והסיכונים מתעדכן מעת לעת ומתוקף על ידי הגורמים המקצועיים ברשות וכן על ידי החטיבה לסיכול איומי סייבר בשב"כ.

7.2. אבטחת מידע – היבטי המבנה הארגוני

הוקמה רשות ייעודית לצורך הקמה, אבטחה וניהול של המאגר הביומטרי. הרשות לניהול המאגר הביומטרי פועלת בכפיפות ישירה לשר הפנים. הרשות מנהלת פעילות אוטונומית, בדגש על ניהול ותפעול עצמאיים של מערכות המידע.

7.2.1. סיווג בטחוני

בוצע תהליך הכשר בטחוני לעובדי הרשות - כל עובדי הרשות הם בעלי הכשר ביטחוני ברמה הנדרשת ואושרו על ידי השב"כ.

7.2.2. הרשאת גישה

העקרון המנחה את הרשות בפעילותה הנו מתן ההרשאות המזעריות ביותר הנדרשות לצורך מילוי התפקיד לכל בעל תפקיד ברשות. עובדי הרשות אשר מתוקף אחריותם ותפקידם נדרשים לגישה לנתונים הביומטריים, אושרו בכתב על ידי ראש הממשלה ושר הפנים, וזאת לאחר בחינה מדוקדקת של הצורך בגישה של העובד לנתונים ביומטריים.

7.2.3. מידור והפרדת תפקידים

קיימת חלוקה ברורה ומידור פנימי בין עובדי הרשות בנושא הגישה לנתונים ביומטריים. מידור זה בא לידי ביטוי הן בנושאים פיזיים כגון גישה למתחמים ואזורים שונים והן בנושאים טכנולוגיים כגון גישה למערכות המידע והרשאות גישה למידע.

7.3. אבטחה פיטית

מתחם הרשות לניהול המאגר הביומטרי מאובטח ומוגן בהתאם לדרישות הרשות הממלכתית לאבטחת מידע בשב"כ. יתרה מכך, מתחם הרשות מצויד באמצעים פיזיים וטכנולוגיים מתקדמים ביותר אשר מבטיחים כי כל פעילות מחוץ ובתוך המתקן תתועד ותבוקר באופן שוטף. מערכות האבטחה אשר הוקמו נבדקו ואושרו על ידי הרשות הממלכתית לאבטחת מידע בשב"כ.

7.4. אבטחת מידע

7.4.1. הפרדת סביבות וניתוק תקשורתי

מערכות המחשוב ברשות הוקמו כסביבת מחשוב נפרדת לחלוטין אשר אינה מקושרת לכל רשת חיצונית בכל צורת חיבור שהיא לרבות לא למערכות רשות האוכלוסין.

7.4.2. הקשחה

המערכות הקיימות הוקשחו על פי נהלי אבטחה מחמירים ביותר ועל פי הנחיות הרשות הממלכתית לאבטחת מידע בשב"כ, והן מנוטרות ומבוקרות באופן שוטף.

7.4.3. הצפנה

הנתונים הביומטריים המאוחסנים בבסיסי הנתונים של הרשות מוצפנים. הצפנה זו מבטיחה כי גורם שאינו מורשה לא יוכל להפיק מנתוני המאגר מידע בעל ערך.

7.4.4. מזעור כמות וסוג הנתונים במאגר

בסיסי הנתונים המרכיבים את המאגר מכילים אך ורק צילומי טביעות שתי האצבעות המורות וכן צילום פנים ומזהה מוצפן לכל רשומה. המאגר אינו מכיל כל פריט מידע ממרשם האוכלוסין. אין בבסיסי הנתונים נתונים ביוגרפיים או דמוגרפיים של מבקשי התיעוד. המאגר אינו מכיל כתובות, שמות, מספרי זהות או נתונים אחרים דומים.

7.4.5. בקרת פעילות וביקורת

פעילות העובדים מול בסיסי הנתונים מבוקרת ומנוטרת הן בצורה ממוכנת והן על ידי בקרה של גורמי אבטחת המידע והממונה על הגנת הפרטיות במאגר. פעילות העובדים מבוקרת ומנוטרת ע"י מנהל אבטחת

המידע בתחום הפיזי בגישה למתחמים המסווגים. פעילות העובדים מול מערכות המחשוב המסווגות מתועדת ומנוטרת. בנוסף, מיושמים מנגנונים (ע"פ החוק) המחייבים מעורבות של שני עובדים בעת ביצוע פעולות בבסיסי הנתונים של המאגר (Dual control).

7.4.6. נהלים ותהליכי עבודה

אושר מסמך מדיניות אבטחה ונכתבו ואושרו נהלי עבודה מתאימים. כלל תהליכי העבודה ברשות נבנים לאור דרישות אבטחה והגנה על הפרטיות המחמירות ביותר.

