הצוות הבין-משרדי לבחינה של ההסדר הראוי להעברת מידע אישי בין גופים ציבוריים

טיוטת דו"ח להערות הציבור

תוכן העניינים

פתח דבר 3
תקציר מנהלים 5
פרק א: רקע לעבודת הצוות 7
1. ההליכים שקדמו לעבודת הצוות 7
2. התשתית הנורמטיבית להעברת מידע אישי בין גופים ציבוריים 10
3. ההליך לאישור העברת המידע האישי 12
פרק ב: ממצאי הצוות 14
1. נתוני שימוש במנגנון הקיים 14
2. אתגרים בהעברת מידע אישי בין גופים ציבוריים 14
פרק ג: סקירה בין לאומית 17
1. המסגרת הנורמטיבית המסדירה שיתוף מידע בין גופים ציבוריים 17
2. ההליך הבירוקרטי הכרוך בשיתוף מידע אישי בין גופים ציבוריים 19
3. התשתית הטכנולוגית התומכת בהעברות מידע בין גופים ציבוריים 20
פרק ד: המלצות הצוות 21
1. גילוי ואיתור הנתונים בין גופים ציבוריים 21
2. הליך אישור העברת המידע האישי 23
3. שלב מימוש העברת המידע האישי 30
4. הנחיות אבטחת המידע והגנת סייבר בהעברת מידע בין גופים ציבוריים 33
5. מדיניות כלכלית ותקציבית בהעברת מידע בגופים ציבוריים 35
6. היבטים רוחביים 38
פרק ה: נושאים מוצעים להמשך בחינה 42
פרק ו: סיכום המלצות הצוות 46
נספח א': מדדים ליישום ההמלצות ולהצלחתן 50
נספח ב': הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים 56

<u>פתח דבר</u>

בעידן שבו המידע הפך למשאב אסטרטגי מרכזי, ובתוך מהפכת הדיגיטציה הממשיכה לשנות את פני החברה, נדרשת חשיבה מחודשת על דרכי שיתוף המידע בין גופים ציבוריים. גישה חכמה למידע יכולה לאפשר למשרדי הממשלה ולגופים ציבוריים לא רק לייעל את תהליכי העבודה ולשפר את השירותים הניתנים לציבור, אלא גם להתמודד עם אתגרי השעה באופן יעיל ומדויק יותר. עם זאת, שיתוף מידע חייב להתבצע תוך שמירה על האיזון הנכון מול הזכות לפרטיות, שהיא זכות יסוד המעוגנת בחוקי היסוד של מדינת ישראל.

הצוות הבין משרדי לבחינה של ההסדר הראוי להעברת מידע אישי בין גופים ציבוריים הוקם במטרה לבחון לעומק את המצב הקיים בתחום העברת המידע בין גופים ציבוריים בישראל. עבודת הצוות נשענה על תהליך ניתוח מקיף, שכלל בחינה השוואתית של מודלים ממדינות מובילות בעולם, ניתוח של תהליכים קיימים בישראל וזיהוי הקשיים והפערים המונעים העברת מידע יעילה. ניתוח המצב העלה כי אין חסם עקרוני המונע העברת מידע, אולם הליכי העברת המידע כיום הם מסורבלים, בירוקרטיים וממושכים. בממוצע, נדרשים מאות ימים לאישור העברת מידע, ועקב כך, הליכים רבים ננטשים. הנטל הכרוך בהליכי אישור העברת המידע הוא רוחבי, והם אינם ממוקדים במקרים בהם צפויה פגיעה משמעותית בפרטיות. מצב זה פוגע הן ביכולת של הגופים הציבוריים לפעול ביעילות והן בזמינות השירותים לציבור. הממצאים שהוצגו בדו"ח מדגישים את הצורך בתשתיות דיגיטליות רוחביות, בתהליכי עבודה מהירים וגמישים יותר, בהגדרת מסלולים משפטיים מבוססים על ניהול סיכונים שיפשטו את תהליכי קבלת ההחלטות, בהגדרת מנגנונים ברורים לשמירה על המידע ואבטחתו ובקשב ניהולי לתהליך העברת המידע.

הדו"ח מדגיש תועלות רבות הנובעות מייעול שיתוף המידע בין גופים ציבוריים. ראשית, תשתיות דיגיטליות ישפרו את היעילות המערכתית, יאפשרו קבלת החלטות מבוססות נתונים בזמן אמת, ויתמודדו עם משברים בצורה מהירה וממוקדת. שנית, מנגנוני שיתוף מידע יפחיתו כפילויות בתהליכים ויחסכו משאבים יקרים, הן מבחינת כוח אדם והן מבחינת עלויות תפעול. כך, לדוגמה, משרדים לא יצטרכו לאסוף שוב ושוב את אותם נתונים, אלא יוכלו להסתמך על מידע קיים ומאומת. יתרה מכך, הפחתת הבירוקרטיה והנגשת שירותים דיגיטליים תאפשר לאזרחים לקבל מענה מהיר ואפקטיבי יותר, תוך חיסכון בזמן ובמאמץ מצידם.

יותר מכל, אנו רואים בדו"ח זה הזדמנות להוביל שינוי תפיסתי, המעמיד את האזרח במרכז. המידע שייך בראש ובראשונה לציבור. שיפור תהליכי קבלת ההחלטות ושיפור השירות לאזרח יגבירו באופן מיידי את התועלת לציבור, כאשר השימוש בו חייב להיעשות תוך אחריות, רגישות וכבוד לפרטיות. בכך אנו מאמינים שמהלכים אלה לא רק יתרמו לייעול המערכת הציבורית ולאזרח הבודד, אלא גם יחזקו את אמון הציבור בגופים הפועלים לטובתו.

אני רוצה להודות לכל אחד מחברי הצוות על שהיו שותפים מלאים לדרך ולעבודה המקצועית-

משרד ראש הממשלה: עדו קמחי פלדהורן, אליענה זלר ושירי נוימן

משרד האוצר: גל אסף וגד רחמני

הרשות להגנת הפרטיות: נעמה גורני (שסיימה את תפקידה ברשות במהלך עבודת הצוות) ורינת ברנדל

מערך הסייבר הלאומי: קרן גלאון ושרית ארונוב

מערך הדיגיטל הלאומי: יערה בן שחר, רותם ארנרייך וגל תמיר

לחברי צוות המשנה שגיבשו את המסמך בדבר הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים - אליאב נורי (מערך הסייבר הלאומי), לינא כמאל טרודי (הרשות להגנת הפרטיות), ניר בן יוסף וסער בן יהודה (מערך הדיגיטל).

לאנשים נוספים ממערך הדיגיטל שהיו שותפים לדיונים ולתהליך: מירב פרץ בילינסקי, אשר דולב, נעמה שחל, גיל שטיינהרט, טל רוזנפלד, רותם קלמר סיני, אפרת ברגמן ספיר, ליליה שוורצמן וטלי אבירם.

אני רוצה להודות גם לנציגים מטעם הגופים הציבוריים השונים (בשלטון המרכזי והמקומי) שהופיעו בפני הצוות, העבירו התייחסויות, ותרמו תרומה משמעותית לגיבוש ההמלצות.

תודה מיוחדת **לעו״ד עמית יוסוב עמיר** מהאשכול שלי, על תרומתו החשובה והחיונית לדו״ח בחשיבה מקורית ויצירתית, בהשקעה של זמן ומחשבה ועל חלקו המשמעותי בהובלה נכונה וחכמה של עבודת הצוות.

דו״ח זה מתפרסם כטיוטה לצורך קבלת הערות הציבור. הצוות מזמין כל גורם המעוניין בכך להגיש התייחסויות ולשתף מידע או תובנות רלוונטיות בנושא.

לירון מאוטנר לוגסי, עו״ד

ראש אשכול פרטיות ומידע

ייעוץ וחקיקה (ציבורי חוקתי), משרד המשפטים

תקציר מנהלים:

במסגרת [החלטת ממשלה מס׳ 213](#) מיום 24.02.2023 בנושא האצת הדיגיטציה במגזר הציבורי וצמצום בירוקרטיה בשירותים ציבוריים, הוחלט על הקמת צוות בין-משרדי לבחינה של ההסדר הראוי להעברת מידע בין גופים ציבוריים לפי פרק ד׳ לחוק הגנת הפרטיות, התשמ״א – 1981 (להלן – חוק הגנת הפרטיות). הצוות הוקם במטרה להמליץ על הסדר בתחום העברת מידע אישי בין גופים ציבוריים, שישקף איזון ראוי בין הזכות לפרטיות לבין היכולת של גופים ציבוריים לפעול ביעילות ולהעניק שירות טוב יותר לציבור. ביסוד עבודת הצוות עמדה התפישה לפיה בעידן הדיגיטלי הנוכחי העברת מידע אישי בין גופי הממשלה והמגזר הציבורי בכללותו היא כלי חיוני לייעול עבודת הגופים הציבוריים והשירות שהם מעניקים לציבור. התשתית העובדתית שעמדה בפני הצוות הצביעה על קשיים משמעותיים ביישום ההליכים הנדרשים להעברת מידע אישי כיום בין גופים ציבוריים. כך, נדרשים בממוצע מאות ימים לאישור העברת המידע, והליכים רבים לא מושלמים לאור התמשכותם. לצד זאת הצורך בהעברת מידע אישי הולך וגובר, ועימו גם הסיכון לפגיעה בזכות לפרטיות והפגיעה בה בפועל.

הצוות מצא כי אין חסם משפטי, או אחר, המונע באופן עקרוני העברת מידע אישי בין גופים ציבוריים. בפרט, הסמכות החוקית בישראל להעברת מידע אישי בין גופים ציבוריים רחבה יותר מאשר במדינות אירופאיות הידועות ברמת דיגיטציה גבוהה של המנהל הציבורי שלהן, לגביהן נערכה השוואה. לצד זאת, ישנם קשיים משמעותיים בשלושה היבטים מרכזיים, הפוגעים מאוד ביעילות התהליך הנדרש להעברת המידע האישי – קשיים בשלב איתור המידע המבוקש; קשיים בהליך האישור להעברת המידע וקשיים במימוש העברת המידע לאחר שניתן אישור להעברתו. נוסף על כך נמצאו קשיים רוחביים המשפיעים על הליך העברות המידע באופן כללי, וכן קושי בהיבטים כלכליים ותקציביים של העברות המידע.

הצוות ממליץ על סל של פתרונות – משפטיים, טכנולוגיים, ניהוליים, ארגוניים ותקציביים, ששילוב שלהם יוכל לתת מענה למרבית הקשיים שנמצאו.

לגבי שלב איתור המידע האישי והכנת הבקשות להעברת מידע, ממליץ הצוות על פיתוח והנגשה של קטלוג של סוגי המידע המצויים במאגרים מרכזיים של גופים ציבוריים, שהמידע בהם נדרש בהיקף ובתדירות גבוהים מגופים ציבוריים רבים. כמו כן מוצע להשלים את פיתוחה של מערכת דיגיטלית חדשה שתסייע בהכנת הבקשות להעברת מידע אישי ובטיפול בהן.

בהיבט הליך אישור העברת המידע האישי, מומלץ לקבוע כמה מסלולים חלופיים לאופן בו ניתן לאשר את העברת המידע, במקום מסלול יחיד של ועדות להעברת מידע הקיים כיום. חלופות אלה יקבעו במודל של ניהול סיכונים, לפי רגישות והיקף המידע המועבר, ושכיחות הצורך בסוגי מידע מסוימים בקרב גופים ציבוריים רבים. כן תוקם ועדה מרכזית, שתוסמך להתיר העברת מידע אישי בין יותר משני גופים ציבוריים ובכלל זה תוסמך להתיר להעביר מידע הנדרש לטובת טיפול בסוגיות לאומיות - רוחביות. שינויים אלה יחייבו תיקון של תקנות הגנת הפרטיות.

כמו כן, מוצע לפתח מערכות דיגיטליות מרכזיות שיסיעו להפחית את הסיכון הנובע מהעברת המידע האישי, בין היתר על ידי התממה חלקית או מלאה שלו, דבר שיאפשר להעבירו במסלולי אישור מקלים יותר. בנוסף, מוצע

לקבוע הנחיות אחידות בהיבטי אבטחת מידע והגנת סייבר בהעברת מידע בין גופים ציבוריים, שתייתר את הצורך בהסדרת הנושא לפני כל אישור של העברת המידע, ותקל גם על מימוש ההעברה.

לגבי שלב מימוש העברות המידע האישי, מוצע לתמרץ ולסייע בפיתוח ממשקים למערכות רוחביות להעברת המידע, כך שהעברת המידע לא תצריך פיתוח ייחודי הכרוך בהקצאת זמן ומשאבים. לצורך כך יוקצה צוות פיתוח ייעודי מטעם מערך הדיגיטל הלאומי ויקודמו ממשקים למאגרי מידע שלמידע בהם קיים ביקוש גבוה במיוחד מצד גופים ציבוריים אחרים.

עוד מוצע, ביחס לכלל שלבי העברת המידע האישי, על מספר צעדים רוחביים, ובהם: מינוי אחראי על תחום העברות המידע בכל גוף ציבורי (POC), חידוש עבודת ועדת היגוי שתפעל בנושא ופעולות לתיעדוף סוגית העברות המידע ברמה הארגונית והממשלתית. מבחינה כלכלית-תקציבית, מוצע לתקצב פיתוח וחיבור למערכות מרכזיות שייעלו את העברת המידע, ולקבוע כללים אחדים בדבר האפשרות לגבות תשלום עבור העברת מידע, שישקפו את עלות ההעברה בפועל וימנעו גבית תשלום בנסיבות בהן עלויות העברת המידע נמוכות.

בעקבות התקדמות עבודת הצוות, חלק מההמלצות בתחומים הטכנולוגיים והארגוניים כבר הוטמעו במסגרת הליכי הכנת תקציב המדינה בהחלטת ממשלה.[1]

טיוטת הדו״ח מתפרסמת להערות הציבור. את ההתייחסויות יש להעביר לידי עו״ד עמית יוסוב עמיר בדוא״ל amitam@justice.gov.il. התייחסויות תתקבלנה עד ליום 18 בפברואר 2025.

[1] החלטת ממשלה מס׳ 2273 מיום 831.10.2024 בנושא ״ייעול המגזר הציבורי: האצת שירות הדיגיטל לאזרח ויצירת תשתיות דיגיטליות וכלי מדיניות תומכים ותיקון החלטות ממשלה״.

פרק א: רקע לעבודת הצוות

1. ההליכים שקדמו לעבודת הצוות:

בהחלטת ממשלה מס' 213 מיום 24.02.2023, בנושא האצת הדיגיטציה במגזר הציבורי וצמצום בירוקרטיה בשירותים ציבוריים, הוחלט על הקמת צוות בין-משרדי לבחינה של ההסדר הראוי להעברת מידע אישי בין גופים ציבוריים לפי פרק ד' לחוק הגנת הפרטיות, התשמ"א – 1981 (להלן – חוק הגנת הפרטיות). תכלית הקמת הצוות היא להסיר חסמים, לשפר את תחום העברות המידע האישי ולוודא כי מתקיים איזון ראוי בין הזכות לפרטיות לבין היכולת של גופים ציבוריים לפעול ביעילות ולהעניק שירות טוב יותר לציבור, וכי ההסדר להעברת המידע האישי משרת בצורה מיטבית איזון זה. בראש הצוות עמדה עו"ד לירון מאוטנר לוגסי, ראש אשכול פרטיות ומידע בייעוץ וחקיקה, וחברים בו נציגי מערך הדיגיטל הלאומי, אגף התקציבים במשרד האוצר, אגף ממשל וחברה במשרד ראש הממשלה, הרשות להגנת הפרטיות ומערך הסייבר הלאומי.

הצורך בהעברת מידע אישי כחלק אינטגרלי מפעילות המנהל הציבורי הלך וגבר בשנים האחרונות עם התקדמות מהפכת המידע ותהליכי הדיגיטציה, בדגש על תהליכי תכנון מדיניות, מתן שירותים לציבור וניהול ותפעול שוטפים. רבים מהשירותים ותחומי המדיניות בהם עוסקים משרדי הממשלה וגופים ציבוריים אחרים מערבים מספר משרדי ממשלה וגופים ציבוריים אחרים. כמו כן, שיתוף נתונים בין משרדי הממשלה ויתר הגופים הציבוריים הוא תנאי הכרחי למימוש פתרונות "One Stop Shop" לשירותים ממשלתיים[2] ולהפעלת מנגנונים של "Ask once" (להלן: מדיניות "שאל פעם אחת").[3] העברת מידע אישי נדרשת גם לטובת מיצוי זכויות באופן יזום. בעת מיצוי זכויות ביוזמת הגוף המעניק את הזכות, הדרישה לספק מידע ולהשלים מסמכים סותרת את תאוריית הדחיפות (באנגלית – Nudge Theory) בכלכלה התנהגותית, הווה אומר, עצם הסרבול הבירוקרטי מקשה על מיצוי הזכויות ומונע את התכליות המבוקשות על ידי צעד המדיניות הציבורית.

לצד הצורך להעביר מידע אישי בין גופים ציבוריים, הולכת וגדלה הפגיעה בפרטיותם של אזרחי ותושבי המדינה כתוצאה מהעברת המידע האישי. העברת מידע אישי בין גופים ציבוריים רבים, לתכליות שונות מאלה לשמן נאסף, ולעיתים קרובות תוך שמירתו במאגרי מידע נוספים על מאגר המידע ממנו נמסר, פוגעים כשלעצמם בפרטיות, ומגבירים בנוסף את הסיכונים הכרוכים בשמירת והעברת המידע, ובכלל זה החשש לשימוש לא מורשה במידע או לדליפתו.

הצורך בהעברת יותר ויותר מידע אישי, לתכליות חשובות וראויות, ולצידו הפגיעה בפרטיות הנגרמת מהעברת המידע, מחייבות טיוב ועדכון של תהליכי העברת מידע אישי והגדרת דרכי השימוש במידע המועבר, הן בין משרדי ממשלה שונים והן בין משרדי הממשלה לגופים ציבוריים נוספים. נדרש שיפור של היכולת של הממשלה לשתף נתונים בזמן אמת, באופן שוטף, רציף ובטוח, עבור ריבוי צרכנים ושימושים, בתדירות משתנה ותוך גמישות לשינויים, והכל תוך נקיטת אמצעים מתאימים שיבטיחו שהפגיעה בפרטיות נעשית כדין ובמידה שאינה עולה על הנדרש.

---

[2] מודל ארגוני לפיו מרכזים את כלל השירותים לציבור במקום אחד במטרה לספק לצרכן כניסה אחת לתוך מערכת המספקת מגוון רחב של שירותים, תוך שימת דגש על נקודת מבטו.

[3] מדיניות קבלת מידע מהציבור פעם אחת בלבד לשם שיפור השירות הממשלתי לציבור והפחתת הנטל הבירוקרטי עליו באמצעות שיתוף מידע בין גופים ציבוריים, אשר אומצה בהחלטת ממשלה מס' 1933 עליה יפורט בהמשך.

התהליכים להעברת מידע אישי הקיימים כיום זוהו כאתגר מרכזי כבר בשלבים המוקדמים של קידום הדיגיטציה בממשלה, כאשר העברת נתוני אזרחים ותושבים נדרשה לצורך שיפור השירותים הדיגיטליים ונתקלה בקשיי מימוש, בין היתר לאור הבירוקרטיה הכרוכה בכך. לאור זאת, בהחלטת ממשלה מס׳ 2097 מיום 10.10.2014 בדבר ״הרחבת תחומי פעילות התקשוב הממשלתי, עידוד חדשנות במגזר הציבורי וקידום המיזם הלאומי ״ישראל דיגיטלית״״ הוחלט על הקמת צוות בין-משרדי ייעודי לבחינת שיפור העברת מידע בין משרדי הממשלה. על הצוות הוטל לגבש המלצות בתחומים הבאים: סטנדרטים ונהלים לפעולת הוועדות להעברת מידע; הגדרת דרישות למערכת מידע רוחבית לניהול עבודת ועדות העברת המידע; ומדיניות לטווח הבינוני והרחוק בדבר קבלת מידע מאזרחים פעם אחת בלבד. בשנת 2016, גיבש הצוות שורת המלצות לשיפור התהליך, אשר התמקדו בחיזוק היבטי הניהול והבקרה ותיקונים פרטניים בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ״ו-1986 (״תקנות הגנת הפרטיות״ או ״התקנות״). לצד זאת, הצוות לא המליץ על עריכת שינוי מהותי בהסדר המשפטי הקבוע בתקנות. בכלל זה, הדרישה לאישור העברת מידע אישי בידי ועדות לעניין זה בגוף מוסר המידע ובגוף מקבל המידע, נותרה ללא שינוי מהותי.

עיקרי המלצות הצוות אומצו בהחלטת ממשלה מס׳ 1933 מיום 30.8.2016 בדבר ״שיפור העברת המידע הממשלתי והנגשת מאגרי מידע ממשלתיים לציבור״ (להלן: החלטת ממשלה מס׳ 1933). החלטת הממשלה אימצה את מדיניות ׳שאל פעם אחת׳ (Ask once) להעברת מידע לטובת שיפור השירות, וקבעה שורת החלטות שנועדו לשפר את תהליך העברת המידע, לרבות: יעדים ממשלתיים למימוש מדיניות ׳שאל פעם אחת׳; מיפוי המידע והאישורים הנדרשים לקבלת שירותים ממשלתיים; הקמת תשתית טכנולוגית מאובטחת לשיתוף מידע (״שדרת המידע הממשלתית״); והקמת מערכת מחשוב רוחבית לניהול עבודת הוועדות להעברת מידע (מערכת "מועד"). בנוסף, הסמיכה החלטת הממשלה את רשות התקשוב הממשלתי (כיום מערך הדיגיטל הלאומי) לפקח מנהלית על עבודת הוועדות להעברת מידע, ואימצה את נוהל עבודת הוועדות שהוצע על ידי הצוות הבין-משרדי. לבסוף, החלטת הממשלה קבעה כי יש לקדם תיקון לתקנות הגנת הפרטיות עליו המליץ הצוות, בהיבטים הנוגעים לאבטחת מידע, הסדרת נוהל עבודת הוועדות ועדכון נוסח הטפסים לאישור העברת המידע. טיוטה לתיקון התקנות שהוכנה בהתאם להחלטת הממשלה הונחה על שולחן ועדת החוקה, חוק ומשפט של הכנסת ה – 24 אך לא נדונה ולא אושרה על ידה. בהחלטת ממשלה מס׳ 213 הושהתה ההחלטה לקדם את התיקון לתקנות, מאחר שהוחלט, כאמור, לבחון מחדש את הסדר העברת המידע בכללותו. בהחלטת ממשלה מס׳ 260 מיום 26.7.2020 בדבר ״תכנית להאצת השירותים הדיגיטליים לציבור ולקידום הלמידה הדיגיטלית ותיקון החלטת ממשלה״ (להלן: ״החלטת ממשלה מס׳ 260״) הוחלט על פיתוח תשתיות דיגיטליות נוספות למימוש מדיניות ׳שאל פעם אחת׳, ובכלל זה החצנה של תחומי מידע מרכזיים בשדרת המידע הממשלתית, במטרה להקל על הנטל הרגולטורי לאזרח ולשפר את השירותים הציבוריים הניתנים לו.[4]

[4] לצד צעדים אלו, הממשלה קידמה תהליכים שיהוו כלים משלימים להליך העברות המידע בין גופים ציבוריים. בהחלטת ממשלה מס׳ 1440 בדבר ׳הקמת ״אגם מידע ממשלתי״ בלשכה המרכזית לסטטיסטיקה׳ מיום 15.5.2022 אומצו המלצות הצוות הבין-משרדי שהוקם בעקבות החלטת ממשלה מס׳ 4753 מיום 24.11.2019 בדבר ׳הגברת השימוש במידע ממשלתי לצורך שיפור המדיניות הממשלתית והגברת האפקטיביות של פעולות הממשלה׳. הצוות המליץ להקים אגם מידע ממשלתי בלמ״ס במטרה להגביר את יכולות משרדי הממשלה לקדם מדיניות מבוססת נתונים לצורך שיפור המדיניות הממשלתית, להגביר את האפקטיביות של פעולות הממשלה ולסייע בייעול תהליכי העבודה של המערכת הסטטיסטית במוסדות המדינה.

בשנים שחלפו מאז התקבלה החלטת ממשלה מס׳ 1933 נעשו פעולות רבות כדי לקדם את יישומה. הוקמה ועדת היגוי לשיפור העברות מידע בין משרדי ממשלה אשר התכנסה בין השנים 2017-2021, הופצו נהלי עבודה לוועדות להעברת מידע ומונו ממוני העברות מידע במשרדי הממשלה וביחידות הסמך. נוסף על כך, נערכה הדרכה משותפת על ידי רשות התקשוב הממשלתי וייעוץ וחקיקה במשרד המשפטים לכלל משרדי הממשלה בנושא העברת מידע אישי בין גופים ציבוריים. כמו וכן, נעשו פעולות כדי לטייב את תהליכי אישור העברת המידע, בהיותם חסם למימוש המדיניות. רשות התקשוב החלה באיסוף מידע ובקרה על עבודת הוועדות המשרדיות להעברת מידע אישי, וכן הקימה והטמיעה את מערכת "מועד" לניהול תהליכי אישור בקשות להעברת מידע. הידע המקצועי שנצבר בתקופה זו ונתוני עבודת הוועדות מצביעים על כך כי חרף המאמצים הרבים שנעשו, הקושי בהליכי העברת מידע אישי עדיין מהווה אתגר משמעותי לשיתוף נתונים בכלל ערוצי הפעילות הממשלתיים בפרט, והציבוריים בכלל, וכי יש צורך בשינוי עומק של המנגנון הקיים. בפועל, על אף שבהחלטת ממשלה 1933 הוחלט כי החל משנת 2023 משרדי הממשלה לא יבקשו מאדם או מתאגיד מידע הקיים בידי משרד ממשלתי אחר, במרבית הטפסים הממשלתיים האזרח נדרש פעמים רבות להיות ה"מתווך" בין משרדי הממשלה השונים ולעדכנם ואף לספק מסמכים המוכחים נתונים בסיסיים לגביו.

סוגית העברת המידע האישי, למרות שיכולה להשתמע כאתגר טכנולוגי או משפטי בלבד, טומנת בחובה שילוב של מספר היבטים ותהליכים, ומתייחסת לתשתיות שונות: תשתית חוקית, תשתית טכנולוגית, היבטי אבטחת מידע והגנת סייבר, היבטים מקצועיים, היבטים ניהוליים וארגוניים והיבטים כלכליים ותקציביים. דו"ח זה נכתב במטרה לייצר מסגרת של פתרונות ושילובם זה בזה, כך שיוכלו לתת מענה מקיף למגוון האתגרים המאפיין את התהליכים המורכבים הנדרשים לצורך העברת מידע אישי.

כחלק מעבודת הצוות וכבסיס לגיבוש ההמלצות, ביצע הצוות תהליך למידה אשר בחן את כלל היבטי העברות המידע, ובכלל זה היבטים משפטיים, טכנולוגיים, ארגוניים, ניהוליים ותקציביים. תהליך הלמידה כלל מספר מהלכים עיקריים: ניתוח נתוני אישורי העברות מידע שעובדו במערכת מועד; שיחות תיקוף עם גורמי מקצוע מגופים ציבוריים שונים על מנת להבין את תמונת המצב תחת ההסדר הנוכחי,[5] ביצוע סקירה בין לאומית שתכליתה למפות את האתגרים והפתרונות המיושמים במספר מדינות מובילות, ולבסוף שיחות התייעצויות עם פורומים שונים על ההסדר המתגבש על -ידי הצוות הבין משרדי.[6]

לקראת סיום עבודת הצוות, הוטמעו חלק מהמלצותיו המתגבשות בהיבטים טכנולוגיים וארגוניים [בהחלטת ממשלה מס׳ 2273] מיום 31.10.2024 בנושא: "ייעול המגזר הציבורי: האצת שירות הדיגיטל לאזרח ויצירת תשתיות דיגיטליות וכלי מדיניות תומכים ותיקון החלטות ממשלה".

[5] השיחות התקיימו, בין היתר, עם רשות האוכלוסין וההגירה, משרד הרווחה, משרד הבינוי והשיכון, משרד המשפטים, המוסד לביטוח לאומי, נציגות של מרכז השלטון המקומי ורשויות מקומיות שונות והלשכה המרכזית לסטטיסטיקה.
[6] השיחות על ההסדר המתגבש התקיימו, בין היתר, עם פורום של השלטון המקומי ופורומים של מנהלי מערכות מידע (מנמ"רים), יועצים משפטיים וסמנכ"לים מקרב משרדי הממשלה.

2. התשתית הנורמטיבית להעברת מידע אישי בין גופים ציבוריים:

העברת מידע אישי בין גופים ציבוריים מוסדרת בפרק ד' לחוק הגנת הפרטיות.[7] ככלל, גופים ציבוריים רשאים להעביר ביניהם מידע אישי כשהדבר נדרש לטובת ביצוע חיקוק (חוק או תקנה) או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו, ואם מסירת המידע האישי היא לגוף ציבורי שאיננו משרד ממשלתי או "מוסד מדינה אחר", היא מותנית גם בכך שמסירת המידע האישי כשלעצמה היא במסגרת הסמכויות או התפקידים של הגוף המוסר, או שהגוף הציבורי מקבל המידע "רשאי לדרוש אותו מידע על פי דין מכל מקור אחר". זאת, למעט במקרים בהם מסירת המידע נאסרה באופן פרטני בחיקוק מסוים או בכללים של אתיקה מקצועית, או כאשר מדובר במידע שהתקבל בתנאי שלא יימסר לאחר.

העברת מידע אישי בין גופים ציבוריים מהווה חריג לכלל האוסר על מסירת מידע אישי מגוף ציבורי, הקבוע בסעיף 23ב(א) לחוק. גוף ציבורי מוגדר לעניין זה כמשרדי הממשלה, מוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקידים ציבוריים על פי דין,[8] וכן גוף אחר ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת.[9] הוראות הפרק חלות רק על מידע אודות אדם "טבעי", ואינן חלות על מידע אודות תאגידים (ככל שאינו מתייחס לאדם כאמור).[10]

להלן יובאו הוראות הסעיפים הרלוונטיים:[11]

"23ב. (א) מסירת מידע מאת גוף ציבורי אסורה, זולת אם המידע פורסם לרבים על פי סמכות כדין, או הועמד לעיון הרבים על פי סמכות כדין, או שהאדם אשר המידע מתייחס אליו נתן הסכמתו למסירה. (ב) אין בהוראות סעיף זה כדי למנוע מרשות בטחון כמשמעותה בסעיף 19 לקבל או למסור מידע לשם מילוי תפקידה, ובלבד שהמסירה או הקבלה לא נאסרה בחיקוק.

23ג.מסירת המידע מותרת, על אף האמור בסעיף 23ב, אם לא נאסרה בחיקוק או בעקרונות של אתיקה מקצועית-

1. בין גופים ציבוריים, אם נתקיים אחד מאלה:

(א) מסירת המידע היא במסגרת הסמכויות או התפקידים של מוסר המידע והיא דרושה למטרת ביצוע חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו;

[7] נכון למועד הגשת הדו"ח, חלות הוראות פרק ד' על "מידע", כהגדרתו בסעיף 7 לחוק, וכן על ידיעות על ענייניו הפרטיים של אדם, אף שאינן בגדר מידע (ס' 23א). עם כניסתו לתוקף של תיקון מס' 13 לחוק הגנת הפרטיות, ב - 14.8.2025, יחול ההסדר על "מידע אישי" כהגדרתו בסעיף 3 לחוק לאחר התיקון, הגדרה הקובעת כי מידע אישי הוא כל "נתון הנוגע לאדם מזוהה או ניתן לזיהוי...". השימוש ב"מידע" ו – "מידע אישי" נעשה לאורך הדו"ח לחליפין, אלא אם כן מצוין במפורש אחרת.

[8] לפרשנות המונח "גוף אחר הממלא תפקידים ציבוריים על פי דין" ר' ע"א 8825/03 **שירותי בריאות כללית נ' משרד הבטחון** (11.04.07).

[9] ר' צו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו-1986. בצו נקבעו שורה של גופים פרטיים הממלאים תפקיד ציבורי מסוים ("גופים דו מהותיים"), כגון מוסדות אקדמיים, ארגוני בריאות וארגונים יציגים כגופים ציבוריים לעניין קבלת מידע אישי מסוים, המפורט בצו, מגופים ציבוריים אחרים. הצו מתוקן על ידי שר המשפטים באישור ועדת החוקה מעת לעת כאשר עולה צורך ציבורי העומד במבחני המידתיות בהעברת מידע לגוף דו מהותי כאמור.

[10] ר' הגדרת "אדם" בסעיף 3 לחוק הגנת הפרטיות.

[11] סעיף 23ב(ב) קובע הסדר מיוחד הנוגע לרשויות ביטחון כהגדרתן בסעיף 19(ג), נושא שאינו בתחום טיפולו של הצוות, ובהתאם האמור בדו"ח זה אינו נוגע אליו.

(ב) מסירת המידע היא לגוף ציבורי הרשאי לדרוש אותו מידע על פי דין מכל מקור אחר;

2. מגוף ציבורי למשרד ממשלתי או למוסד מדינה אחר, או בין משרדים או מוסדות כאמור, אם מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו;

אולם לא יימסר מידע כאמור שניתן בתנאי שלא יימסר לאחר."

הסמכות להעברת מידע אישי בין גופים ציבוריים מהווה חריג לעקרון צמידות המטרה.[12] בהתקיים התנאים המפורטים בסעיף 23ג, מאפשר חוק הגנת הפרטיות לגוף ציבורי להעביר מידע אישי לצורך שימוש בו בידי גוף ציבורי אחר שלא למטרה לשמה התקבל או נוצר. מלשון הסעיף, מההיסטוריה החקיקתית שלו ומהאופן בו פורש בפסיקה, עולה כי לא דרוש מקור סמכות חיצוני לחוק לשם העברת המידע, וגופים ציבוריים מוסמכים להעביר ולקבל מידע אישי בעת התקיימות הנסיבות המפורטות בסעיפים 23ב ו – 23ג לחוק.[13] לצד זאת, הסמכות הרחבה להעברת מידע אישי בין גופים ציבוריים מהווה פגיעה בזכות החוקתית לפרטיות, המעוגנת בסעיף 7 לחוק יסוד: כבוד האדם וחירותו. בהתאם, על כל העברת מידע אישי לעמוד בתנאי פסקת ההגבלה לפי חוק היסוד, ובפרט לעמוד במבחני המידתיות שנקבעו בפסיקה.[14] דווקא בשל רוחב הסמכות להעברת מידע אישי בין גופים ציבוריים, והדרישה ההולכת וגוברת למידע לשלל פעולות חשובות וראויות של רשויות השלטון השונות, נדרש לוודא כי הסמכות מופעלת בזהירות הנדרשת, ולא גורמת לפגיעה בפרטיות במידה העולה על הנדרש.

למעט חריגים מסוימים, על העברת מידע אישי בין גופים ציבוריים להיות שקופה ופומבית. כך, סעיף 23ד קובע, בין היתר, חובה על גוף ציבורי המוסר מידע אישי דרך קבע לפרט עובדה זו על כל דרישת מידע בהתאם לחוק,[15] וחובה על גוף ציבורי המקבל דרך קבע מידע אישי שנאגר במאגר מידע להודיע על כך לרשות להגנת הפרטיות שתכלול עובדה זו במרשם מאגרי המידע הפתוח לעיון הציבור.[16]

לשלמות התמונה יצוין כי לצד ההסדר הכללי בדבר העברת מידע אישי בין גופים ציבוריים בפרק ד' לחוק הגנת הפרטיות, קיימות הוראות חוק פרטניות רבות המסדירות העברת מידע אישי בין גופים ציבוריים בנסיבות מסוימות הקבועות בהן.[17]

---

[12] עקרון יסוד בדיני הגנת הפרטיות, בארץ ובעולם, לפיו מידע ישמש רק לתכלית לשמה נאסף או נמסר. ר' סעיפים 2(9) ו – 8(ב) לחוק הגנת הפרטיות; סעיף 5(1)(b) לתקנות הגנת המידע האישי של האיחוד האירופי (GDPR); OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, סעיף 9.

[13] ר' בבג"ץ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים ואח'**, סעיף 6 לפסק דינה של כב' השופטת (בדימוס) דורנר (בג"ץ מרשם האוכלוסין); ע"פ 3050/13 **פלוני נ' מד"י**, סעיף 4 לפסק דינה של כב' השופטת ברק – ארז; בר"ש 1190/18 **ועדת האתיקה המחוזית של לשכת עורכי הדין נ' דוד ידיד**, סעיף 18 לפסק דינו של כב' השופט מזוז. כן ר' דבריו של ח. קלוגמן, נציג משרד המשפטים, בדיון בועדת החוקה חוק ומשפט מיום 17.12.84 לגבי תיקון מס' 1 לחוק הגנת הפרטיות בו נקבע פרק ד' בנוסחו כיום: "העיקרון שביסוד ההצעה הוא שבין גופים ציבוריים חייבת להיות זרימה של מידע, אם כי הזרימה הזו חייבת להיות מבוקרת".

[14] ר' בג"ץ מרשם האוכלוסין.

[15] חובת היידוע בכל פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע מוסדרת בסעיף 11 לחוק.

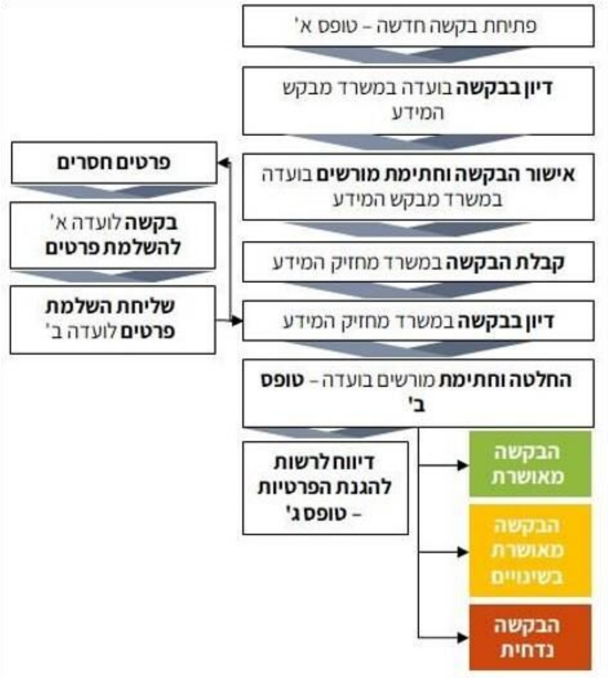
[16] עד לכניסתו לתוקף של תיקון מס' 13 לחוק הגנת הפרטיות, המונחים המופיעים בחוק, חלף המצוין לעיל, הם רשם מאגרי המידע ופנקס מאגרי המידע.

[17] ר' לדוגמא, מבין רבים: סעיף 15א לפקודת הסטטיסטיקה; סעיף 384 לחוק הביטוח הלאומי, התשנ"ה - 1995; סעיף 9ד לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998; סעיף 83 לפקודת התעבורה [נוסח חדש].

3. ההליך לאישור העברת המידע האישי:

ההליך לאישור העברת מידע אישי לפי פרק ד' לחוק הגנת הפרטיות מוסדר בתקנות הגנת הפרטיות. תקנות אלה תוקנו בעקבות פסיקת בית המשפט העליון בבג"ץ 8070/98 האגודה לזכויות האזרח נ' משרד הפנים ואח' (להלן: **בג"ץ מרשם האוכלוסין**). בעניין זה נקבע, בין היתר, כי המצב שקדם לפסק הדין, בו נעשו מאמצים להבטיח כי מידע אישי המועבר בין גופים ציבוריים יגיע רק לעובדי הציבור הזקוקים לו, אך לא היו תקנות או הנחיות מנהל בנושא, אינו עומד במבחני המידתיות, וכי יש הכרח לקבוע הוראות שימזערו את הפגיעה בפרטיות הנובעת מהעברת המידע.[18] ההליך המפורט בתקנות קובע כי בכל משרד תוקם ועדה משרדית להעברות מידע אישי שתורכב לכל הפחות משלושה חברים בראשם מנכ"ל המשרד או נציג בכיר מטעמו, היועץ המשפטי של המשרד או נציגו ועובד שתחום עיסוקו הוא בניהול המידע ואבטחתו. כל בקשה להעברת מידע אישי בין גופים ציבוריים מוגשת על גבי טופס "בקשה לקבלת מידע מאת גוף ציבורי" הקבוע בתוספת לתקנות (טופס א') חתום על ידי מספר גורמים (מנהל המאגר, הממונה על אבטחת המאגר והיועץ המשפטי של הגוף המבקש) לוועדה המשרדית להעברת מידע בגוף שברשותו המידע, וזאת לאחר שאושרה על ידי הוועדה המשרדית להעברת מידע בגוף מבקש המידע. הוועדה בגוף שברשותו המידע דנה בבקשה, רשאית לבקש פרטים נוספים אם נדרשים, ומקבלת החלטה בהתאם לאחת מהחלופות האפשריות: אישור הבקשה, אישור הבקשה בשינויים או דחייתה. החלטת הוועדה בגוף שברשותו המידע האישי נשלחת לגוף מבקש המידע על גבי טופס "הסכמת גוף ציבורי למסירת מידע" הקבוע גם הוא בתוספת לתקנות (טופס ב') חתום על ידי מנהל המאגר, הממונה על אבטחת המאגר והיועץ המשפטי של הגוף שברשותו המידע. כמו כן, במקרה והבקשה אושרה כך שמתקבל מידע אישי דרך קבע, נשלח דיווח לרשות להגנת הפרטיות על גבי הטופס הקבוע בתקנות ל- "הודעה על קבלת מידע דרך קבע" (טופס ג').