7.5. סקרי סיכונים ומבדקי חדירות

בהתאם ללשון הצו עומדת הרשות לניהול המאגר הביومتر בהנחיות הרשות הממלכתית לאבטחת מידע, התקבלו מלוא האישורים להתחיל בתקופת המבחן והפעילות מבוצעת על פי הנהלים הקיימים.

טרם התחלת תקופת המבחן בוצעו ברשות לניהול המאגר הביומרטי מגוון מבדקי אבטחה, ביקורות וסקרי סיכונים על ידי גורמי הביטחון האמונים על הנושא וכן על ידי גורמים בלתי תלויים שעברו סיווג מתאים. כל ממצאי הסקרים נבדקו וטופלו. הפעילות החלה רק לאחר קבלת האישורים הנדרשים מכל הגורמים המוסמכים לכך.

סקרי סיכונים, ביקורות ומבדקי חדירה נוספים מתוכננים כחלק מתוכנית העבודה השנתית וכחלק מהוראות החוק כאשר מטרתם אחת - להמשיך ולעמוד ברף האבטחה הגבוהה הקיים היום.

בדצמבר 2014 בוצעו מבדקי חדירה וסקר סיכונים על ידי גורמי הביטחון הרלוונטיים, אותם עברה הרשות בהצלחה

8. בדיקת אתר גיבוי

בהתאם ללשון הצו "בתקופת המבחן תבצע הרשות אחת לחצי שנה ניסוי מעבר לעבודה באתר הגיבוי. מדד ההצלחה בניסוי ייחשב מעבר לעבודה באתר הגיבוי, אשר בחלוף שישים שעות מתחילת ביצועו אפשר עבודה באתר הגיבוי".

הרשות לניהול המאגר הביומטרי הקימה אתר גיבוי מאובטח ונפרד לחלוטין ממערכות האתר הראשי. אתר זה משמש כאתר חלופי בעת אסון. האתר מאובטח ברמה המתאימה לאתר מחשוב ברמת סיווג "סודי ביותר" בהתאם להנחיות הגורם המנחה בשב"כ אף על פי שאינו כולל נתונים ביומטריים או נתונים רגישים כלל. באתר הגיבוי בוצעו מספר ניסויים שמטרתם ולוודא כי בעת אסון ניתן להמשיך בשגרת הפעילות מהאתר החלופי.

במהלך תקופת הדיווח הנוכחית בוצע תהליך התאוששות מאסון אשר כלל מעבר מלא ועבודה באתר הגיבוי. העבודה באתר הגיבוי בוצעה בהצלחה מלאה וזאת בתוך פחות משישים שעות מתחילת הפעילות ובהתאם לנדרש בצו.

יש לציין כי בכל מהלך תקופת המבחן בוצעו ודווחו כנדרש, תהליכי התאוששות מאסון אשר כללו מעבר מלא ועבודה באתר הגיבוי בכל חצי שנה כנדרש.

הנתונים הביומטריים נשמרים ומאובטחים ברשות לניהול המאגר הביומטרי בלבד ואינם מועברים או נשמרים בשום אופן בידי חברה פרטית חיצונית או גורם אחר כלשהו

9. הסתייעות בגורמי חוץ

סעיף 16.2 בפרוטוקול נותן את הדעת לאפשרות שבמאגר נדרש יהיה להסתייע אד-הוק במומחים/גורמי חוץ. כניסה של גורמי חוץ למאגר הנה אירוע המחייב תשומת לב מיוחדת בהיבט אבטחת המידע והפרטיות ויש לדווח עליו במידה והוא מתקיים.

בתקופת הדיווח הנוכחית לא הסתייעה הרשות לניהול המאגר הביומטרי בגורמי חוץ כלשהם.

10. שמירת המידע

סעיף 16.3 בפרוטוקול קובע כי מידע שייאסף במהלך הפיילוט לא יכלול נתונים או אמצעים ביומטריים או מידע מזהה אחר. באותם מקרים בהם יש לשמור תמונה ממערך ההרכשה (כדי לנתח בעיות תאורה למשל) יש לשמור אך ורק תמונה מופחתת. דבר זה אמור גם לגבי התמונות הסרוקות.

בתקופת הדיווח הנוכחית, כמו גם בתקופות הקודמות, המידע הביומטרי נשמר במערכות הרשות לניהול המאגר הביומטרי בלבד שאינן מחוברות למערכות חיצוניות אחרות. מידע ביומטרי לא נשמר מחוץ למערכות המאגר למעט תמונות מופחתות הנשמרות במערכת רשות האוכלוסין כפי שמתיר החוק.