להלן תיאור גרפי של התהליך:



[18] בג"ץ מרשם האוכלוסין, סעיף 7 לפסק דינה של השופטת (בדימוס) דורנר.

ככלל, ניתן לומר כי שלושת ההיבטים העיקריים שבהם דנות שתי הוועדות הם: 1) סמכות הגוף לבקש ולקבל את המידע האישי, בהתאם לתנאים הקבועים בסעיף 23ג לחוק, 2) מידתיות הבקשה, ובכלל זה תכנון העברת המידע באופן בו ההעברה תיפגע בפרטיות במידה שאינה עולה על הנדרש ו-3) היבטי אבטחת מידע, ביחס לתווך שבו יועבר המידע, ולאופן שמירתו של המידע בגוף המבקש.[19] במסגרת בחינת מידתיות העברת המידע, על הוועדות להעברת מידע לוודא, בין היתר, כי המידע המועבר אכן נדרש לצורך התכלית הציבורית לשמה הוא מועבר; כי מועבר המידע המינימאלי הנחוץ בנסיבות העניין; כי השימוש במידע מוגבל לתכלית העברתו; כי המידע נשמר רק למשך הזמן הנדרש לשם התכלית לשמה הועבר כי הרשאות הגישה למידע מצומצמות רק לבעלי התפקידים להם נדרשת גישה למידע לצורך מילוי תפקידם, וכן שהעברת המידע לא גורמת לנזק של פגיעה בפרטיות בעוצמה העולה על התועלת שבהעברת המידע. לכל וועדה סמכות לאשר הגשת בקשות לקבלת מידע על ידי הגוף הציבורי; לאשר קבלת בקשות להעברת מידע שמוגשות על ידי גוף ציבורי אחר, ולקבוע הוראות לעניין הרשאות והגבלות ביחס לגישה למאגרי המידע. האישור יכול להינתן להעברת מידע חד פעמית או מתמשכת, לתקופה של לכל היותר 5 שנים.[20] כמו כן, בעת מסירת מידע אישי, על מנהלי מאגר המידע בשני הגופים לנקוט פעולות אבטחה ובקרה וכן, כאשר מועבר מידע אישי דרך קבע, לקבוע נוהל התקשרות להעברת מידע הכולל יישום עקרונות אבטחת מידע, בקרת גישה וכדומה.[21]

עוד קובעות התקנות חובה להפריד בעת קבלת מידע אישי בגוף בין המידע שהעברתו נתבקשה לבין מידע עודף שהתקבל יחד אתו, ולמחוק מיד את המידע העודף.[22]

---

[19] ר' בג"צ מרשם האוכלוסין; כמו כן, לעניין אופן ביצוע תפקידי הועדות להעברת מידע ר' [הנחית המשנה ליועץ המשפטי לממשלה (ייעוץ) מיום 16.3.2006 בדבר "העברת מידע בין גופים ציבוריים"].

[20] פרט ב(4)(1) לטופס א' שבתוספת לתקנות.

[21] תקנות 4-5 לתקנות.

[22] תקנה 6 לתקנות; ר' גם את ההסדר הכללי יותר בנושא, מכוחו נקבעה התקנה האמורה, בסעיף 23ה לחוק.

פרק ב: ממצאי הצוות

1. נתוני שימוש במנגנון הקיים:

בהחלטת ממשלה מס' 1933 הוטל על רשות התקשוב הממשלתי, בין היתר, לפקח על הפן האדמיניסטרטיבי של עבודת הוועדות המשרדיות להעברת מידע אישי ולהקים מערכת מחשוב רוחבית לניהול עבודת הוועדות להעברת מידע. החל משנת 2018 עלתה לאוויר מערכת "מועד" שאפשרה לראשונה מעקב אחר התהליך וניטור פעילות הוועדות. מהנתונים שנאספו עד כה על ידי מערך הדיגיטל הלאומי ממערכת מועד עולות מספר מסקנות, התומכות בטענה כי תהליך אישור העברת המידע האישי כפי שהוא פועל היום אינו יעיל, ומהווה חסם משמעותי לשיתוף נתונים:

- **משך זמן הטיפול**: מניתוח שעשה מערך הדיגיטל הלאומי המנהל את מערכת מועד על נתונים מהשנים 2019-2023, עולה כי כיום משך הטיפול הממוצע בבקשות לאישור העברות המידע הממוצע בתקופות שגרה עומד על כ-240 ימים עם טווח מקסימלי של מעל ל-500 ימים. בממוצע זו הובאו בחשבון כלל הבקשות להעברות מידע המצויות במערכת – בין אם הוזן עבורן סטטוס המעיד על סיום הטיפול בהן ובין אם לאו. יצוין כי בשנים 2018-2021 פעלה ועדת היגוי בין-משרדית בנושא העברות מידע בין משרדי ממשלה בהובלת רשות התקשוב. בתקופת פעילותה צומצם משך הזמן הממוצע לאישור בקשות.
- **מיעוט הבקשות**: מנתוני עבודת הוועדות ודוחות שנתיים שהוכנו על ידי מערך הדיגיטל הלאומי עולה כי היקף הבקשות להעברת מידע נותר יציב לאורך הזמן ועומד על כמה מאות בקשות בשנה. נתון זה אינו תואם את הגידול בקצב והיקף השימוש בנתונים בממשלה, ומעלה את החשש ל"תהליכי צל" של אישור העברת מידע שאינם מתבצעים בהתאם לנהלים ובמערכת מועד, או ל-"ביקוש חסר" כאשר משרדים נמנעים מבקשת מידע עקב הכבדת התהליכים והסיכוי הנמוך להשלמתם בהצלחה. נוסף על כך, ישנם גופים ציבוריים שאינם מחויבים לניהול התהליך במערכת מועד (כגון הרשויות המקומיות) ולפיכך נתונים לגבי העברות מידע של גופים אלו אינם מתועדים במערכת.
- **שיעור השלמה נמוך**: למעלה ממחצית הבקשות הנפתחות במערכת מועד לא מגיעות לכדי השלמה. משמעות הדבר היא כי תהליך האישור אינו אפקטיבי ועובר לצירים מקבילים או ננטש על ידי המשרד המבקש.
- **שיעור דחיית הבקשות**: שיעור דחיית הבקשות נותר יציב לאורך השנים האחרונות (2017-2020) והוא עומד על 10-15% מהבקשות שהושלמו. לצד נתונים אלו, המבוססים על ניהול תהליך דיגיטלי באמצעות מערכת מועד, מראיונות והיוועצות עם גורמי שטח עולה כי קיימים מקרים רבים שבהם הצורך בקבלת מידע אינו מגיע אפילו לשלב הבקשה הרשמית בשל אורך התהליך ומורכבותו, שאינם עולים בקנה אחד עם פרקי הזמן הנדרשים לאספקת שירותים או לגיבוש מדיניות.

2. אתגרים בהעברת מידע אישי בין גופים ציבוריים:

במסגרת עבודת הצוות הבין משרדי אותרו ששה אתגרים מרכזיים בתהליכי העברות מידע (פירוט נרחב יותר של כל אחד מהאתגרים יובא בהמשך, בפרק ההמלצות):

1. גילוי ואיתור הנתונים (Data discovery): איתור הנתונים המבוקשים הוא שלב מקדים בתהליך העברת

המידע האישי. על המבקש לזהות את מיהות הגורם הציבורי המנהל את הנתונים הכי רלבנטיים לצרכיו, ובכלל זאת לפי קריטריונים של מהימנות ועדכניות. כיום יש קושי לדעת אילו נתונים קיימים בכל גוף ציבורי ומי בעלי התפקיד שיכולים לעזור באיתור המידע ובאישור העברתו. נוסף על כך, העדר שפה ממשלתית אחידה בתחומי הנתונים,[23] והעדר מנגנונים לשימור ידע על אודות הגשת בקשות להעברת מידע אישי בין גופים ציבוריים יוצרים קושי בגילוי הנתונים.

2. <u>אישור העברת המידע האישי</u>: פרוצדורת אישור העברת המידע האישי במנגנון הקיים מורכבת למדי, בשל ריבוי הגורמים הנדרשים לאשר את ההליך, בכירותם וריבוי המשתתפים בכל תהליך אישור כמפורט לעיל. כמו כן, עלולה להתקיים כפילות מסוימת בתהליך האישור, למשל כאשר השאלה האם פעולה מסוימת מצויה במסגרת הסמכויות והתפקידים של מקבל המידע נבחנת הן בידי הוועדה בגוף מוסר המידע והן בידי הוועדה בגוף מקבל המידע.

3. <u>מימוש העברת המידע האישי</u>: לאחר קבלת האישורים להעברת המידע האישי נדרשת השקעת תשומות הן מצד הגוף מוסר המידע והן מהצד המבקש לטובת הכנת המידע להעברה, לרבות ניתוח המערכות הרלבנטיות, טיוב הנתונים, הקמת ממשקים טכנולוגיים להעברת המידע בכלל ובאופן מאובטח בפרט. חוסר אחידות בהגדרות שדות המידע, בממשקים להעברת מידע והצורך בפיתוח ממשקים טכנולוגיים חדשים מובילים לעיכובים גם בשלב המימוש ולעיתים אף לאי העברת המידע המבוקש, אף אם העברתו אושרה על ידי הוועדות כנדרש. נוסף על כך אין כיום ממשק דיגיטלי המאפשר העברה ישירה של המידע לאחר קבלת האישור להעברתו (טופס ב'). לדוגמה, אין חיבור דיגיטלי בין אישור שניתן במערכת מועד למערכת שדרת המידע הממשלתית המשמשת להעברת המידע בפועל.

4. <u>היבטים רוחביים</u>: קיימים מספר אתגרים רוחביים המקשים על העברת המידע האישי בין גופים ציבוריים: הליך העברת המידע האישי בגופים ציבוריים רבים לא מנוהל באופן מרכזי המתייחס לכלל היבטי ההליך - משפטי, טכנולוגי, עסקי ועוד; בקיאות נמוכה של עובדי הגופים הציבוריים בתהליך ובדרישותיו; העדר אינטרס של גוף ציבורי לשתף מידע עם גוף אחר, בין היתר בשל העלויות הכרוכות בהליך העברת המידע, הכוללות את הדרישות התקציביות להעברה, את הבירוקרטיה הנובעת מהטיפול בבקשה ואת עלויות הנגשת המידע והעברתו, ובין היתר את הצורך בפיתוח ממשקים וטיוב הנתונים.

5. <u>תשלום עבור העברות מידע אישי</u>: לעניין משרדי ממשלה נקבע עוד בהחלטת ממשלה 1933 בשנת 2016, כי, ככלל, משרדי ממשלה לא יגבו תשלום ממשרדי ממשלה אחרים עבור העברת מידע, אולם בהחלטה נקבעו חריגים מסוימים, וכן היא אינה חלה על גופים ציבוריים מחוץ לממשלה כגון רשויות מקומיות ותאגידים סטטוטוריים, שנדרשים במקרים רבים לשלם עבור קבלת המידע. מדובר בחסם משמעותי בדמות תשלום כספי הנדרש לשם קבלת המידע האישי, ופעמים רבות מונע מהרשויות המקומיות ומגופים ציבוריים נוספים לקבלו בתדירות גבוהה מספיק. כתוצאה מכך המידע המצוי בידם הוא מידע חסר או מידע שאינו עדכני, המקשה על הרשויות לספק שירות מיטבי לתושביהן ולקבוע מדיניות מבוססת נתונים. בפועל נמצא שגם משרדי ממשלה נדרשים לעיתים לשלם עבור מידע המבוקש על ידם.

6. להפקת מידע ישנה עלות המשתנה לפי סוג המערכת, היקף המידע והתשתיות הקיימות שבאמצעותן ניתן לשלוף את המידע. כנגד עלויות אלו, התשלום לשם קבלת מידע מהווה חסם במקרים בהם נדרשת

[23] הגדרות אחידות לשמות שדות מידע המצויים בשימוש נרחב צפויים להקל על מציאת המידע הנמצא בכל משרד.

העברת מידע לצורך מימוש אחריות הגופים הציבוריים והעלות של העברת המידע מקשה על הגופים המבקשים לשלם אותה, מה שמוביל, כאמור, לכך שמידע עשוי להיות לא מעודכן דיו או חסר בגופים הציבוריים. היעדר תשתיות דיגיטליות מתקדמות מוביל לכך שהעלות להעברת מידע בודדת הינה גבוה מאוד ופעמים רבות דורשת עבודה ידנית. הנתונים הנדרשים נמצאים פעמים רבות בתוך המערכות התפעוליות של המשרדים באופן בו נדרשים משאבים משמעותיים לשליפת המידע. יתרה מזאת, משרדי ממשלה מעטים מחוברים זה אל זה בתשתית API המאפשרת את "העברת הנטל" של יישום העברות המידע למשרד המבקש את המידע, כך שהוא יהיה זה שיצטרך לפתח את הממשק. בהמשך לכך, היעדר האפשרות לגבות תשלום יוצרת תמריץ שלילי להעברת המידע, בפרט בנסיבות בהן עלויות ההעברה הן גבוהות ודורשות השקעת משאבים משמעותיים מצד המשרד המחזיק במידע. מעבר לתשלום עצמו, גם ההליך הבירוקרטי הנוגע להסדרת התשלום מהווה גורם מעכב להשלמת הליך העברת המידע. <u>ביזוריות</u> - לעניין רשויות מקומיות - כיום על אף שכלל הרשויות נדרשות באופן עקרוני לאותם פרטי מידע אישי על מנת לספק שירות בסיסי לתושביהן, כל אחת מהן נדרשת לפנות בנפרד לגוף הממשלתי לשם קבלת המידע. בנוסף, רשויות רבות, כמו גם גופים ציבוריים אחרים שאינם עוסקים בהעברת מידע דרך שגרה, נעדרים היכרות עם ההליכים הנדרשים לצורך קבלת מידע אישי ולעיתים אף נעדרים כוח אדם המתאים לטיפול בנושא, כך שהלכה למעשה הפרוצדורה הכרוכה בהעברות המידע מהווה אתגר משמעותי עבורם.

<u>פירוק האתגרים בתהליך העברות מידע אישי:</u>

פרק ג: סקירה בין לאומית

החלטת ממשלה מס׳ 213 קבעה כי בעת גיבוש הצעת הצוות לעדכון של התהליכים הנוגעים להעברות מידע אישי בין גופים ציבוריים, יתייחס הצוות, בין היתר, להסדרים קיימים להעברת מידע אישי בין גופים ציבוריים במדינות בנות השוואה, בפרט במדינות האיחוד האירופי לרבות ההסדרים החלים בדנמרק, בלגיה ואסטוניה. לאור זאת, בוצעו סקירות משוות ביחס למדינות אלו. כמו כן נבחנו היבטים הקשורים לתהליכי העברות מידע אישי בגרמניה. במסגרת הסקירות נבחנו שלושה היבטים מרכזיים: המסגרת הנורמטיבית המסדירה שיתוף מידע אישי בין גופים ציבוריים; ההליך הבירוקרטי הכרוך בשיתוף מידע אישי בין גופים ציבוריים; והתשתית הטכנולוגית התומכת בתהליכי העברות מידע.

המדינות שנסקרו הן מדינות החברות באיחוד האירופי, ומשכך הן כפופות לתקנות האיחוד האירופי בדבר הגנה על מידע אישי - General Data Protection Regulation (להלן: ״**GDPR**״). הכללים המעוגנים בתקנות אלה חלים ישירות בדין המקומי של המדינות שנסקרו, והם מהווים, בנוסף, גם מקור רלוונטי להשוואה בשל היותם סטנדרטים בינלאומיים מקובלים.[24]

1. <u>המסגרת הנורמטיבית המסדירה שיתוף מידע בין גופים ציבוריים:</u>

תקנה 5 לתקנות ה-GDPR קובעת, בין היתר, כי מידע אישי ייאסף למטרות ספציפיות, מפורשות ולגיטימיות, ולא יעובד עיבוד נוסף למטרה שאינה תואמת למטרות אלה (עקרון צמידות המטרה).[25] מטרות נוספות לעיבוד המידע, ובכלל זה להעברתו, יכולות להיקבע בחקיקה מדינתית, בכפוף לכך שמדובר באמצעי נחוץ ומידתי בחברה דמוקרטית, וזאת בסייגים הקבועים בתקנה 23 ל- GDPR, המגבילה חקיקה מדינתית כאמור לתכליות מסוימות, כגון ביטחון המדינה, אכיפת החוק, הגנה על זכויותיו של נושא המידע או אדם אחר, ותכליות ציבוריות חשובות אחרות.[26] על עיבוד קטגוריות מסוימות של מידע, להן מיוחסת רגישות מיוחדת, חלות מגבלות

---

[24] לבחירה בסקירה של מדינות מהאיחוד האירופי שתי סיבות מרכזיות. האחת, נסקרו מדינות הידועות ברמת הדיגיטציה הגבוהה של רשויות השלטון שלהן ובזמינות של שירותים שלטוניים מקוונים לציבור, כאשר העברת מידע יעילה בין גופים ציבוריים היא אחת מהתשתיות המרכזיות המאפשרות דיגיטציה והנגשה של שירותים באופן מקוון. סיבה שניה היא הסטנדרט הגבוה בתחום הגנת המידע האישי במדינות האיחוד האירופי, הנחשב לסמן ימני בתחום דיני הגנת המידע האישי בעולם כולו, ואשר למדינת ישראל מעמד מיוחד לגביו כמדינה שהדין בה נאות ביחס לדין האירופאי (Adequacy), מעמד המאפשר זרימת מידע חופשית בין ישראל ומדינות האזור הכלכלי האירופי (EEU). כתוצאה משני אלה, ההסדרים בדבר העברת מידע בין גופים ציבוריים במדינות האיחוד האירופי יכולים להוות דוגמה למודל יעיל של העברות מידע המשמר רמת הגנה גבוהה על הפרטיות.

[25] סעיף 5(1)(b) ל – GDPR מחיל את עקרון צמידות המטרה על כל עיבוד מידע, כאשר העברת מידע בין גופים ציבוריים מהווה סוג של עיבוד מידע לעניין זה:

"1. Personal data shall be:
…(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);"

[26] תקנה 6(4) ל – GDPR:

"Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject’s consent **or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)**, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia …"

בתקנה 23(1) נקבעו המגלות על אפשרות חוק המדינה לחרוג מכללי הGDPR, ובכלל זה מעקרון צמידות המטרה, ובכלל זה התכליות המותרות לחריגה כאמור:

נוספות, המאפשרת לעבדן למטרות מצומצמות עוד יותר.[27] עקרון צמידות המטרה חל לפי ה- GDPR גם במקרים של העברת מידע אישי בין גופים ציבוריים.[28] לפיכך, העברת מידע אישי בין גופים ציבוריים כפופה במדינות אירופה לעקרון צמידות המטרה או למטרות ספציפיות שהותרו בחקיקה, בכפוף למגבלות על מטרות אלה. זאת, בניגוד לדין בישראל שפורט לעיל, לפיו הסמכות להעברת המידע האישי בין גופים ציבוריים מהווה חריג (במגבלות התנאים הקבועים בחוק ובמבחני המידתיות) לעיקרון צמידות המטרה, ומאפשרת, בכפוף לתנאים הקבועים בסעיף 23ג לחוק הגנת הפרטיות, להעביר מידע אישי למטרה הרחבה מאוד של מילוי הסמכויות או התפקידים של גוף ציבורי (וזאת גם כאשר מדובר במידע בעל רגישות מיוחדת כהגדרתו בחוק).

כאמור, החריג לעקרון צמידות המטרה ב – GDPR, במגבלות הקבועות בו, דורש יישום קונקרטי בחקיקה של כל אחת ממדינות האיחוד. בגרמניה, נמצא כי עיבוד מידע אישי, לרבות העברתו לגוף ציבורי אחר, שלא לתכלית לשמה אסף את המידע, מותרת לצורך מילוי חובותיו של הגוף, וזאת רק לתכליות מצומצמות בלבד: כשההעברה נועדה לטובת האינטרסים של נושא המידע ואין סיבה להניח שהיה מסרב לה; כאשר נדרש לבדוק מידע אישי שנמסר על ידי נושא המידע ויש חשש לגבי אמיתותו; מניעת נזק לשלום הציבור, פגיעה בביטחון המדינה, לטובת אינטרס ציבורי כללי חשוב או לטובת גבית מס ומכס; לטובת הליכים משפטיים פליליים או מנהליים; מניעת פגיעה חמורה בזכויות אדם אחר; פיקוח ובקרה על מעבד מידע.[29] באסטוניה, נראה כי לא נדרשת ככלל העברת

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
1. national security;
2. defence;
3. public security;
4. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
5. other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
6. the protection of judicial independence and judicial proceedings;
7. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
8. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
9. the protection of the data subject or the rights and freedoms of others;
10. the enforcement of civil law claims.