הנתונים הביומטריים נשמרים במאגר הביומטרי **בלבד** והמאגר מנוהל על ידי הרשות לניהול המאגר הביומטרי בקפידה רבה בהתאם להוראות החוק ונהלי אבטחת מידע והפרטיות שהוגדרו על ידי הממשלה. אין אפשרות לקשר בין פרטי האדם הנרכש לנתונים הביומטריים הנשמרים במאגר הביומטרי.

11. העברת המידע מהמאגר לגורמי חוץ

סעיף 17.1 בפרוטוקול קובע כי בתקופת המבחן לא תהיה הוצאה של מידע כלשהו מהמאגר לגורם חיצוני. לרשות האוכלוסין תועבר אך ורק תוצאת תהליך ההשוואה לאחר השוואת הרשומות במאגר (תשובה "חיובית", "שלילית" או "בבירור"). תוצאת הזיהוי תועבר על ידי מילוי ידני של נתונים בשדה/מסך ייעודי במערכת רשות האוכלוסין. לא יועבר כל מידע נוסף מהמאגר.

כפי שדווח בתקופות הדיווח הקודמות, כך גם בתקופת הדיווח הנוכחית (ובמהלכה של כל תקופת המבחן) מערכת המחשוב של הרשות לניהול המאגר הביומטרי היא מערכת אוטונומית אשר מנותקת ומופרדת לחלוטין מהעולם החיצוני ואין כל העברה של נתונים ביומטריים מהמערכת לגורם חיצוני.

המידע הנמסר על-ידי רשות לניהול המאגר הביומטרי לרשות האוכלוסין על מנת לאשר או לדחות בקשה לקבלת תיעוד ביומטרי מבוצע מול מספר בקשה כאשר התשובה הנה סטטוס הבקשה בלבד (אישור/דחייה/בבירור), פרט למידע זה, לא מועבר כל מידע אחר מהמאגר הביומטרי לשום גורם כזה או אחר.

12. נגישות למידע במאגר

סעיף 17.2 קובע כי מספר מורשי הגישה למאגר הינו מצומצם ביותר ומוגבל רק לבעלי תפקידים החיוניים להפעלתו של המאגר. המידע השמור במאגר הביומטרי יהיה נגיש אך ורק לבעלי תפקידים שהינם עובדי הרשות לניהול המאגר, בעלי תפקידים חיוניים כמוגדר בחוק ומומחי זיהוי (בכפוף להתאמתם מבחינת סיווג

ביטחוני ולדרישות החוק והתקנות). רק עובדי הרשות לניהול המאגר הביומטרי יוכלו לבצע פעולות מול המאגר.

בתקופת הדיווח הקודמת, מספרם של מורשי הגישה למערכת המאגר שהוגדרו ואושרו בהתאם להנחיות הצטמצם בבעל תפקיד מורשה גישה אחד. בתקופה הנוכחית נוספו שני בעלי תפקידים מורשי גישה.

13. עלויות תקציביות

מסגרת התקציב להקמת הרשות לניהול המאגר הביומטרי ולהפעלתה עומדת על כ- 60 מיליון ₪ לחמש שנים מיום הקמת הרשות בסוף שנת 2011.

מסגרת תקציב זו כוללת את סך כל הוצאות ועלויות הרשות לשנים אלו. כולל עלויות שכר עובדי הרשות ויועצים חיצוניים, כולל הקמת מערך המחשוב ותחזוקתו, רכש מערכות והטמעתן, כולל עלויות אבטחה פיזית ואבטחת מידע, כולל עלויות שכירות אתר הרשות, הוצאות תפעול, עלויות אתר גיבוי, הסברה ויחסי ציבור וכל הוצאה נוספת כנדרש.

**תקציב הרשות לניהול המאגר הביומטרי בסך כולל של כ- 12 מיליון ₪ בשנה
ומהווה כ- 7% בלבד מתקציב פרויקט התעוד הלאומי החכם**

14. סיכום

המעבר לתיעוד ביומטרי חכם המבוסס על מאגר נתונים ביומטריים הנו פרויקט לאומי בעל חשיבות עליונה. כפי שהובהר בדו"חות התקופתיים הקודמים ובדין וחשבון המסכם, תופעת גניבת הזהות וההתחזות במדינת ישראל הנה תופעה נפוצה אשר מסבה נזקים משמעותיים למדינה ולתושביה בהיבטים הכלכלי, הביטחוני ואף בהיבט הדמוקרטי. **על המדינה חלה חובה לאפשר לתושביה רמה גבוהה של ביטחון אישי והגנה על פרטיותם.** התעוד הביומטרי החכם בשילוב המאגר הביומטרי מאפשרים עמידה ביעד אשר נקבע: **"תעוד אחד לאדם אחד".** יישום המאגר הביומטרי הכולל שתי טביעות אצבע ותמונת פנים בלבד מאפשר למדינה לממש את חובתה כלפי אזרחיה תוך איזון מידתי בין ההגנה על פרטיות זהותם מחד, למניעת תופעת גניבת הזהות וההתחזות, מאידך.

המאגר הביומטרי מאפשר ניהול תקין של מרשם האוכלוסין לצד הבטחת קיומו של תיעוד לאומי אמין ומהימן אשר מהווים נדבכים מרכזיים בשמירת חוסנה הלאומי של החברה בישראל.

דין וחשבון זה, שנערך לתקופה חמישית של שישה חודשים, מסכם תקופת פעילות של שנתיים וחצי במסגרת הפרויקט. **במהלך תקופה זו קיבלו מעל 850 אלף מתושבי מדינת ישראל תעודות זהות ו/או דרכונים ביומטריים חדשים.** נתון זה מצביע על רמת האמון הגבוהה אשר הציבור הרחב מביע בפרויקט. יעדי הפרויקט כפי שהוצגו בשלבי התכנון מושגים בצורה מלאה. תהליכי ההרכשה וההנפקה מבוצעים בצורה טובה, תהליכי ההשוואה הביומטרית במערכות הרשות לניהול המאגר הביומטרי מאתרים ומונעים הרכשות כפולות. הפעילות כולה מתאפיינת במינימום תקלות. רמת האבטחה וההגנה על הפרטיות הן גבוהות ביותר כפי שנדרש בחוק וכפי שמוגדר ומפוקח על ידי הגורמים הרלוונטיים.

תקופת המבחן ליישום החוק נקבעה, בין היתר, לצורך למידה והפקת לקחים. תהליכי הבחינה, הלמידה והפקת הלקחים נמשכו ברשות לניהול המאגר הביומטרי לכל אורכה של תקופת המבחן והרשות פעלה ופועלת לשיפור השירות ולייעול התהליכים.

כפי שצוין בדו"ח המסכם את תקופת המבחן הראשונה, אשר הוגש לשר הפנים ולרה"מ במרץ 2015 והדו"ח המסכם המעודכן אשר הוגש בדצמבר 2015 בעקבות הארכתה של תקופת המבחן, הרשות לניהול המאגר הביומטרי ביצעה באופן מלא את החובות המוטלות עליה ובכללן את הבדיקות ואת הבחינות הנדרשות ועמדה במדדים וביעדים הנדרשים כפי שקבע המחוקק. עובדה זו צוינה גם במסמך המסכם של הוועדה המייעצת המפקחת על התנהלותה של תקופת המבחן אשר הוגש בסוף מאי 2015 לשר הפנים.

תוצאות ביצוע מבדקי החלופות אשר נערכו ברשות עד כה, מצביעות בבירור על כך שהשוואה של מספר נתונים ביומטריים (MultiModal Biometric) מאפשרת ביצועים טובים בהרבה מן הביצועים המתקבלים מהשוואתם של נתונים ביומטריים נפרדים, כדוגמת תמונת פנים בלבד או טביעת אצבע בלבד.

שימוש במנגנון Fusion שהינו איחוד תוצאות השוואת הנתונים הביומטריים השונים מאפשר רמת דיוק גבוהה יותר. כלומר, **שילוב תוצאות של מנוע השוואת הפנים עם מנוע השוואת טביעות האצבע מאפשר קבלת תוצאות מדויקות וטובות, הן מבחינת כמות התראות שווא והן מבחינת הסיכוי לאיתור מתחזה.**

פעילות ההשוואה במערכות הרשות הביומטרית אפשרה בתקופת הדיווח הנוכחית את מניעת הנפקתם של מאות מסמכים מזהים (תעודות זהות ו/או דרכונים), אשר היו כוללים נתונים ביומטריים אשר אינם תקינים או אינם תואמים את זהותו של בעל התעוד.

פעילות הרשות תומכת בחזון מדינת ישראל אשר כולל שיפור ניכר ברמת השירותים המקוונים הניתנים לתושבים במגוון נושאים. השימוש בתיעוד הביומטרי החכם ישמש כבסיס עבור חלק ניכר מנושאים אלו. **המאגר מאפשר רמת מהימנות גבוהה ביותר של התיעוד. על בסיס שילוב של השניים מתקבל הבסיס למימוש חזון זה.**

העולם סביבנו מתקדם לשימוש בטכנולוגיה המבוססת על זיהוי ביומטרי ככלי מרכזי לאימות זהות. במסגרת תהליכים אלו, מדינות רבות, כגון ארצות הברית, מדינות האיחוד האירופי ורבות נוספות, מקימות מאגרים ביומטריים המאפשרים הגנה על זהות האזרחים ורמת מהימנות גבוהה מאוד של התעוד. מדינת ישראל מצטרפת למועדון המדינות המתקדמות אשר מציעות ומיישמות שירותים הניתנים בגישה מרחוק (ממשל זמין ויישומים נוספים) ואשר מבוססים על מהימנות התיעוד וזהות האזרח.