[27] תקנות 9-10 ל – GDPR.

[28] עיבוד מידע אישי (processing) מוגדר בתקנה 4(2) ל – GDPR ככל פעולה במידע אישי, לרבות, בין היתר, העברתו.

[29] חוק הגנת המידע הפדרלי הגרמני (BDSG) - Federal Data Protection Act, סעיפים 25 ו- 27. רשימת התכליות המלאה להעברת שלא למטרה לשמה נאסף קבועה בסעיף 25(1) לחוק:
"Public bodies shall be permitted to process personal data for a purpose other than the one for which the data were collected where such processing is necessary for them to perform their duties and if
1. it is obviously in the interest of the data subject and there is no reason to assume that the data subject would refuse consent if he or she were aware of the other purpose;
2. it is necessary to check information provided by the data subject because there is reason to believe that this information is incorrect;
3. processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security; to safeguard substantial concerns of the common good; or to ensure tax and customs revenues;

מידע אישי בניגוד לתכלית לשמה נאסף המידע. כל מאגר מידע של גוף ציבורי באסטוניה מוסדר במסגרת חקיקה ראשית או חקיקת משנה. במסגרת חקיקה זו, נקבעת תכלית עיבוד המידע שבמאגר, לרבות התכליות לשמן ניתן להעביר את המידע האישי לגופים ציבוריים אחרים. חקיקה כזו נבחנת בחינה מוקדמת, בין היתר, עד ידי רשות הפיקוח על מידע אישי של אסטוניה (Data protection inspectorate).[30]

הגדרת הגופים הנחשבים כגופים ציבוריים לעניין העברת המידע האישי ביניהם דומה יחסית בין המדינות שנסקרו (וכן ביחס להסדר הישראלי). כך, בבלגיה ההסדר חל על הממשלה (הפדרלית, המדינתית והמקומית), על ישויות ציבוריות הנתמכות במדינה ומוסדותיה הפדרליים והמקומיים, וכן על כל אדם או גורם הפועל למען האינטרס הציבורי ופעילותו ממומנת על-ידי הרשויות הנ״ל או שהוא נתון לפיקוח על ידן.[31] בגרמניה, גופים ציבוריים מוגדרים באופן רחב יחסית וכוללים רשויות מקומיות, גופים שיפוטיים, גופים ציבוריים אחרים לרבות גופים פרטיים שמבצעים משימות ציבוריות.[32]

<u>2. ההליך הבירוקרטי הכרוך בשיתוף מידע אישי בין גופים ציבוריים:</u>

נתאר להלן את המנגנונים הפרוצדוראליים המרכזיים לאישור העברת מידע אישי בין גופים ציבורים אשר נמצאו בסקירה הבין לאומית.

מנגנון מרכזי שנמצא במדינות שנסקרו, וכן במדינות נוספות, הוא **הסכמי שיתוף מידע** בין גופים ציבוריים. הסכמים אלו יכללו, בין היתר, את סוג המידע המבוקש, האוכלוסייה שלגביה מבוקש המידע, התכלית לשמה מותר השימוש במידע המועבר, הסדרת הבטי אבטחת המידע וקביעת הפלטפורמה הטכנית לשיתוף המידע. בבלגיה, העברות מידע אישי סיסטמתיות מבוצעות באמצעות חתימה על הסכם (פרוטוקול) שיתוף מידע בין הגופים הציבוריים הרלוונטים להעברה. הפרוטוקול צריך לכלול את הפרטים הבאים: זהות הגוף המעביר ומקבל המידע האישי; פרטי הקשר של ממוני הגנת המידע האישי (DPO) משני הצדדים; מטרת ההעברה; קטגוריות של מידע אישי מועבר; הבסיס החוקי להעברה; מגבלות על ההעברה; זכויותיו של האדם נשוא המידע האישי; תדירות ההעברה, תוקפו של הפרוטוקול; סנקציות בגין אי ציות והוראות נוספות.[33] כמו כן, ישנה חובה בפרסום הפרוטוקול לציבור.[34]

גם בגרמניה נמצא כי העברת מידע אישי בין גופים ציבוריים מוסדרת באמצעות הסכם להעברת המידע בין הגופים. הסדרת העברת המידע האישי בהסכם נדרשת כאשר מועבר מידע על יותר מ – 50 נושאי מידע. באישור

---

4. processing is necessary to prosecute criminal or administrative offences, to carry out or enforce punishment or measures as referred to in Section 11 (1) no. 8 of the Criminal Code or educational or disciplinary measures as referred to in the Juvenile Court Act or to enforce fines;
5. processing is necessary to prevent serious harm to the rights of another person; or
6. processing is necessary to exercise powers of supervision and monitoring, to conduct audits or organizational analyses of the controller; this shall also apply to processing for training and examination purposes by the controller, as long as it does not conflict with the legitimate interests of the data subject."

[30] מבוסס על התייעצות עם נציג משרד המשפטים האסטוני.

[31] Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens in translation: Act on the Protection of Natural Persons with regard to the Processing of Personal Data, [Belgian Official Gazette], 5 September 2018, Article 5.

[32] חוק הגנת המידע הפדרלי הגרמני (BDSG) - Federal Data Protection Act, סעיף 2.

[33] שם, בסעיף 20.

[34] ראו סעיף 20(3) לחוק הגנת המידע הבלגי: כמו כן ראו דוגמאות לפרוטוקולים שנחתמו בין גופים ציבוריים בבלגיה.

העברת מידע אישי בין גופים ציבוריים מעורב הממונה על הגנת הפרטיות (DPO). בנוסף, בכפוף לגודל הגוף הציבורי עשויים להיות גופי אישור פנימיים או ועדות האחראיות לבדיקה ואישור העברת המידע.

כמנגנון נוסף להסדרת העברת מידע אישי בין גופים ציבוריים נמצא במספר מדינות שנסקרו כי ישנו **גוף מרכזי** אשר לו סמכות לאשר העברות המידע. בחלק מהמקרים גוף זה אף מבצע פעולות פיקוח. בבלגיה למשל, ישנה ועדה מרכזית - "ועדה להגנת המידע", אשר במקרים מסוימים מטפלת בבקשות להעברת מידע, ודנה במקרים בהם גופים ציבוריים לא הגיעו להסכמות ולחתימה על פרוטוקול שיתוף מידע. הוועדה היא גוף עצמאי שחבריה מתמנים כל 6 שנים ומורכבת מנציגי לשכות הבריאות, הבטחון הלאומי, נציגי הרשות הפדרלית וכן מומחים בתחום הגנת המידע והפרטיות. החלטות הוועדה להגנת המידע מפורסמות לציבור.[35]

3. התשתית הטכנולוגית התומכת בהעברות מידע בין גופים ציבוריים:

ברוב המדינות שנסקרו נמצא כי קיימת פלטפורמה מרכזית שבאמצעותה מבוצעים הליכי העברות מידע. הפלטפורמה המרכזית מבטיחה כי המידע העובר דרכה יהיה מקוטלג וקובעת סטנדרטים טכנולוגיים אחידים להעלאת והעברת מידע. כך למשל בבלגיה, ישנו גוף הנקרא שירותי האינטגרציה הפדרליים (The Federal Service Integrator) שנועד לשרת הליכי העברת מידע מתמשכים בין גורמי ממשל. כל גוף ציבורי מחויב למפות ולהעלות כל מידע שבבעלותו (למעט מידע סודי ביותר) לפלטפורמה מרכזית, וזו תעביר את המידע לכל משרד מבקש בכפוף להרשאה מתאימה.[36] בעת הצטרפותו של גוף ממשלתי לפלטפורמה, עליו להוכיח את הבסיס החוקי המקנה לו גישה למידע, וכאשר מדובר בבקשה לצפות במידע אישי נדרש פרוטוקול הסכם לשיתוף מידע בין גופים (כפי שצוין לעיל) או החלטת ועדה.

גם באסטוניה ישנה פלטפורמת מידע מרכזית המכונה X-tee וכוללת 8 מאגרי מידע מרכזיים (מתוכם 3 מאגרים ממשלתיים – מנהל רישום אוכלוסין, מנהל ביטוח בריאות ומאגר מידע לרישוי רכב). מקורות המידע אינם מתקשרים ביניהם ישירות, אלא באמצעות ממשקים לפלטפורמה המרכזית. המידע הקיים במאגרים חייב להיות ממופה ומקוטלג, ושיתוף המידע בין גופים ציבורים מבוצע באמצעות הפלטפורמה המרכזית.

בדנמרק, כחלק מרפורמה ממשלתית שבוצעה בהליכי העברות מידע, בוצע הליך של מיפוי המידע הקיים בכל מאגר ממשלתי וכן מיפוי של המערכות הקיימות להעברת מידע. לאחריו הוקם פורטל למגזר הציבורי ובו קטלוג שאמור לסייע באיתור המידע ושיתופו בין הגופים הציבוריים. מבחינה טכנולוגית העברת מידע מבוססת על מודל Point to Point כלומר אינה מתבצעת באמצעות תיווך, אלא באמצעות סטנדרט API[37] - סטנדרט טכנולוגי מקובל המעביר מידע באופן מאובטח בין המערכות השונות. על אף שההליך הטכני מעט שונה מההליכים בבלגיה ובאסטוניה משום שהמידע אינו מועלה לפלטפורמה מרכזית, הליכי העברות המידע מבוצעים בסיוע הפורטל והקטלוג המרכזי; מבקש המידע נכנס לפורטל למגזר הציבורי, יוצר בו שאילתה, מקור המידע מאותר במערכת בעלת המידע ולאחר קבלת אישור, מבקש המידע מקבלו בפורמט שביקש.[38]

[35] ראו הסבר באתר הוועדה להגנת המידע הבלגית.
[36] ראו: https://bosa.belgium.be/nl/services/federale-dienstenintegrator.
[37] – Application Programming Interface - ממשק תכנות יישומים
[38] https://en.digst.dk/digital-governance/data/

פרק ד: המלצות הצוות

המלצות הצוות מחולקות לפי השלבים העיקריים בתהליכי מימוש העברות מידע אישי, החל משלבי הגילוי והאיתור, בקשת המידע ואישורה, מימוש העברה והיבטים רוחביים הנוגעים לתהליך בכללותו. מטרת ההמלצות היא להעמיד מענה, מלא או למצער חלקי, לאתגרים להעברה יעילה של מידע אישי בין גופים ציבוריים, בשלל התחומים שפורטו לעיל. בהתאם, מציע הצוות סל משולב של פתרונות – משפטיים, טכנולוגיים, ניהוליים, ארגוניים וכלכליים-תקציביים.

<u>1. גילוי ואיתור הנתונים בין גופים ציבוריים:</u>

כפי שצוין בפרק ב' לעיל, ישנו קושי כיום באיתור הנתונים הקיימים בכל גוף ציבורי, ואין פלטפורמה מרכזית ואחודה לגילוי (Data discovery), לקיטלוג ואיתור הנתונים בקרב גופי המגזר הציבורי בכלל, וגופי הממשלה בפרט.

על מנת להתמודד עם קשיים אלו, הצוות ממליץ על יצירת קטלוג מידע אחוד והנגשתו לגופי המגזר הציבורי. קטלוג המידע צריך לכלול פונקציות שונות לרבות: יכולת לבצע **גילוי מאפייני סוגי המידע** (מטא-דאטה) של המאגרים המרכזיים, יצירת מערכת **תיוג** סוג המידע לפי תוויות נושאיות, וזיהוי קשרים בין מאגרים שונים. כמו כן הקטלוג יאפשר **חיפוש** לפי שאילתות בדבר תחום התוכן של מידע, מיהות מנהלי המידע, פרטי שדות המידע, מועד עדכונו ו**ניהול המשתמשים** השונים לרבות מנגנון ניהול הרשאות, ותיעוד ומעקב אחר שימוש. הצוות מבין כי ברשות גופים ציבוריים שונים ישנו מידע בהיקפים עצומים ולכן ממליץ לתעדף את בניית הקטלוג לפי סוגי מאגרי מידע המצויים או צפויים להימצא בשימוש הנרחב ביותר.

כמו כן, ישנם גופים שהמידע המנוהל על ידם אינו מטויב דיו, ולפיכך קיים קושי להעבירו לגוף ציבורי אחר בטווחי זמן קצרים. בניית קטלוג מרכזי והקצאת משאבים לפרויקט קיטלוג מאגרים נבחרים בגופים מתועדפים, יוצרים הזדמנות להשקעת תשומות בארגון וניהול המידע הפנים ארגוני. הדבר נכון במיוחד ביחס לגופים ציבוריים בהם מאגרי המידע נבנו לאורך השנים בצורת "טלאי על טלאי". הכנת המידע לקטלוג, מאפשרת חשיבה מחדש על ניהול המידע והנתונים ועשויה להוביל לארגון יעיל יותר שלו.

נוסף על האמור, הצוות ממליץ על יצירת ממשקים בין קטלוג המידע לבין הפלטפורמות השונות הקשורות לתהליכי שיתוף מידע כגון מערכת חדשה לניהול הליך העברת המידע במקום מערכת מועד, עליה יפורט בהמשך ("מערכת צ'יטה"), ופלטפורמות להעברת המידע בפועל כגון שדרת המידע הממשלתית.

בעת פיתוח הקטלוג והזנת הנתונים אליו, יבחן מערך הדיגיטל הלאומי את האפשרות להשתמש גם בנתונים אודות מאגרי מידע שקיימים בלשכה המרכזית לסטטיסטיקה במסגרת פרויקט "אגם המידע".

<u>המלצות לשלב הגילוי והאיתור:</u>

א. <u>בניית קטלוג מידע של גופים ציבוריים</u> – מאחר שמדובר במוצר תשתיתי, הצוות ממליץ כי מערך הדיגיטל הלאומי יהיה אמון על פיתוחו ותפעולו, וזאת בשיתוף פעולה עם משרדי הממשלה, יחידות

הסמך והתאגידים הסטטוטוריים הרלוונטיים.[39]

ב. <u>הטמעת הקטלוג בגופים ציבוריים מרכזיים והקצאת המשאבים הנדרשים לכך</u> – הצוות ממליץ כי הגופים הציבוריים המנהלים מאגרים מרכזיים יתועדפו בחיבור לקטלוג, לצרכי מיפוי פנימי ועדכון. בשלב ראשון, יחוברו לקטלוג וינגישו באמצעותו את המידע אודות המאגרים שנקבעו בסעיף 13 להחלטת ממשלה מס׳ 2273,[40] מאגרים רלוונטיים של הגופים המפורטים בנספח ב׳[41] להחלטה האמורה, וכן מאגרים רלוונטיים של משרד הבריאות ומשרד הרווחה והביטחון החברתי. תיעדוף הגופים והמאגרים הרלוונטיים בגופים יתבצע על-ידי מערך הדיגיטל הלאומי, אגף התקציבים במשרד האוצר, משרד ראש הממשלה והלשכה המרכזית לסטטיסטיקה (למ״ס), בתיאום עם הגופים הציבוריים הרלוונטים ובהתאם לקריטריונים הכוללים את היקף השימוש הקיים והצפוי במידע. כמו כן, הצוות ממליץ כי גופים אלה יבצעו עבודות של טיוב המידע לרמה כזו שתאפשר מוכנות גבוהה להעברתו. לשם כך, מוצע להקצות משאבים מתאימים עבור אותם גופים ציבוריים.

ג. <u>מאמצים משלימים</u> – כפי שיפורט בפרק בדבר ההיבטים הרוחביים להלן, לצד ההיבט הטכנולוגי של הקמה והטמעת השימוש בקטלוג מידע מרכזי, יש צורך בהמשך חיזוק היבטים ניהוליים וארגוניים הנוגעים גם לשלב איתור המידע. זאת, בין היתר על ידי מינוי בעל תפקיד לניהול תחום העברות המידע בגוף הציבורי, ופעולות להגברת אוריינות המידע והנתונים הממשלתיים בקרב גורמי המקצוע בגוף, כגון

---

[39] בשלב זה לא מצא הצוות מקום להמליץ על הרחבת הקטלוג לרשויות המקומיות, והוא יתמקד במשרדי הממשלה ובמוסדות מדינה אחרים כגון המוסד לביטוח לאומי.

[40] בסעיף 13(א) להחלטה 2273 הוחלט לעניין זה כדלקמן:

״13. להטיל על מערך הדיגיטל הלאומי בתיאום עם הלמ״ס ועל משרדי הממשלה הרלוונטיים לפתח פתרונות טכנולוגיים רוחביים תוך שימת דגש על עיצוב לפרטיות (Privacy by Design), אבטחת מידע והגנת סייבר:

א. קטלוג מידע של גופים ציבוריים:

1) להטיל על מערך הדיגיטל לגבש פתרון לקטלוג, אשר יכלול מידע רלוונטי בדבר סוג המידע המצוי במאגרי מידע רלוונטיים, שמות שדות המידע, פרטי מנהלי המאגר, ותדירות עדכון המידע (להלן – מטא-דאטה), בכפוף להוראות כל דין, ולהחצין קטלוג מידע לגופים הציבוריים (להלן – הקטלוג המרכזי). הקטלוג יהווה תשתית אשר תאפשר לכל גוף ציבורי לפרט את המטא-דאטה הקשור למאגרי המידע המרכזיים המנוהלים על ידו, להבדיל מתוכן שדות המידע, ותאפשר למשתמשים השונים מתוך הגופים הציבוריים לאתר ביעילות סוגי מידע הנדרשים להם מגופים ציבוריים אחרים, ולממש מדיניות ״פעם אחת בלבד״ רצוי להפוך את זה לבסט פרקטיס, גם אם לא מחייב בהתחלה כמשמעותה בהחלטה 1933.

2) גרסה ראשונה של הקטלוג תעלה לאוויר ותאפשר הזנת מידע וחיפוש בקטלוג בתוך 6 חודשים ממועד אישור ההחלטה, ותתבצע בשיתוף, בין היתר, עם מנהלי המאגרים המרכזיים המפורטים להלן.

3) הנגשת מידע בשימוש נרחב:

(א) להטיל על הגורמים הבאים, בתיאום עם מערך הדיגיטל הלאומי ובהתייעצות במידת הצורך עם הלשכה המרכזית לסטטיסטיקה (להלן – הלמ״ס), לשתף את מערך הדיגיטל במטא-דאטה הרלוונטי לצרכי איתור מידע, ולעדכן בדבר שינויים אחת לשנה לכל הפחות, או באופן אוטומטי במצבים שניתן, הקשור במאגרים הבאים:

(1) רשות האוכלוסין וההגירה – לעניין מרשם האוכלוסין ונתוני כניסות ויציאות מהארץ.

(2) משרד המשפטים – לעניין מרשמי התאגידים ומרשם המקרקעין (טאבו).

(3) רשות המיסים – לעניין מרשם העוסקים והעסקים.

(4) משרד התחבורה והבטיחות בדרכים – לעניין מאגר רישיונות הנהיגה.

(ב) לרשום את הודעת המוסד לביטוח לאומי, שיפעל לשתף את מערך הדיגיטל במטא-דאטה הרלוונטי לצורכי איתור מידע בין גופים ציבוריים ולשמור על עדכניות המידע.

(ג) לרשום את הודעת שירות התעסוקה, שיפעל לשתף את מערך הדיגיטל במטא-דאטה הרלוונטי לצורכי איתור מידע בין גופים ציבוריים ולשמור על עדכניות המידע.

(ד) תוכנית השלמת הקטלוג:

(1) להנחות את משרדי הממשלה המופיעים בנספח ב׳ להחלטה זו להגיש למערך הדיגיטל הלאומי בתוך 12 חודשים ממועד אישור החלטה זו המלצה למיפוי 5 ממאגרי המידע שברשותם, שבמידע שבהם ישנו כיום, או צפוי להיות, היקף שימוש משמעותי על ידי גופים ציבוריים אחרים, ולהנגשת המטא-דאטה של המאגרים הללו לקטלוג המרכזי.

(2) להטיל על ראשת מערך הדיגיטל הלאומי, בתיאום עם הלמ״ס, להגיש עבור הגופים המפורטים בנספח, בתוך 90 יום מאישור החלטה זו, את פורמט הקטלוג ומדריכים לבנייתו.

(3) להטיל על ראשת מערך הדיגיטל הלאומי, בתיאום עם הלמ״ס, לפרסם את פורטל הקטלוג בתוך 150 יום מאישור החלטה זו. פורטל זה ייבנה תוך סיוע משרדי הממשלה הנוגעים לדבר וצרכני המידע. הפורטל יכיל את תיאור פורמט הקטלוג מדריכים לבניית קטלוג ארגוני סטנדרטי.״

[41] הגופים שנקבעו בנספח ב׳ להחלטה 2273 כגופים עליהם מוטלת חובה להכנת תכנית להשלמת הקטלוג הם: רשות האוכלוסין וההגירה; משרד התחבורה והבטיחות בדרכים; רשות המיסים; בתי הדין הרבניים; משרד החינוך; משרד המשפטים; משרד העבודה; המשרד לשירותי דת; המרכז למיפוי ישראל; המוסד לביטוח לאומי; שירות התעסוקה.

המשך ההכשרות בתחומי הנתונים והשתלמויות בתחום.

סיכום ההמלצות לשלב גילוי ואיתור המידע:

1. בניית קטלוג מידע ממשלתי על ידי מערך הדיגיטל הלאומי, והקצאת המשאבים הנדרשים לפיתוחו.
2. הטמעת הקטלוג בגופים ציבוריים מרכזיים, שינגישו באמצעותו את המידע על המאגרים שפורטו לעיל, על ידי הגופים בסיוע מערך הדיגיטל הלאומי, והקצאת המשאבים נדרשים לכך.
3. יצירת עזרים ומדריכים להנגשה וחיפוש של מידע הממשלתי.

2. הליך אישור העברת המידע האישי:

כמפורט לעיל, נמצא כי היקף הסמכות החוקית להעברת מידע אישי בין גופים ציבוריים הוא רחב מאוד, ואינו מהווה כשלעצמו חסם להעברת המידע. לצד זאת, קושי מרכזי בהעברת המידע האישי שזוהה בעבודת הצוות נוגע להליך הנדרש לאישור ההעברה. בהתאם להוראות תקנות הגנת הפרטיות, כל העברה של מידע אישי (למעט העברת מידע פרטנית) נדרשת להיות מאושרת בשתי ועדות להעברת מידע – בגוף מבקש המידע ובגוף מוסר המידע, כאשר ההסדר הקבוע כיום בתקנות אינו מבחין בין סוגים שונים של העברות מידע אישי מבחינת היקף המידע המועבר או רגישותו של המידע.

הדרישה לאישור להעברת המידע האישי גם בגוף המבקש את המידע וגם בגוף המוסר את המידע משרתת תכלית חשובה של בקרה על העברת המידע האישי, ואיזון בין האינטרסים הציבוריים העומדים ביסוד הצורך במידע, המיוצגים ככלל על ידי מבקש המידע, לבין האינטרס בהגנה על המידע האישי ושמירה על הפרטיות, המיוצג ככלל על ידי מוסר המידע. מנגד, הדרישה לאישור כפול מטילה נטל לא מבוטל על שני הגופים. כך, הגוף ממנו מתבקש המידע האישי, נדרש, בין היתר, לאשר את חוקיות ומידתיות העברת המידע, כשזו תלויה פעמים רבות בהיכרות עם צרכיו ואופן פעולתו של מקבל המידע ופרשנות הדינים מכוחם הוא פועל, עניינים שלרוב לא נמצאים בתחום מומחיותו של הגוף ממנו מתבקש המידע. כמו כן, עצם הצורך לאשר פעולה מנהלית תדירה יחסית של העברת מידע אישי בין גופים ציבוריים בשתי ועדות שונות, יוצר קושי בירוקרטי המתבטא בפרק הזמן הממושך הנדרש לקבלת אישורים אלה. לאור זאת, הצוות ממליץ לקבוע כמה מסלולים חלופיים לאופן בו ניתן לאשר העברת מידע אישי, במקום המסלול היחיד של הוועדות להעברת מידע הקיים כיום. המסלולים החלופיים גובשו תוך יישום תפישה של ניהול סיכונים, לפי רגישות והיקף המידע המועבר, ושכיחות הצורך בסוגי מידע מסוימים בקרב גופים ציבוריים רבים.

ביחס להעברת מידע אישי בהיקפים גדולים או בעלי רגישות מיוחדת סבר הצוות כי המנגנון הקיים משקף איזון ראוי בין הצורך להעביר את המידע, לבין הפגיעה בפרטיות כתוצאה מהעברתו. לעומת זאת, כאשר מועבר מידע אישי שאינו בהיקף גדול ואינו בעל רגישות מיוחדת, וכן כאשר מועבר מידע בנסיבות המפחיתות את עוצמת הפגיעה בפרטיות, נראה כי נכון לאפשר להעביר את המידע בהליך מכביד פחות.

קושי נוסף באופן בו מובנה כיום הליך האישור של העברת מידע הוא שמנגנון האישור מתוכנן להסדיר העברת מידע אישי בין שני גופים ציבוריים בלבד. אולם, הצורך העולה מן הגופים הציבוריים, בין השאר לאור תהליכי הדיגיטציה ומהפכת המידע, הוא להעביר גם מידע אישי בהעברות מרובות משתתפים. כך, בחלק מהמקרים

נדרש גוף ציבורי להעביר אותו סוג מידע באותן נסיבות לגופים ציבוריים רבים, למשל במקרה של העברת מידע ממשרד ממשלתי לרשויות המקומיות, כל אחת לגבי תושביה. במקרים אחרים, נדרש להעביר את המידע בין כמה גופים ציבוריים שונים, לדוגמה לשם הפקת נתון הדרוש לתכנון מדיניות באמצעות הצלבת יותר משני מקורות מידע. בהתאם, ממליץ הצוות על קביעת חלופות שיאפשרו לאשר באופן מרוכז העברת מידע אישי בין יותר משני גופים ציבוריים.

א. לאור האמור, מוצע לקבוע מסלולים נוספים שיפורטו להלן לאישור העברת מידע אישי:

1. <u>מסלול להעברת מידע בסיסי (Basic Data)</u> – הצוות מצא כי לגבי סוגי מידע אישי מסוימים, שאינם בעלי רגישות מיוחדת[42], ובהיקף שאינו עולה כדי העתקה של המאגר או של חלק ניכר ממנו, וקיים צורך נרחב בקבלתו על ידי גופים ציבוריים רבים המספקים שירות לציבור. מדובר בפרטי מידע כגון מספר זהות, שם מלא בעברית ובאנגלית, מין, כתובת מגורים, כתובת למשלוח דואר, מספר טלפון נייד, כתובת דואר אלקטרוני, תאריך לידה, מדינת האזרחות, רישיון נהיגה, מספר ותוקף רישיון רכב, מצב אישי, תאריך מצב אישי, תאריך כניסה למען, אינדיקציית שהות בחו״ל מעל חצי שנה, אינדיקציית פטירה, תאריך פטירה. מוצע לקבוע את פרטי המידע האישי שיחשבו למידע בסיסי ברשימה סגורה בחקיקת משנה. לגבי פרטי מידע אלה, מוצע לקבוע הליך מיוחד ומקל לאישור העברתם. כך, כל גוף ציבורי הזקוק למידע הבסיסי לצורך מתן שירות לציבור, יוכל, לאחר התייעצות עם ממונה הגנת הפרטיות של אותו גוף,[43] להודיע לגוף הציבורי המנהל מידע אישי כאמור כי הוא זקוק למידע ועומד בתנאים הקבועים בסעיף 23ג לחוק הגנת הפרטיות, ולקבלו ללא צורך בבדיקות נוספות של הגוף מעביר המידע בדבר חוקיות העברת המידע. הודעת הגוף הציבורי מבקש המידע תאושר על ידי היועץ המשפטי של הגוף או נציגו.

2. <u>מסלול להעברת מידע אישי על סמך אישור מבקש המידע</u> - מידע אישי שאינו רגיש ובהיקף שאינו עולה כדי העתקה של המאגר או של חלק ניכר ממנו, יועבר ללא צורך באישור הוועדה להעברת מידע של הגוף הציבורי מוסר המידע. האחריות לערוך בחינה משפטית של חוקיות העברת המידע - עמידת העברת המידע בתנאי סעיף 23ג ובמבחני המידתיות, תוטל על הוועדה להעברת מידע של הגוף מבקש המידע בלבד. הוועדה להעברת מידע בגוף מוסר המידע תתבקש לאשר רק כי לא חל איסור חוקי על העברתו של סוג המידע המבוקש.[44] ככל שנסיבות המקרה לא מחייבות אחרת, יוכל אישור על העדר איסור חוקי על העברת המידע להינתן באופן כללי לגבי סוג מידע מסוים, ללא צורך בבחינה חוזרת שלו לגבי כל בקשה ובקשה.

עוד מוצע, כי מסלול אישור זה יחול גם על מקרים בהם מידע בעל רגישות מיוחדת או בהיקף ניכר עבר התממה לא מלאה, כך שהוא אינו מזוהה בפועל, אך עדיין קיימת אפשרות מסוימת לזהות למי הוא מתייחס (ולכן הוא מהווה ״מידע אישי״ כהגדרתו בחוק הגנת הפרטיות). זאת, בתנאי שההתממה הלא מלאה של המידע היא ברמה כזו המאפשרת לייחס להעברתו פגיעה נמוכה בפרטיות. דוגמה להתממה

[42] ר׳ הגדרת ״מידע בעל רגישות מיוחדת״ בסעיף 3 לתיקון מס׳ 13 לחוק הגנת הפרטיות. הצוות שוקל לאפשר קביעה של פרטי מידע נוספים כבעלי רגישות מיוחדת לעניין העברתם לגופים ציבוריים אחרים (לדוגמה תמונות פנים בצרוף שם ותעודת זהות, גם עם המידע לא משמש או נועד לשמש לזיהוי ביומטרי, ולכן לא נכלל בהגדרה של מידע בעל רגישות מיוחדת).

[43] החובה למנות ממונה על הגנת הפרטיות בגופים ציבוריים (ובגופים פרטיים מסוימים) נקבעה בסעיף 17ב1 לחוק הגנת הפרטיות, בנוסחו בתיקון מס׳ 13 לחוק.

[44] בהתאם להוראות סעיף 23ג, חל איסור על העברת סוג מסוים של מידע אם מסירתו נאסרה בחיקוק או בכללים של אתיקה מקצועית, או אם המידע נמסר בתנאי שלא ימסר לאחר.

לא מלאה כזו יכולה להיות הסרה של פרטים מזהים ישירים כמו שם, מספר זהות, כתובת וכו', וכן של פרטי מידע המאפשרים זיהוי חוזר באמצעות הצלבת מידע פשוטה יחסית עם מידע זמין, אך מבלי שניתן להבטיח כי הצלבה של המידע עם כל מידע אחר לא תוכל לאפשר את זיהוי המידע במאמץ סביר.[45] עמידה בתנאי זה תיבחן על ידי הוועדה להעברת מידע של הגוף מוסר המידע, אשר תוכל לתת אישור כללי לגבי כלל המידע שהותמם בדרך האמורה. לעניין התקיימות התנאי, היכולת להסתמך על התממה לא מלאה נובעת מהעובדה שהמידע מועבר לגוף ציבורי אחר, החב חובת סודיות ואבטחת מידע לגבי המידע ושחלה עליו חזקת תקינות המנהל. בפרט, בהעברה מסוג זה יקבע במפורש כי הגוף מקבל המידע לא יבצע כל פעולה שעשויה, במישרין או בעקיפין, לאפשר זיהוי של מי שהמידע הוא עליו. כמו כן יובהר כי מידע שיועבר במסלול זה על סמך התממה לא מלאה עדיין יחשב למידע אישי כהגדרתו בחוק הגנת הפרטיות, ועדיין יחולו עליו כל הוראות הדין החלות על מידע אישי המוחזק בידי גוף ציבורי. רמת אבטחת המידע והגנת הסייבר של מידע מסוג זה תקבע לפי רמת הרגישות של המידע המקורי לפני התממתו החלקית.

3. <u>הסכמי העברת מידע אישי</u> – מוצע לקבוע כי שני גופים ציבוריים או יותר יוכלו לחתום ביניהם על הסכם להעברת מידע אישי, כתחליף לאישורי הוועדות להעברת מידע. חלופה זו נועדה לאפשר, בין היתר, הסדרה של העברת מידע אישי בין יותר משני גופים ציבוריים במסמך מחייב אחד. כמו כן, כאשר נחתם הסכם בנושאים אחרים בין גופים ציבוריים, ניתן יהיה לכלול בתוכו גם את ההסדר להעברת המידע האישי הנדרש לצורך ביצועו של אותו הסכם. בכך המסמך יתכלל את כל ההיבטים הנוגעים לאותו עניין והנדרשים לביצועו. הסדרת העברת המידע האישי יחד עם הסדרת הנושא לשמו העברת המידע נדרשת תאפשר שיח יעיל יותר בין הגופים הציבוריים, שיביא בחשבון את הצרכים והתמריצים של כלל הצדדים להסכם ויגביר את שיתוף הפעולה ביניהם. כמו כן, יישום ההסכם לא יהיה מותנה בהליך בירוקרטי נפרד של אישור הוועדות להעברת מידע וגם במובן זה הליך העברת המידע יהיה יעיל יותר. יובהר כי מסלול אישור זה נועד לרכז את הטיפול באישור העברת המידע האישי באופן שיקל על ביצוע ההליך, ולא להפחית מרמת הבחינה של העברת המידע האישי. כך, מבחינת הנושאים שנדרש לבחון במסגרת אישור העברת מידע אישי וזהות הגורמים המאשרים בגוף מקבל המידע ובגוף המעביר, חלופה זו דומה לחלופה של אישור הוועדות להעברת מידע. בהתאם, בהסכם העברת מידע אישי יהיה צורך להסדיר את כל הנושאים שנדרש להסדיר במסגרת הוועדות להעברות מידע. בדומה, לחלקים הנוגעים להעברת מידע אישי בהסכם יידרש אישור של גורמים דומים לאלה שבוועדות להעברת מידע, בשני הגופים, קרי המנכ"ל או עובד בכיר הכפוף לו, היועץ המשפטי או נציגו, ועובד אחד לפחות בתחום ניהול ואבטחת מידע. ממילא, סביר שגורמים אלה (המנכ"ל והיועמ"ש או מי מטעמם) יהיו מעורבים בגיבוש ההסכם. כמו כן, הסכם להעברת מידע יהיה טעון התייעצות עם הממונים על הגנת הפרטיות של הגופים הציבוריים.

4. <u>ועדה מרכזית לאישור העברות מידע אישי בין גופים ציבוריים :</u> מוצע להקים ועדה מרכזית להעברת מידע אישי בין גופים ציבוריים, שתוסמך להתיר העברות מידע אישי בין יותר משני גופים ציבוריים ובכלל זה לתת היתר להעברות מידע הנדרש לטובת טיפול בסוגיות לאומיות רוחביות. הוועדה תורכב מנציגי הגורמים הבאים :

---

[45] דוגמה לכך יכולה להיות אגרגציה של נתונים, והחלפת נתונים מדויקים בקטגוריות אגרגטיביות. (במקום לציין שגיל של אדם מסוים הוא 57, ניתן לומר שהוא שייך לקבוצת גיל 50-60, כמובן בנוסף למחיקת מזהים ישירים).

1) מערך הדיגיטל הלאומי, והוא יהיה יושב הראש;
2) משרד ראש הממשלה;
3) מערך הסייבר הלאומי;
4) הרשות להגנת הפרטיות;
5) הממונה על התקציבים במשרד האוצר;
6) היועצת המשפטית לממשלה.

תפקידה של הוועדה יהיה מתן אישור להעברת מידע אישי בין יותר משני גופים ציבוריים המוסרים ומקבלים את המידע (אישור מרכזי). אישור מרכזי יינתן על ידי הוועדה המרכזית לאחר שקיבלה את התשתית העובדתית הנדרשת לשם קבלת ההחלטה מהגופים הציבוריים שמבוקש לאשר להם להעביר ולקבל את המידע האישי. הוועדה תיתן הזדמנות לכל גוף ממנו מתבקש לאשר העברת מידע להשמיע את עמדתו בפניה, אולם לגבי גופים שמבוקש לאשר להעביר אליהם מידע, ככל שמדובר בגופים רבים בעלי מאפיינים דומים (כגון רשויות מקומיות) לא תהיה הוועדה מחויבת לעמוד בקשר עם כל הגופים, והיא תפעיל את שיקול דעתה לעניין הגורמים הרלוונטיים מצד הגופים מקבלי המידע אותם נכון לשמוע. ככלל בהחלטת הוועדה יוסדרו כל הנושאים שנדרש להסדיר במסגרת החלטת הוועדות להעברות מידע אישי, אולם הוועדה המרכזית תהיה רשאית לאשר העברת מידע ללא הסדרה של ממשק העברת המידע ואופן אבטחתו. במקרה זה, יוסדרו נושאים אלה בין הגופים המקבלים ומעבירים את המידע.

5. <u>העברת מידע מותמם במנגנון התממה טכנולוגי דוגמת קופסה שחורה:</u>
מנגנון התממה דוגמת קופסה שחורה הוא מנגנון טכנולוגי הפועל באמצעות מערכת מחשוב מופרדת לחלוטין המקבלת מידע משני מקורות שונים או יותר, מצפינה אותם ואז מבצעת הצלבה ביניהם, בכדי להפיק מההצלבה נתון סטטיסטי בלתי ניתן לזיהוי, ואז מוחקת את הנתונים הגולמיים, וכל זאת מבלי שעין אנושית חשופה למידע הגולמי. על מנגנון מסוג זה לעמוד בתנאי מחמיר, לפיו המנגנון מונע, מבחינה טכנולוגית, את האפשרות לזיהוי מי שהמידע הוא עליו בהינתן עמידה בתנאים של אותו מנגנון, וכי אבטחתו תהיה בסטנדרט גבוה לפחות ברמה המתאימה למידע בעל הרגישות הגבוהה ביותר המועבר באמצעותו. מוצע לקבוע כי ככל שייושם מנגנון התממה כאמור, והמנגנון יופעל על ידי גורם ממשלתי שאינו מוסר המידע או מקבלו (דוגמת מערך הדיגיטל הלאומי), יהיה ניתן להתייחס אליו ככזה שההסדר לא חל עליו, גם אם באופן תיאורטי יוכל אותו גורם ממשלתי, שלא כדין, לנסות ולפענח את זהות מי שהמידע הוא עליו.[46] יובהר כי האמור מכוון רק לכך שיהיה ניתן להעביר מידע אישי במנגנון האמור ללא אישור העברת המידע באחד מהמתווים המפורטים לעיל, וכי ההוראות המהותיות של סעיף 23ג ויתר הוראות הדין בנושא הגנת הפרטיות ואבטחת המידע והגנת סייבר ימשיכו לחול על מידע מסוג זה.

6. <u>שימור המסלול הקיים של הוועדות להעברת מידע אישי</u> - מוצע להותיר כאחת מהחלופות את מסלול האישור הקיים כיום, כך ששני גופים ציבוריים המעוניינים בכך, יוכלו להמשיך לאשר העברת מידע אישי ביניהם על ידי הוועדות להעברת מידע. השוני מהמצב הקיים יהיה שבעוד שעד כה היה מדובר

[46] דוגמה למנגנון כאמור הוא הצלבת מידע משני מקורות מידע, כאשר המידע המוצלב משני המקורות מקודד על ידי מפתח הצפנה המאפשר שחזור של המידע המוצפן, כאשר המפתח מוחזק על ידי צד ג' שהוא גוף ממשלתי אשר מתחייב לא לעשות בו שימוש. בהנחה שמבחינה טכנולוגית, ככל שלא יעשה שימוש במפתח לא יהיה ניתן להביא לזיהוי מי שהמידע הוא עליו, ותוך התחייבות חד משמעית שלא לעשות שימוש במפתח הקידוד, יהיה ניתן לראות במידע, לעניין העברתו, ככזה שאינו ניתן לזיהוי במאמץ סביר.

במסלול החוקי היחיד לאישור העברת מידע אישי, כעת מוצע לקבוע חלופות נוספות אשר פורטו לעיל, כך שתתאפשר לגופים בחירה בין החלופות השונות, בהתאם למאפיינים של אותה העברת מידע מבוקשת.

נוסף על האמור, מוצע ליישם צעדים שונים עליהם הוחלט בהחלטת ממשלה מס׳ 1933 לייעול עבודת הועדות, ואשר עד כה יושמו באופן חלקי בלבד. בין היתר, כפי שיפורט בהמשך, מוצע להשלים את תיקון תקנות הגנת הפרטיות כך שייקבעו מועדים מרביים לפרק הזמן בו מטפלות הוועדות בבקשות המובאות בפניהן (SLA), החזרה לפעילות של ועדת היגוי שתעסוק באופן רוחבי בהיבטים המנהליים של עבודת הוועדות, והטמעת מערכת חדשה לניהול הליך העברת המידע במקום מערכת מועד (מערכת "צ׳יטה", עליה יפורט בהמשך).

ב. <u>היבטים כלליים שנדרש להסדיר בכל אחד ממסלולי האישור המפורטים לעיל:</u>

1) המאפיינים הבסיסיים של העברת המידע האישי: נדרש לקבוע בין היתר את פרטי המידע שיועברו (שדות המידע וקבוצת האנשים לגביהם יועבר המידע) ואת סוג ההעברה ותדירותה (כגון העברה חד פעמית, עיתית או בממשק להעברת מידע בזמן אמת לפי שאילתות פרטניות, דוגמת ממשק API). קביעת מאפיינים אלה תיעשה תוך עיצוב העברת המידע לפרטיות, ובכלל זה כך שלא יועבר ולא ישמר מידע מעבר למידע המינימאלי הדרוש לשם הגשמת התכלית, ותוך העדפה ליצירת ממשקים מקוונים בין מאגרי מידע על פני שכפול מאגרי מידע.[47]

2) היבטים הנוגעים לממשק העברת המידע האישי, לאבטחת המידע ולהגנה עליו לאחר העברתו ובמהלכה: נדרש לקבוע את הממשק או האמצעי באמצעותו יועבר המידע האישי ואת היבטי אבטחת המידע והגנת הסייבר בממשק זה, וכן את היבטי אבטחת המידע והגנת הסייבר, ובכלל זה הרשאות הגישה למידע האישי, לאחר העברתו. ראו בהמשך פירוט לגבי מסמך הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים.

3) יש ליידע את הממונים על הגנת הפרטיות בגוף מקבל המידע ובגוף מוסר המידע לגבי כל אישור להעברת מידע אישי שניתן לפי כל אחד ממסלולי האישור שלא כרוכים בהתייעצות עם הממונים.[48]

4) דיווח על העברת מידע ביומטרי:

מוצע לקבוע שמשרדי ממשלה ויחידות סמך המעבירים מידע ביומטרי יידעו אודות ההעברה את הממונה על היישומים הביומטריים במערך הסייבר הלאומי. זאת, על מנת לאפשר לממונה להפעיל את סמכותה לפי החלטות הממשלה בנוגע ליישומים ולמאגרים ביומטריים להם נועד

[47] דוגמאות לאופנים בהם עיצוב לפרטיות של העברת מידע יכולה להפחית את עוצמת הפגיעה בפרטיות:

1. מסירת תשובה בינארית לגבי אדם, האם מתקיים לגביו כלל כלשהו או לא. למשל, כאשר נדרש לדעת האם אדם עומד במבחן הכנסה מסוים לקבלת זכות, הטבה וכו׳, ניתן לערוך את מבכן ההכנסה בגוף מוסר המידע, ולמסור למבקש המידע רק האם האדם עומד או לא עומד במבחן, מבלי למסור את המידע על הכנסותיו עליו מבוססת הקביעה (בתנאי שמדובר בקביעה טכנית שאינה כרוכה בהפעלת שיקול דעת בידי מקבל המידע).
2. כאשר מידע אישי מועבר לשם הצלבתו עם מידע אישי ממקור אחר לטובת הפקת נתון מצרפי (אגרגטיבי), שנועד לשמש להפקת סטטיסטיקה או לקבלת החלטות המבוססות על נתונים. במקרה כזה, ככל הניתן, עדיף להצליב את המידע במנגנון של "קופסה שחורה" שפורט לעיל. לחלופין או בנוסף, ככל שהמידע האישי הפרטני לא נדרש להגשמת התכלית, יש לעצב את העברת המידע כך שלאחר הצלבת המידע האישי הוא ימחק לחלוטין ממערכות מקבל המידע, כך שברשותו יוותר רק מידע מצרפי שאינו ניתן לזיהוי במאמץ סביר.
3. כאשר תהליך שירות דיגיטלי בגוף ציבורי דורש קבלת נתון מסוים אודות מקבל השירות מגוף ציבורי אחר, נכון ככלל לעצב את העברת המידע כממשק מקוון את מערכות שני הגופים (API) כך שרק כאשר ניתן בפועל שירות לאדם מסוים מועבר הנתון אודותיו לגוף נותן השירות, ללא העברה גורפת של כל הנתונים במאגר המידע.

[48] ר׳ סעיפים 17ב1 ו – 17ב2 לחוק הגנת הפרטיות בנוסחו לאחר תיקון מס׳ 13 לעניין החובה למנות ממונה על הגנת הפרטיות ולעניין תפקידיו של הממונה.

המידע המועבר.[49] לשם כך, מוצע כי החובה תחול כאשר המידע המועבר משמש או נועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב, קרי לצורך יישום ביומטרי בהתאם להגדרת מידע ביומטרי הנכלל בהגדרה של מידע בעל רגישות מיוחדת כפי שזו נקבעה בתיקון מס' 13 לחוק הגנת הפרטיות,[50] וכן כאשר העברתו יוצרת מאגר מידע ביומטרי בעל היקף משמעותי ואפשרות לשיוך המידע לזהות אדם. זאת, מאחר שדליפה של מאגר מידע של מזהים ביומטריים בהיקף גדול, בפרט כאשר המידע משויך לזהות אדם (כלומר כאשר המידע הביומטרי מועבר לצד פרטי זיהוי כמו שם ומספר זהות), מהווה גורם סיכון גם אם המאגר עצמו לא מיועד ליישום ביומטרי.
לעניין אמת המידה להיקף המשמעותי של מידע ביומטרי, מוצע לקבוע כי חובת היידוע המוצעת תחול, כשמדובר בתמונות פנים או מאגר קולי, שאינם מיועדים לשימוש באמצעות יישום ביומטרי, על העברת מידע ביומטרי על 100,000 נושאי מידע או יותר (באופן חד פעמי או במצטבר). כאשר מדובר במידע ביומטרי מסוג אחר, כגון טביעות אצבע, שככלל כל העברה שלו מצביע על שימוש בו לצורך זיהוי ביומטרי, כל העברת מידע תהיה כפופה לחובת היידוע.
מוצע כי חובת היידוע לא תעכב את ביצוע ההעברה, אבל ידרש למלאה בסמוך לאחר קבלת ההחלטה על העברת המידע.

ג. <u>הבהרת הדין ביחס לתחולת ההסדר</u>:
בעבודת הצוות נמצא כי לעיתים גופים ציבוריים סבורים כי הדרישה לאישור העברת מידע אישי נוגעת גם לסוגי מידע שאינם מידע אישי, ולפיכך ההסדר הנוגע להעברת מידע אישי לא חל עליהם. מקרים כאלה פוגעים ביעילות עבודת הגופים הציבוריים ומביאים להליכים מיותרים הנוגעים למידע שהעברתו אינה פוגעת בפרטיות. לאור זאת, מוצע, במסגרת פעולות כלליות להגברת הידע בגופים הציבוריים אודות העברת מידע אישי, להבהיר את סוגי המידע שההסדר חל עליו, ובפרט להבהיר כי ההסדר חל רק על מידע אישי כהגדרתו בחוק הגנת הפרטיות.[51] בפרט, ההסדר לא חל על מידע אודות תאגידים, ועל מידע שלא ניתן לזהות במאמץ סביר, במישרין או בעקיפין, את מי שהמידע הוא עליו, כדוגמת מידע סטטיסטי ומידע שהותמם באופן מלא בהתאם למבחן האמור.

ד. <u>תיקון תקנות הגנת הפרטיות</u>:
יישום המסלולים החדשים לאישור העברת מידע אישי המפורטים להלן, יהווה שינוי של ההסדר הקבוע בתקנות הגנת הפרטיות, ובהתאם ידרוש תיקון שלהן. במסגרת תיקון זה, מוצע להטמיע גם את עיקרי ההמלצות שנקבעו לעניין תיקון התקנות בהחלטת ממשלה מס' 1933, ובכלל זה לעניין קביעת לוחות זמנים לעבודת הוועדות ולעניין התאמת דרישות אבטחת המידע לרגישות המידע המועבר. כן מוצע לכלול בתיקון לתקנות נושאים נוספים שנכללו בטיוטת התיקון לתקנות שהונחה על שולחן ועדת חוקה בכנסת הקודמת בעקבות החלטה 1933, ובכלל זה הסדרה של אופן אישור העברת מידע הדרוש לשם איתור והעברת מידע אחר ("נתוני תשאול") והסדר ייחודי הנוגע לרשויות הביטחון.

---

[49] החלטת ממשלה מס' 4510 מיום 01.04.2012 בנושא: "תפקידיו וסמכויותיו של הממונה על היישומים הביומטריים".
[50] פרט 4 להגדרה "מידע בעל רגישות מיוחדת" בסעיף 3 לחוק הגנת הפרטיות בנוסחו לאחר תיקון מס' 13 לחוק.
[51] כפי שצוין לעיל, עד לכניסתו לתוקף של תיקון מס' 13 לחוק הגנת הפרטיות, ההסדר חל על מידע כהגדרתו בסעיף 7 לחוק וכן על ידיעות אודות ענייניו הפרטיים של אדם, תחולה שבמהותה היא דומה.

ה. <u>מערכת לניהול תהליך אישור העברת המידע האישי</u>

בימים אלו מפותחת על ידי מערך הדיגיטל הלאומי מערכת "צ'יטה" אשר תחליף את מערכת מועד כמערכת לניהול תהליכי האישור להעברת מידע אישי בין גופים ציבוריים. למערכת צ'יטה הוכנסו מגוון מאפיינים, שאינם קיימים במערכת מועד, שמטרתם לייעל ולשפר את חוויית המשתמש ובכלל זאת, גנריקה של טפסים, קטלוג של שדות מידע קיימים ושל מקורות סמכות משפטית להעברת מידע, וצ'טבוט לתמיכה ומילוי אוטומטי של שדות. מאפיינים אלו יסייעו בין היתר לשימור ידע על אודות הגשת בקשות קודמות להעברת מידע, אשר זוהה כחסם משמעותי בגילוי ואיתור נתונים. כמו כן, מוטמעים במערכת צ'יטה מאפיינים המאפשרים ניתוח מהיר של המטא-דאטה של הבקשות, כך שיתאפשר זיהוי של נקודות כשל בתהליך, לרבות זיהוי קשיים וחסמים של מוסרי ומבקשי מידע.

על אף האמור, יצוין כי מערכת צ'יטה מבוססת על ההסדר החוקי הקיים הן מבחינת השדות המחויבים במילוי כפי שמפורט בתוספות לתקנות, והן מבחינת מסלול אישור ההעברה הקיים באמצעות הוועדות להעברות מידע. עם תיקון תקנות הגנת הפרטיות כאמור בסעיף קטן ד' לעיל, והוספת מסלולי אישור נוספים להעברות מידע אישי, יהיה צורך לעדכן את המערכת, כך שיוטמעו בה מסלולי האישור החדשים המוצעים והדרישות הרוחביות הנוגעות לכל מסלולי העברת המידע.[52]

סיכום ההמלצות לשלב אישור העברת המידע האישי:

1. <u>קביעה של מסלולים נוספים לאישור העברת מידע אישי בהתאם לתנאים המפורטים לעיל</u>:
   (א) מסלול להעברת מידע בסיסי (Basic Data);
   (ב) מסלול להעברת מידע אישי על סמך אישור מבקש המידע;
   (ג) הסכמי העברת מידע אישי;
   (ד) ועדה מרכזית לאישור העברת מידע אישי בין גופים ציבוריים;
   (ה) העברת מידע מותמם במנגנון התממה טכנולוגי דוגמת קופסה שחורה;
   (ו) שימור המסלול הקיים של הוועדות להעברת מידע אישי.
2. <u>קביעת היבטים כלליים שנדרש להסדיר בכל אחד ממסלולי האישור המפורטים לעיל</u>:
   (א) המאפיינים הבסיסיים של העברת המידע;
   (ב) היבטים הנוגעים לממשק העברת המידע ולאבטחת המידע והגנת סייבר בכל שלבי העברת המידע;
   (ג) יידוע של הממונים על הגנת הפרטיות בגוף המוסר ובגוף המקבל.
   (ד) קביעת חובת יידוע על העברת מידע ביומטרי של הממונה על היישומים הביומטריים.
3. הבהרת הדין ביחס לתחולת ההסדר.
4. עיגון הסדרים אלה בתיקון לתקנות הגנת הפרטיות, אשר במסגרתו יכללו גם עיקרי ההסדרים שהוצעו בטיוטת התיקון שהוכנה בעקבות החלטת הממשלה מס' 1933.

---

[52] לעניין מערכת זו הוחלט בסעיף 13(ג) להחלטה 2273:
"(ג) פלטפורמה עדכנית לניהול תהליכי אישורי העברת המידע – להטיל על ראשת מערך הדיגיטל הלאומי להקים, בתוך 12 חודשים, פלטפורמה מעודכנת ורוחבית לניהול תהליכי הנפקת אישורי העברות המידע באופן דיגיטלי, המפורטים בסעיף 12 להחלטה זו, ולחבר פלטפורמה זו לקטלוג המידע המפורט בסעיף קטן (א) לעיל".

5. פיתוח מערכת לניהול תהליך אישור העברת המידע (מערכת צ׳יטה).

3. שלב מימוש העברת המידע האישי:

על מנת לספק מענה לצורך במימוש יעיל של הליכי העברות מידע אישי סבור הצוות כי יש להציע פתרונות טכנולוגיים המורכבים משלושה נדבכים מרכזיים: מערכת לניהול תהליך אישור העברת המידע כמפורט לעיל (מערכת צ׳יטה); תשתיות טכנולוגיות מרכזיות לשיתוף מידע, ופלטפורמות משלימות המאפשרות אנליזה של מידע ממגוון מקורות תוך שימוש בטכנולוגיות מגבירות פרטיות (״**PETs**״).[53] על מנת לייצר תהליך רציף ואוטומטי ככל הניתן, יש לייצר ממשקים טכנולוגיים ודיגיטליים בין שלושת הנדבכים הללו.

א. תשתיות העברת מידע מרכזיות:

הנדבך השני לשיפור התהליכים הטכנולוגיים להעברות מידע, לאחר שלב אישור העברת המידע באמצעות מערכת צ׳יטה המפותחת לצורך זה, נוגע לתשתיות העברת המידע.

העברת מידע יכולה להתבצע בין גורמים אנושים, בין מערכות מידע (לרבות מערכת לאפליקציה), וכן בין מערכות לבין גורמים אנושיים. ישנן מגוון שיטות טכנולוגיות להעברת מידע באופן דיגיטלי ובכלל זאת:

ממשק מחשב למחשב (API)[54] – שיטה זו רלבנטית בעיקר כאשר יש צורך לייצר אוטומציה בתהליך או שירות מסוים, בהעברת מידע בין מערכת מידע למערכת מידע, וכן כאשר יש צורך בהעברת מידע בזמן אמת בין גוף שברשותו המידע למבקש מידע. הפלטפורמה המרכזית שקיימת כיום במגזר הציבורי היא שדרת המידע הממשלתית. לשדרת המידע מחוברים כיום מרבית משרדי הממשלה, וחלק ניכר מהתאגידים הסטטוטוריים והרשויות המקומיות (בין היתר באמצעות ספקיות התוכנה עימן התקשרו).

פלטפורמות לשיתוף קבצים (MFT)[55] – גישה זו מאפשרת שיתוף קבצים בפלטפורמות מאובטחות. ככלל, הפלטפורמות מתאימות לצרכי העברת נתונים ומידע שאינו בזמן אמת. כיום במגזר הציבורי נפוצה הטכנולוגיה של העברת מידע באמצעות מערכת ״כספות״, אך ישנם מוצרים חדשים יותר לרבות כלים בענן הממשלתי.[56]

אגמי מידע – גישה נוספת להעברת מידע היא איגומו באופן מרכזי על ידי מספר בעלי עניין במידע, תוך ניהול ההרשאות. לרוב, המידע יאוגם בענן הממשלתי.

הבחירה בין תשתיות שיתוף המידע תלויה, בין היתר, בצורך במידע, ברגישות ובסוג המידע, בנפח המידע ובתדירות הנדרשת של עדכונו. כאשר נדרש שיתוף מידע קרוב לזמן אמת לצורך מוגדר וידוע מראש מוצע להשתמש בממשק API בשדרת המידע. לעומת זאת, כאשר מדובר בנפח גדול של מידע שאינו נדרש בזמן אמת, פלטפורמות לשיתוף קבצים תהינה מתאימות יותר.

---

[53] Privacy Enhancing Technology
[54] Application Programming Interface
[55] Managed File Transfer
[56] כגון המוצר ״Go Anywhere״, אשר מאפשר העלאת קבצים לענן.

לצד אלו ניתן לבצע העברות מידע, בפלטפורמות נוספות כגון Google Drive בתשתית "ענן" ממשלתית, ותיבת דואר אלקטרוני ארגוני.

מומלץ כי מערך הדיגיטל הלאומי יכין תוכנית עבודה לחיבור לתשתיות העברת המידע המרכזיות שפורטו לעיל של גופים ציבוריים שטרם התחברו אליהן.[57]

שימוש בפלטפורמת מרכזיות לשיתוף מידע צפוי לייעל תהליכים, לחסוך משאבים ולקצר את זמני העברות המידע משום שבפלטפורמות אלו הוסדרו מראש סוגיות שונות הקשורות להיבטים הטכניים של העברת מידע, לרבות סוגיות של אבטחת מידע והגנת סייבר. לאור זאת, מומלץ לקבוע כי ממשקים חדשים להעברת מידע בין גופים ציבוריים יפעלו באמצעות תשתיות שיתוף המידע המרכזיות (בגופים המחוברים לתשתיות אלה).

בהמשך לאמור, וכדי לסייע בחיבור הגופים הציבוריים לפלטפורמות המרכזיות להעברת מידע ובשימוש בהן, מוצע להקים צוות ייעודי במערך הדיגיטל הלאומי שיסייע לגופים הציבוריים לפתח את הממשקים הדרושים לכך. מוצע שהצוות יפעל לפי תיעדוף שיקבע בשיתוף עם משרד ראש הממשלה, אגף התקציבים במשרד האוצר והמשרדים הרלוונטיים, ויבצע פרויקטים לחיבור המשרדים המרכזיים לפלטפורמות שיתוף המידע המרכזיות, תוך ליווי המשרדים בביצוע פרויקטים הקשורים לניהול הנתונים ומאגרי המידע המנוהלים על-ידם. הצוות יורכב מאנשי מקצוע בעלי מומחיות בתחומי הנתונים. במידה וישנם מאגרים אשר מחוברים באופן שוטף או בתהליך חיבור לאגם המידע הממשלתי, ישנה עדיפות לחיבור לממשק הקיים על פני יצירת ממשקים חדשים.

נוסף על האמור, יש לייצר **ממשקים** בין תהליך איתור המידע האישי, לקבלת אישור להעברת המידע (באמצעות מערכת צ׳יטה), עובר לקבלת ההרשאה להעברת המידע, והעברתו בפועל. כך שמתן אישור להעברת המידע יוביל באופן אוטומטי או אוטומטי למחצה למתן הרשאה טכנית לשלוף את המידע מהממשק הרלבנטי, כל זאת תוך ניהול מנגנוני הרשאות ושימוש בכלים טכנולוגיים ורובוטיים (טכנולוגיות RPA), כגון תהליכי אוטומציה ושליפה אוטומטית של נתונים. השקעה בפיתוח ממשקים אלו צפויה להפחית את זמני העברת המידע. הישימות של פיתוח ממשק כאמור תיבחן על ידי מערך הדיגיטל הלאומי בעת פיתוח המערכות הרלוונטיות.

ב. <u>פלטפורמות אנליזה משלימות</u>

כאמור, הנדבך השלישי הנחוץ לשיפור התהליכים הטכנולוגיים נוגע ליכולות אנליזה של מידע לפי שאילתות מגוונות בתחום הפקת הסטטיסטיקה ואיסוף מידע לצורך קבלת החלטות מבוססות נתונים. כיום, על מנת לבצע עיבוד של מידע אישי ממקורות שונים במגזר הציבורי, למשל לצורך מענה על שאילתות מורכבות, יש צורך בתהליכים עתירי משאבים. לעיתים נדרש להשמיט באופן "ידני" מידע שאינו נדרש ולעיתים נוצר מצב של העברת מידע עודף בשל העדר יכולת ל"סנן" את המידע המבוקש. עם זאת, בשנים האחרונות חלה התפתחות משמעותית בפיתוח פלטפורמות לשיתוף, עיבוד וניתוח מידע, תוך הטמעת טכנולוגיות מגבירות

[57] הכוונה לכלל הפלטפורמות המנויות לאורך הדו"ח: קטלוג מידע ממשלתי, מערכת צ׳יטה, מנגנון התממה טכנולוגי, מערכות אנליזה משלימות ומערכת לניהול הסכמות.

פרטיות (PETs).[58] לפיכך, מומלץ כי מערך הדיגיטל הלאומי יפתח פלטפורמות רוחביות המבוססות על שליפה מבוזרת של נתונים ויגיש אותם ככלי למאגרי מידע הנמצאים במשרדים אחרים, תוך יישום מרכיבים המתממימים את המידע באופן אוטומטי. נוסף על כך, מומלץ לפתח פלטפורמות המאפשרות יצירת מידע סינתטי.[59]

נציין שתי דוגמאות המצויות בימים אלו בשלבי ייזום ואפיון על ידי מערך הדיגיטל הלאומי, בשיתוף עם גופים שונים:

- <u>פלטפורמת "רקמ"ה"</u>: רשת לקידום מדעי הנתונים - רשת מבוזרת של אגמי נתונים נושאיים ומשרדיים המאפשרת הנגשת נתוני עתק בין משרדים לחוקרים מתוך הממשלה, מהתעשייה ומהאקדמיה לצורך ביצוע מחקרים ולטובת קבלת החלטות וקביעת מדיניות של גופים ציבוריים. המערכת תאפשר גישה למידע שמקורו במערכות תפעוליות של משרדי ממשלה שונים, ותדע להתמודד הן עם נתונים מובנים (structed dataוהן עם נתונים שאינם מובנים כגון טקסט חופשי, קבצי אודיו ווידאו. פלטפורמת רקמ"ה תוכל לשלב מידע ממגוון רחב של תחומים בהם עוסק המגזר הציבורי. על מנת לאפשר ביצוע מחקרים מתקדמים ולמנוע פגיעה בפרטיות, המערכת תאפשר הנגשה של מידע סינטטי וכן הנגשת מידע מותמם. השימוש בפועל במערכת כפוף לבחינה משפטית שהתממת המידע עומדת באמת המידה הנדרשת לכך, והיא שהמידע הסינטטי והמידע המותמם אינם ניתנים לזיהוי במאמץ סביר, וכן בנקיטה באמצעים משפטיים, תהליכיים וטכנולוגיים נוספים לצמצום אפשרות הפגיעה בפרטיות.[60]

- <u>מערכת "מחל"ף"</u>: מזעור החשיפה לנתוני פרט - תשתית מחשוב לשאילתות מבוזרות, המאפשרת למשרדי הממשלה לתת מענה מיידי לשאילתות הנוגעות למידע המאוחסן במספר משרדים שונים, מבלי לאגם את כלל המידע למקום מרכזי אחד, תוך שימוש במנגנוני הצפנה מתקדמים ומזעור הסיכון לפגיעה בפרטיות. מערכת מחל"ף תוכל לספק מענה אגרגטיבי ללא חשיפה לנתוני פרט, וכן תוכל לספק מענה לשאילתות פרטניות תוך שמירה מקסימלית על פרטיות המידע.

- מומלץ כי מערך הדיגיטל הלאומי יפעל להשלמת פיתוח הפלטפורמות האמורות, אשר צפויות להעצים את יכולות התפעוליות הבינית (Interoperability) בכל הנוגע לשיתוף מידע בין מערכות ובין גורמים אנושיים בקרב המגזר הציבורי, להפחית את הנטל המבוזר הכרוך כיום בשימוש בממשקים להחצנת המידע ולקצר את זמני העברת המידע. פיתוח המערכות יושלם בתוך 12 חודשים ממועד קבלת החלטת ממשלה מספר 2273, בהתאם לקבוע בה.[61] כן מוצע כי החיבור למערכות אלו יתבצע על פי תיעדוף של מערך הדיגיטל

---

[58] EMERGING PRIVACY ENHANCING TECHNOLOGIES: CURRENT REGULATORY AND POLICY APPROACHES, OECD DIGITAL ECONOMY PAPERS, March 2023

[59] מידע שנוצר באופן מלאכותי וממוחשב, המשמר את המאפיינים הסטטיסטיים של אוכלוסיית המידע, והוא נטול תוכן מזהה.

[60] ר' הגדרת "מידע אישי" בתיקון מס' 13 לחוק הגנת הפרטיות, התשמ"א, 1981.

[61] לעניין מערכות אלה, הוחלט בסעיף 13(ד) להחלטה 2273:

"(ד) פלטפורמת שיתוף נתונים אחודה – להקים בתוך 18 חודשים תשתית טכנולוגית המאפשרת לבצע שליפה והצלבות מידע מזוהה ושאינו מזוהה בהתאם לאמצעי הגנת הסייבר ואבטחת המידע הנדרשים, לרבות מידע מותמם ומידע סינטטי ממגוון מקורות, ולהחצין את תוצרי הניתוח לצרכנים שונים מקרב הגופים הציבוריים, בהתאם לכל דין. במסגרת פיתוח פלטפורמה זו, יפותחו ממשקים המאפשרים אוטומציה חלקית או מלאה בין תהליך האישור הבירוקרטי של צריכת המידע לבין צריכתו בפועל. שיתוף המידע בתשתיות ייעשה לאחר בחינה משפטית כי השיתוף אפשרי בהתאם לכל דין. השימוש בתשתית ושיתוף המידע יהיה נתון לבחירת הגופים הציבוריים. על גבי פלטפורמה זו יפותחו היישומים הבאים:

1) מערכת מזעור החשיפה לנתוני פרט ("מחל"ף") –

הלאומי בתיאום עם משרד ראש הממשלה ואגף תקציבים במשרד האוצר.

נוסף על פיתוח המערכות האמורות, מומלץ כי מערך הדיגיטל הלאומי ירכז בחינה רוחבית של טכנולוגיות ומתודולוגיות קיימות להתממת מידע במשרדי הממשלה, ויממש את הטכנולוגיות והמתודולוגיות באופן רוחבי ויפעל להנגשתן לגופים הציבוריים, בנסיבות שבהן הדבר מתאים.

מעבר לאמור לעיל, טכנולוגיות מידע חדשניות מאפשרות לצמצם באופן ניכר את היקף החשיפה האנושית למידע אישי, מאחר שמערכות אלו מאפשרות אוטומציה במתן שירותים ממשלתיים, תוך הפחתת התערבות גורם אנושי.

סיכום ההמלצות לשלב מימוש העברת המידע:

1. מערך הדיגיטל יכין תכנית עבודה לחיבור גופים ציבוריים לתשתיות העברת המידע המרכזיות.
2. להקים צוות ייעודי במערך הדיגיטל הלאומי שיסייע לגופים הציבוריים לפתח את הממשקים הדרושים לשם קישור מאגרי המידע המרכזיים שלהם לתשתיות העברת המידע המרכזיות ולשימוש בהן.
3. יצירת ממשקים בין התהליך איתור המידע, קבלת אישור להעברת המידע (באמצעות מערכת צ׳יטה) והעברת המידע בפועל.
4. מערך הדיגיטל הלאומי ישלים את פיתוחן של מערכות אנליזה משלימות לטובת הפקת סטטיסטיקה ואיסוף מידע לצורך קבלת החלטות מבוססות נתונים: רשת לקידום מדעי הנתונים (פלטפורמת רקמ״ה) ותשתית מחשוב לשאילתות מבוזרות (מערכת מחל״ף). בנוסף, המערך ירכז בחינה רוחבית של טכנולוגיות ומתודולוגיות קיימות להתממת מידע במשרדי הממשלה.

<u>4. הנחיות אבטחת המידע והגנת סייבר בהעברת מידע בין גופים ציבוריים:</u>

תיאומים בין מוסרי המידע למבקשי המידע בדבר האופן בו יאובטח המידע בעת העברתו ולאחר העברתו בעת שמירתו בגוף המקבל, הם מרכיב בתהליך העברת המידע בין גופים ציבוריים אשר כרוך לעיתים בנטל רב על שני הצדדים. נטל זה בא לידי ביטוי בצורך בשיח בין שני הגופים בו יקבעו ההוראות הפרטניות הנוגעות לאבטחת המידע, כך שיתאימו הן לדרישות הגוף מוסר המידע והן למאפייני מערכות המידע של הגוף מקבל המידע. ככל שנקבעו תנאים שאינם תואמים ליכולות הנוכחיות של שני הגופים, נדרש בנוסף, בשלב מימוש העברת המידע,

---

א) לפתח בתוך 12 חודשים תשתית מחשוב לשאילתות מבוזרות, המאפשרת לגופים ציבוריים לתת מענה מיידי לשאילתות הנוגעות למידע המאוחסן במספר גופים ציבוריים שונים, מבלי לאחסן את כלל המידע במקום מרכזי אחד ותוך מזעור הסיכון לפגיעה בפרטיות, לעיתים עד כדי העלמת הסיכון, בין היתר על ידי מתן תשובות של מידע אגרגטיבי ולא מזוהה.
ב) להטיל על המשרדים המופיעים בסעיף קטן (א)(3)(א) להנגיש את המאגרים המופיעים בסעיף זה במערכת מחל״ף וללמ״ס בתוך 18 חודשים ממועד אישור החלטה זו.

2) רשת לקידום מדעי הנתונים (״רקמ״ה״) – להקים, בתיאום עם החשב הכללי במשרד האוצר ובתוך 12 חודשים, רשת מבוזרת של אגמי נתונים נושאיים ומשרדיים המאפשרת הנגשת נתוני עתק בין-משרדיים לחוקרים מתוך המגזר הציבורי, מהתעשייה ומהאקדמיה, לצורך מחקרים פורצי דרך. פתרון מבוזר זה משלים את הפתרון המרכזי שיינתן באמצעות אגם המידע הממשלתי, ומאפשר נגישות לנתוני עתק מפורטים הנמצאים במשרדים. התשתית תאפשר לבצע מחקרים מתקדמים, תוך שילוב בין הנגשת מידע גולמי, הנגשת מידע מותמם (de-identified Data) והנגשת מידע סינתטי שאינו מידע כהגדרתו בחוק הגנת הפרטיות.

3) להטיל על הלמ״ס להמשיך ולפתח תשתיות מחשוב לשאילתות המבוססות על נתונים קיימים בלמ״ס, ולהציג פיתוח ראשון בתוך 12 חודשים, תוך מזעור הסיכון לפגיעה בפרטיות, ועיתים עד כדי העלמתו, בין היתר על ידי מתן מידע אגרגטיבי שאינו מזוהה״.

לפתח יכולות אלה.

בדיוני הצוות עלה כי לפחות לחלק משמעותי בהסדרה של היבטי אבטחת המידע והגנת הסייבר בעת העברת מידע בין גופים ציבוריים ניתן לערוך סטנדרטיזציה, ובכך להפחית את הנטל הכרוך בהסדרה פרטנית אגב העברת מידע. זאת, בין היתר בשים לב לכך שבתחום אבטחת המידע והגנת הסייבר קיימות מספר מסגרות של הנחיות החלות באופן רוחבי על כל הגופים הציבוריים או חלק מהם. כך, על כל הגופים הציבוריים חלות הוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017 (להלן: תקנות אבטחת מידע), כאשר לפי התקנות כל גוף ציבורי מחויב לאבטח את המידע האישי שבמאגריו לפחות ברמת האבטחה הבינונית, כהגדרתה בתקנות. נוסף על כך, כפופים משרדי הממשלה להנחיות היחידה להגנת הסייבר בממשלה (יה"ב) במערך הדיגיטל הלאומי, יחידה הכפופה מקצועית להנחיות מערך הסייבר הלאומי.[62] משכך, משרדי הממשלה כפופים ככלל לסטנדרט אחיד יחסית בתחום אבטחת המידע והגנת הסייבר.

במסגרת עבודת הצוות, פעל צוות משנה ליצירת סטנדרטיזציה כאמור בתחום אבטחת המידע והגנת הסייבר בעת העברת מידע בין גופים ציבוריים. צוות המשנה הובל על ידי הגורמים הממשלתיים האמונים על תחומים אלה – הרשות להגנת הפרטיות, מערך הסייבר הלאומי ויה"ב. כחלק מעבודה זו, גם גובשה שפה משותפת, המאפשרת לסנכרן בין רמות הרגישות של סוגי המידע לפי הדינים וההנחיות הרלוונטיות.

צוות המשנה גיבש מסמך הנחיות הקובע סטנדרט אחיד לגבי מכלול ההוראות בתחום אבטחת המידע והגנת הסייבר שיש לעמוד בהן בהתאם לסוג המידע המועבר בין גופים ציבוריים. זאת, תוך התייחסות פרטנית לפלטפורמות הממשלתיות הרוחביות בתחום העברת המידע, כך שלגבי כל אחת מהן יובהר אילו הוראות בסטנדרט מקבלות ממילא מענה בשל השימוש באותה פלטפורמה. פעולה לפי הסטנדרט המוצע תחסוך את השיח בין הגופים בנושא אבטחת מידע והגנת הסייבר, ובכך תקצר את הליך האישור להעברת המידע, ויתכן שגם לחסוך פיתוח אמצעי אבטחת מידע והגנת סייבר חדשים, באמצעות שימוש באמצעים סטנדרטיים קיימים.

בכל הנוגע למידע אישי, ההוראות המפורטות במסמך ההנחיות הן הוראות הנובעות ישירות מתקנות אבטחת מידע, למעט ההוראה במסמך לעניין סינון מידע טרום העברה, ובהתאם הן מחייבות את כלל הגופים הציבוריים בהעברת מידע אישי ביניהם.[63].

מסמך הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים מובא ב__נספח ב'__.

סיכום ההמלצות בנוגע לסטנדרטיזציה של היבטי אבטחת המידע:

1. לאמץ את מסמך הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים.

[62] מערך הסייבר הלאומי, בתורו, הוא הקצין המוסמך לגבי הגופים המנויים בתוספת החמישית לפי החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח – 1998.

[63] ההוראה לעניין סינון מידע לפני העברתו תחול כהוראה מחייבות את הגופים הכפופים להנחיית מערך הסייבר הלאומי ויה"ב, ותהווה בגדר המלצה מקצועית (Best Practice) לגבי יתר הגופים הציבוריים.

2. עדכניות ההוראות במסמך ההנחיות תיבחן מעת לעת על ידי ממערך הסייבר הלאומי, הרשות להגנת הפרטיות ויה״ב, ולכל הפחות אחת לשנתיים או בעת הטמעת מערכת מרכזית חדשה להעברת מידע בין גופים ציבוריים.

5. מדיניות כלכלית ותקציבית בהעברת מידע בין גופים ציבוריים:

כמתואר בדוח עד כה, הפקת מידע ומסירתו על ידי משרד ממשלתי דורשת מצדו השקעת תשומות באופן משתנה, בין היתר בהתאם למערכות והתשתיות הקיימות במשרד, היכרות מוקדמת עם מאגר המידע, גודל הבקשה והיקפה, ואמצעי העברת המידע הנדרשים. מערכות מורכבות, חוסר אוטומציה או תשתיות טכנולוגיות מיושנות עשויים להגדיל את עלות ההפקה. בנוסף, בקשות מורכבות או רחבות דורשות משאבים רבים יותר, כמו כוח אדם, זיכרון ותשתיות טכנולוגיות, המשפיעות על סך עלות התהליך.

לצד זאת, במקרים רבים, המשרד שמפיק את המידע או אחראי לאיסופו נחשב **למונופול בתחום המידע**, משום שאין גופים נוספים המחזיקים במידע זה באותה רמת מהימנות והיקף. מצב זה יוצר תלות מוחלטת של הגוף המבקש בגוף המספק את המידע, מכיוון שאין תחרות או אלטרנטיבות. התוצאה של תשומות הנדרשות בהפקת המידע ומשרד יחיד שיכול להפיק את המידע היא מצב שבו המשרד המחזיק במידע מחזיק גם בכוח משמעותי המשפיע על התמחור, הזמינות וזמני אספקת המידע. **העדר תמריץ כלכלי הופך לחסם בהעברות מידע** אם אין כנגדו תשלום הולם.

בהחלטת ממשלה מס׳ 1933, הוחלט כי **משרדי ממשלה לא ייגבו תשלום** זה מזה עבור העברת מידע, למעט במקרים מסוימים בהם נעשתה גבייה במסגרת תקציב מותנה הכנסה או השתתפות. החלטה זו נועדה לעודד שיתוף פעולה בין המשרדים ולהסיר חסמים כלכליים המונעים העברת מידע חיוני לתפקוד תקין של הממשל. זאת למעט עבור העברת מידע שעד למועד ההחלטה זו גבה המשרד בגינה תשלום במסגרת מתקציב מותנה הכנסה או השתתפות. מצב זה יוצר תמריץ שלילי מצידו לשתף פעולה ולהעביר את המידע למשרד המבקש. מכיוון **שהמשרד המוסר לא זוכה לפיצוי כספי** עבור העלויות שהושקעו בהפקת המידע, ישנה סבירות גבוהה לכך שהמשרד יראה בכך מטלה נוספת ויעדיף להימנע מהעברת המידע, או יתעדף אותה בעדיפות נמוכה, גם כאשר היא הכרחית לפעילות הממשלתית הכוללת. במצב הנוכחי, הן בשל מודלי SaaS המאפשרים תשלום בהתאם לביצוע והן בשל האפשרות להעסיק עובדי מחשוב בהעסקה גמישה בהתאם לצורך במסגרת מכרזים כמו מכרז נתוני שירותים, ישנה אפשרות לשייך עלויות לפעולות ספציפיות ולהקצות משאבים באופן גמיש בהתאם לביקוש.

כאשר מדובר בגופים ציבוריים העובדים מול הממשלה, אין איסור בגביית תשלום, כך שבמקרים מסוימים נוצר סבסוד צולב בו גובים תשלום מרשויות מקומיות או מגופים ציבוריים אחרים, בסכום גבוה יותר מעלות ההפקה השולית, רק כדי לסבסד הוצאות נוספות של המשרד על העברת מידע למשרדי ממשלה מהם יש איסור לגבות. ההשלכות הן שדרישת התשלום, בטח כשהיא גבוהה מהדרוש אבל לא רק, מהווה חסם לבקשת מידע בייחוד במקרים בהם הגוף המבקש לא מפיק מהמידע ערך כלכלי אלא זקוק לו לביצוע תפקידו בצורה טובה יותר (זאת בניגוד למקרים בהם המידע משמש להגדלת הכנסות).

מנגד, היעדר עלות עבור בקשות מידע עלול להוביל לכך שגופים ציבוריים יגישו בקשות בהיקפים גדולים או בתדירות גבוהה, מבלי לקחת בחשבון את עלויות הפקת המידע של המשרד המוסר. ללא מערכת תמחור שקופה

או חישוב עלויות פנימי, ייתכן **שהבקשות יוגשו ללא שיקול דעת כלכלי**, מה שעלול להעמיס על המשרד המוסר ולהקשות על מתן שירות איכותי ואפקטיבי. שיח על תמחור העברת המידע כשלעצמו יכול להיות גורם מעכב בתהליך העברת מידע, בייחוד אם הוא נעשה באופן תדיר אגב כל העברה גם כזו בנפח יחסית קטן, לכן יש לקחת בחשבון את **העלות הבירוקרטית** הזו ולצמצם אותה ככל הניתן.

כדי להתמודד עם האתגרים הכלכליים בהעברות מידע המוצגים לעיל, ממליצים על מודל כלכלי אשר יעוגן בהחלטת ממשלה מעודכנת המשלב בין מענה לעלויות המשרדים המוסרים, הפחתת חסמים בירוקרטיים בהעברות קטנות ופיקוח מסוג דיווח על התעריפים הנגבים בפועל למניעת תשלומים מופרזים זאת לצד המלצה על השקעה בטכנולוגיה שתביא לצמצום עלויות שליפת המידע באופן קבוע כמפורט להלן:

א. במסגרת המודל מוצע **לבטל את איסור דרישת התשלום בגין העברות** מידע בין משרדי ממשלה. כל גוף ציבורי יהיה רשאי לדרוש מגוף ציבורי אחר (ובכלל זה משרד ממשלתי) את **העלות הישירה** של הפקת המידע, בין אם בהעברה חד-פעמית או מתמשכת. התעריף המבוקש לא יעלה על עלות המשאבים הנדרשים כדי להפיק את המידע בפועל ורק בשל הבקשה, כלומר לא כולל עלויות תחזוקה או פיתוח למיניהם שהגוף משלם ממילא. התעריף ייקבע לפי ניתוח של עלות ההפקה וישוקף בצורה מפורטת לגוף המבקש לרבות כל ההסברים הנדרשים על אופן החישוב. גובה התשלום עבור העברת המידע **יתועד במערכת** להעברות מידע במסגרת הבקשה וישרת מנגנון של פיקוח תעריפים מסוג דיווח.

ב. מכיוון שעצם מנגנון גביית והעברת התשלומים עלול להוסיף חיכוך משמעותי גם להעברות מידע שעלות הפקתן קטנה מאוד, יתאפשר למשרד לגבות תשלום לפי הגדרת התעריף רק כאשר עלות הפקת ההעברות מאותו גוף מבקש עד אותה העברה, כולל, **עוברת את הסכום של 200 אלפי ש״ח במצטבר** בשנה קלנדרית. הסכום יוכל לעמוד לבחינה על ידי הועדה המרכזית להעברות מידע לפחות שנה לאחר פרסום המלצות הצוות.

ג. במקרים של בקשות חוזרות למידע שכבר הועבר בעבר, גם אם מדובר בבקשה של משרד אחר, לא תשולם עלות נוספת על חיבור או גישה למאגר שכבר הופק והועבר. במקרה זה, הגוף הציבורי המבקש יישא רק בעלות הישירה של העברת המידע, אם ישנה עלות כזו. העיקרון המנחה הוא למנוע חיוב כפול עבור מידע שכבר הופק, תוך עידוד שימוש חוזר וחסכוני במידע קיים.

ד. כדי למנוע מקרים של ניצול כוח המונופול, ולאזן בחוסר הסימטריה בין הצדדים, יוקם מנגנון **פיקוח על התעריפים שנגבים** על ידי משרדים ממשלתיים. גוף פיקוח בלתי תלוי באגף החשב הכללי, יהיה רשאי לבחון את המחירים שנגבו בהעברות מידע קודמות, להוות בורר עקב בקשה של אחד הצדדים במקרים של בקשה מעל 500 אלפי ש״ח, ולוודא שהתמחור נעשה בהתאם לעלויות סבירות ולא למטרות רווח. התעריף שייקבע על ידי החשב הכללי יהיה מחייב לשני הצדדים.

ה. כמפורט בהחלטת ממשלה 2273, במקרים שבהם המידע נדרש לטובת מדיניות חירום או מטרות לאומיות בנסיבות חריגות, ממליצים כי הועדה המרכזית להעברות מידע תהיה **רשאית להחליט כי העברת המידע תעשה ללא חיוב**. סעיף זה יאפשר גמישות במצבים קריטיים שבהם המידע חיוני לתפקוד הממשל או לביצוע משימות רחבות היקף.

ו. מוצע לקבוע כי לא יגבה תשלום בגין העברת מידע שמשרד רשאי לקבל מתוקף חוק מגוף ציבורי אחר הנדרש לצורך ביצוע תפקידו ועד היום הועבר ללא גביית תשלום בגין העברתו, זאת על מנת לאפשר את המשך הפעילות הרציפה של הממשלה המתבצעת מתוקף חוק.

ז. במסגרת הסכמים להעברת מידע, ניתן יהיה להסדיר גם את ההיבטים הנוגעים לתשלום עבור העברת המידע, בהתאם לעקרונות המפורטים לעיל.

על מנת להפחית את התשומות הנדרשות בשליפת המידע ובהתאמה גם בעלויות הנדרשות מהגופים, צורפו המלצות לאורך הדוח לתקצוב ייעודי של כלים טכנולוגיים שיסייעו בייעול תהליכי העברת המידע והפחתת עלויות באופן רוחבי אשר יפותחו בענן ככל הניתן. מיפוי וקטלוג המאגרים המרכזיים, חיבורם בתשתית קבועה למערכת לאישור העברות ולתשתיות רוחביות כגון שדרת המידע, לצד כלים טכנולוגיים ורובוטיים (טכנולוגיות RPA), כגון תהליכי אוטומציה ושליפה אוטומטית של נתונים, במיוחד כאשר הנתונים עדיין נשלפים באופן "ידני" ממערכות תפעוליות, יכולים לקצר את הזמן שלוקח להעביר את המידע ולהפחית משמעותית את העלות השולית של שליפת המידע והעברתו.

בנוסף חשוב לתקצב את החיבור בין כלל מערכות המידע העוסקות בהעברות מידע, כמו מערכות לניהול תהליך האישור להעברות מידע, התשתית להעברה עצמה והמערכת המשלימות, אשר יאפשרו תפעול יעיל יותר ומערכת אקולוגית דיגיטלית שתשפר את שיתוף הפעולה בין משרדי הממשלה. יישום ההיבטים הטכנולוגים הינו צעד גדול שיקרב אותנו כממשלה ומגזר ציבורי לעולם בו מרגע פקודה, העברת מידע תתבצע במהירות וכמעט ללא עלות, כך שכל נושא התשלומים והעלויות ידחק הצידה בעולם ההעברות הפשוטות ויישאר בעיקר במקרים של צורך בניתוחים מורכבים יותר הדורשים מומחיות משרדית ומקצועית בנושא.

יתרה מזאת, מוצע כי יוטל על מערך הדיגיטל הלאומי, בתיאום עם אגף ממשל וחברה במשרד ראש הממשלה ואגף תקציבים במשרד האוצר, לאתר "מוקדי ערך" במגזר הציבורי אשר ניתן, בעזרת השקעה חד פעמית להוזיל משמעותית את עלות השליפה השולית ולחברם לתשתיות שיתוף המידע המפורטות לאורך מסמך זה, ובהמשך לכך לתקצב השקעה כאמור בהתאם לסדר עדיפויות שיקבע.

החזון המוצע על ידי הצוות הוא כי לאחר הפיתוח וההטמעה של המערכות הממשלתיות הרוחביות להעברת מידע, לא יגבה תשלום עבור העברת מידע באמצעותן שלא תדרוש פעולות עיבוד מיוחדות על ידי הגוף המוסר את המידע.

סיכום ההמלצות למדיניות כלכלית ותקציבית בהעברת מידע בגופים ציבוריים:

1. שינוי מודל התשלומים עבור העברות מידע על ידי החלטת ממשלה מעודכנת בהתאם למפורט לעיל:

(א) יהיה ניתן לגבות עלות ישירה בכפוף לשקיפות מלאה של התעריף, תיעוד התשלומים, ורק כאשר עלות ההפקה מאותו גוף מבקש עוברת את הסכום של 200 אלפי ש"ח במצטבר בשנה קלנדרית.

(ב) יש להימנע מחיוב כפול עבור מידע שכבר הופק, תוך עידוד שימוש חוזר וחסכוני במידע קיים.

(ג) החשב הכללי יקים מנגנון פיקוח על התעריפים שנגבים על ידי משרדים ממשלתיים. הוא יהיה רשאי לבחון, לבקר ובמקרה הצורך לשנות תעריפים שנעשו לפי חישוב מוגזם של עלויות.

(ד) במקרים שבהם המידע נדרש לטובת מדיניות חירום או מטרות לאומיות בנסיבות חריגות, הועדה המרכזית להעברות מידע תהיה רשאית להחליט כי העברת המידע תעשה ללא חיוב.

(ה) לא יגבה תשלום עבור מידע שמשרד רשאי לקבל מתוקף חוק מגוף ציבורי אחר הנדרש לצורך ביצוע תפקידו ועד היום הועבר ללא גביית תשלום בגין העברתו.

2. תקצוב ייעודי של ההמלצות הנוגעות לפיתוח הכלים הטכנולוגיים המפורטים בדו״ח, קטלוג המידע ממשלתי, והחיבור בין המערכות לניהול תהליך האישור להעברות מידע, התשתית להעברה עצמה והמערכת המשלימות.
3. איתור על ידי מערך הדיגיטל בתיאום עם אגף ממשל וחברה ואגף תקציבים של ״מוקדי ערך״ אשר השקעה חד פעמית בהם תוזיל את העלויות להעברת מידע של כלל הממשלה ולחברתם לתשתיות שיתוף המידע המפורטות לאורך מסמך זה, ובהמשך לכך לתקצב השקעה כאמור בהתאם לסדר עדיפויות שיקבע.
4. החזון המוצע על ידי הצוות הוא כי לאחר הפיתוח וההטמעה של המערכות הממשלתיות הרוחביות להעברת מידע, לא יגבה תשלום עבור העברת מידע באמצעותן שלא תדרוש פעולות עיבוד מיוחדות על ידי הגוף המוסר את המידע.

6. היבטים רוחביים:

במטרה לתמוך בפתרונות שפורטו לעיל תוך חיבור הפתרונות השונים לתהליכים סדורים וברורים, הפתרונות בפרק זה יעסקו באתגרים הרוחביים, בהיבטים הארגוניים והתהליכיים, ובין היתר:

א. אוריינות העבודה בתהליכי העברות מידע אישי ובעיסוק בנתונים לעוסקים בתחום מהזוויות השונות – משפטי, טכנולוגי ו״עסקי-מקצועי״. הצוות מצא כי במקרים רבים הגורמים השונים המעורבים בהליך אישור העברת מידע אישי לא מכירים את ההליך ותנאיו ברמה מספקת, דבר אשר מטבע הדברים גורם לקשיים בהשלמת ההליך.

ב. מחסור בגורם אחראי לריכוז התחום ברמת הגוף הציבורי ומול גופים ציבוריים אחרים POC – Point of contact). בעל תפקיד כזה נחוץ, בין היתר, כדי לסייע במקרים בהם מתעורר קושי לאתר את המידע הנדרש בשלב איתור המידע, וכן לשיח בלתי אמצעי עם הוועדה במהלך הכנת בקשות להעברת מידע אישי וליווי הליך הבחינה שלהן.

ג. חיזוק האינטרסים לטובת העברות המידע האישי - העדר אינטרס של גוף ציבורי לשתף מידע אישי עם גוף אחר, אשר גורם לעיתים קרובות לאי העברת המידע בפועל או להארכת לוחות הזמנים להעברת המידע.

ד. יצירת וודאות להיבטי ההשקעה בתהליכי העברות מידע אישי – תשומות ועלויות העברת המידע ו/או הנגשתו, דרישות תקציביות, נטל בירוקרטי וגורמים נוספים.

ה. תעדוף נושא העברות המידע האישי ברמה הממשלתית הרוחבית והארגונית - כפי שתואר לעיל, העברות מידע אישי בין גופים ציבוריים היא מרכיב תשתיתי חיוני בעבודה הממשלתית ובעבודת יתר הגופים הציבוריים. לצד זאת, מכלול ההיבטים אליהם קשור תהליך העברת המידע האישי, ומגוון האתגרים הניצבים בפני הצלחה בתהליך, מלמדים על מורכבותו. מכאן עולה הצורך בהתייחסות מערכתית כוללת אליו. ההמלצות השונות הכלולות בדו״ח זה נועדו לפתור במידה מלאה או חלקית רבים מהאתגרים המקשים כיום על השלמת הליך אישור העברת המידע האישי באופן יעיל ובזמן סביר. אולם, גם

המלצות אלה אינן בבחינת תרופת פלא, שיש בכוחה להפוך הליך מורכב הנוגע לבעלי תפקידים רבים בלפחות שני גופים שונים להליך פשוט. בהתאם, נדרש לבצע פעולות שיעלו את הנושא לסדר היום בפני דרגי הניהול במשרדי הממשלה וביתר הגופים הציבוריים, וכי דרגים אלה יפנו קשב ניהולי לנושא.

<u>במטרה לענות על אתגרים אלו, הצוות מצא לנכון להמליץ כמפורט להלן:</u>

א. העלאת האוריינות בתחומי העברות המידע האישי – מערך הדיגיטל הלאומי, בשיתוף כלל הגורמים הרלוונטיים, יפעל ליצירת בסיס ידע, עזרים והדרכות לגורמים השונים העוסקים בתחומי העברות המידע האישי. בסיס הידע יכלול הן ידע פרוצדורלי לגבי מימוש התהליך והן היבטים מהותיים הנוגעים לסוגיות להעברות מידע אישי. הפעילות לעניין זה תכלול שילוב בין הדרכות עיתיות (וובינרים, פגישות פיזיות וכו׳) וחומרי הדרכה בנושא.

בסיס הידע וההדרכות יפותחו ע״י הגורמים האחראים לתחומי התוכן ויונגשו בערוצים הרלוונטים השונים, תוך חיבור למאמצים משיקים בתחומי הנתונים, אבטחת המידע והגנת הסייבר, הפרטיות ותחומים רלוונטים נוספים.

ב. הגברת האוריינות המשפטית – ישנה חשיבות להגברת ההיכרות של המשפטנים במשרדי הממשלה ובגופים ציבוריים נוספים העוסקים בהעברות מידע אישי עם הדין בנושא. הצוות מצא שבעוד שישנם גופים ציבוריים העוסקים בתדירות גבוהה בהעברות מידע והמשפטנים בהם מכירים ככלל ברמה גבוהה את הדין בנושא, בגופים ציבוריים אחרים, בהם העיסוק בנושא אינו שכיח, רמת האוריינות היא לעיתים נמוכה יותר. בכלל זה, עלו מקרים בהם נדרש לחדד את סוג המידע עליו חל ההסדר להעברת מידע אישי בין גופים ציבוריים, כמפורט לגבי הבהרת הדין בסעיף2(ג) לעיל. מטרה חשובה נוספת היא לעודד את היועצים המשפטיים במשרדי הממשלה ובגופים הציבוריים להכרות רחבה יותר גם עם היבטים לא משפטיים של נושא ניהול מידע והעברתו.

בדומה לסעיף א׳ – מוצע כי משרד המשפטים, בשיתוף וסיוע של מערך הדיגיטל הלאומי, יפעל לייצר הדרכות שוטפות, בסיס ידע חומרי הדרכה לטובת חיזוק ההכרות עם הנושא.

ג. גורם אחראי לתחום העברות המידע ותחומים משיקים בתוך הגופים הציבורים – מוצע כי המנהלים הכלליים של הגופים הציבורים (למעט בתי החולים הממשלתיים) ימנו גורם אחראי על תחום העברות המידע האישי ונושאים נוספים בתחום ניהול המידע. הגורם יהיה אחראי לשני תהליכים עיקריים:

(1) ריכוז תהליך שיתוף והעברות המידע האישי.

(2) הכרות ומיפוי עם נכסי הדאטה הקיימים וצורת הנגשתם.

על משרדי הממשלה ויחידות הסמך לעדכן את מערך הדיגיטל הלאומי (ודרכו את ועדת ההיגוי) בזהות הגורם האחראי לטובת תיקוף הרשימות תוך 30 יום מהמינוי של הגורם האחראי במטרה לשפר את הסנכרון והתיאום בין הגופים הציבוריים השונים.

למען הסר ספק – הגורם האחראי ירכז צוות בשיתוף כלל הגורמים הרלוונטים (אגפי טד״מ – טכנולוגיה דיגיטלית ומידע, אגפי תכנון, מדיניות ואסטרטגיה, אגפי שירות, הממונים על הגנת הפרטיות, הלשכות המשפטיות וגופים נוספים ככל הנדרש) לטובת הנושא וניהולו בצורה המיטבית. הגורם האחראי יוכל למלא תפקידים רלוונטיים נוספים בארגון.[64]

[64] בסעיף 15(א) להחלטה 2273 נקבע לעניין גורם אחראי על תחום העברת המידע:

ד. מנגנון מרכזי לזיהוי חסמים וקשיים ביישום העברות מידע אישי – בהמשך להחלטת ממשלה 1933, יש לחדש בהקדם את עבודת ועדת ההיגוי בראשות מערך הדיגיטל הלאומי תוך שותפות של ייעוץ וחקיקה והרשות להגנת הפרטיות שתסייע בהתרת חסמים ובזיהוי והצלבה בין גופים הזקוקים למידע אישי וגופים שברשותם מידע (Matching), בין היתר על מנת לייעל את תהליכי פיתוח ממשקי העברת המידע.[65] ועדת ההיגוי תפרסם לכל הפחות אחת לשנה את משכי הזמן הממוצעים להעברת מידע מהגופים הציבוריים השונים.

ה. יצירת הסכמים סטנדרטיים להעברות מידע אישי – הסכמי העברות והשימוש במידע הופכים להיות כלי נפוץ בידי מדינות רבות הן לשימוש פנים-ממשלתי, פנים-ציבורי ואף רב מגזרי. ההסכמים מייצרים וודאות לגבי "כללי המשחק" בעולמות הנתונים תוך התייחסויות לסוגיות השימוש, אבטחת המידע והגנת הסייבר, הפרטיות, שימושים משניים, הטכנולוגיה ועוד. ההסכמים הינם כלי שמאפשר שיתופי פעולה במקרים בהם מעל 2 גורמים מעוניינים לשתף פעולה בעולמות הנתונים ולשם כך להעביר ביניהם מידע. השימוש בהסכם סטנדרטי יוכל להקל משמעותית על עריכת הסכמים כאלה.[66] גם כאשר ישנה הסתייעות בגורמים פרטיים לצורך אספקת שירותים שונים מטעם רשויות השלטון, יש חשיבות להתאמת ההסכמים עימם באופן שיאפשר העברה יעילה של המידע מהם, כזרועו הארוכה של הגוף הציבורי ששכר את שירותיהם, לבין גוף ציבורי אחר.[67] בהתאם, מומלץ כי צוות בהשתתפות נציגי מערך הדיגיטל הלאומי, היועצת המשפטית לממשלה, מערך הסייבר הלאומי, הרשות להגנת הפרטיות, החשב הכללי והממונה על התקציבים במשרד האוצר ומשרד ראש הממשלה, יגבש נוסח הסכם כללי מוצע להעברות מידע אישי בין גופים ציבוריים.

ו. תיעדוף סוגית העברות המידע ברמה הארגונית והממשלתית – במטרה לעלות את ההכרות עם סוגית העברות המידע, מוצע לקיים את הפעולות הבאות:

(1) בהמשך לסעיף ד', מוצע כי ועדת ההיגוי תשקף למנכ"לי משרדי הממשלה ויחידות הסמך את סטטוס העברות המידע ומשכי הזמן הממוצעים להעברות מידע אצלם בארגון, לפחות אחת לשנה.

(2) מוצע כי משרד ראש הממשלה יעלה את סוגית העברות המידע בפורומים ממשלתיים באופן תדיר, בין היתר בפורום מנכ"לי משרדי הממשלה, פורום סמנכ"לי התכנון, המדיניות והאסטרטגיה.

"(א) להטיל על המנהלים הכלליים של משרדי הממשלה ויחידות הסמך למנות גורם מטעמם לניהול תחום שיתוף המידע, שיהיה איש הקשר המשרדי לנושא העברות המידע ולעדכן את מערך הדיגיטל הלאומי בדבר מיהות הגורם בתוך 30 יום מיום אישור החלטה זו, ובכל שינוי. תפקידיו של הגורם האמון על התחום יהיו הטמעת ההסדר החדש והשימוש במערכות החדשות, לרבות ביצוע הדרכות בתיאום עם מערך הדיגיטל הלאומי, ולקדם מיפוי נכסי הדאטה הארגוניים. ניתן למנות את הגורם האמון על התחום מבין עובדי אגפי האסטרטגיה, הגורמים האמונים על תחום הדאטה (CDO - מובילי דאטה משרדיים), מחשוב ומערכות מידע ואגפי השירות, בהתאם לסדר העדיפויות והמבנה המגוון של משרדי הממשלה ויחידות הסמך. סעיף קטן זה לא יחול על בתי חולים ממשלתיים".

[65] בסעיף 15(ב) להחלטה 2273 נקבע לעניין ועדת ההיגוי:
"להטיל על ראשת מערך הדיגיטל הלאומי לחדש את עבודת ועדת ההיגוי לעניין העברת מידע שהוקמה מכוח החלטה 1933, בצירוף נציג היועצת המשפטית לממשלה והרשות להגנת הפרטיות, אשר תפקידיה יהיו בין השאר: יצירת מפגשים בין גורמים שברשותם מידע ומוסרי מידע מרכזיים להתרת חסמים נפוצים; הדרכת בעלי תפקיד העוסקים בהעברות מידע בנוגע להסדר העברות המידע; גיבוש מדדי ביצוע של העברות מידע, הטמעת השימוש בפלטפורמות המרכזיות המפורטות בסעיף 13, ויישום ההסדר".

[66] בסעיף 12(א)(5) להחלטה 2273 נקבע לעניין עריכת הסכמים סטנדרטיים:
"(5) להטיל על צוות בהשתתפות נציגי מערך הדיגיטל, היועצת המשפטית לממשלה, מערך הסייבר הלאומי, הרשות להגנת הפרטיות, החשב הכללי והממונה על התקציבים במשרד האוצר ומשרד ראש הממשלה, לגבש נוסח הסכם כללי מוצע להעברות מידע בין גופים ציבוריים כאמור לעיל, עד 90 יום מעיגון ההסדר בדין".

[67] ספק השירותים יחשב כ-"מחזיק", כהגדרתו בחוק הגנת הפרטיות, באמגר המידע של הגוף הציבורי. לעניין הסכמים מסוג זה נקבע בסעיף 14 להחלטה 2273:
"14. להטיל על משרד ראש הממשלה, בשיתוף נציג אגף החשב הכללי במשרד האוצר, לבחון בתוך 120 ימים, את הצורך בעדכון נוסח ההסכמים להתקשרויות לרכישת שירותים חברתיים על ידי הממשלה הניתנים במיקור חוץ, כך שיאפשרו יישום ההוראות שבהחלטה זו, וכן בחינת קביעת הוראות החלטה זו במכרזים חדשים שיתפרסמו לאחר סיום הבחינה כאמור".

ז. מעקב אחר יישום המלצות הצוות- כדי להבטיח את יישום המלצות הצוות ואת ביצוע המדידה וכן כדי לעקוב אחר תוצאותיה, מוצע כי במהלך שנתיים מעת פרסום הדו״ח הסופי, הצוות יתכנס אחת לשישה חודשים וכל גורם שהומלצה לגביו המלצה או שהוטלה עליו האחריות לבצע מדידה בהתאם למדדים המוצעים בנספח א׳ לדו״ח יציג בפני הצוות את סטטוס ביצוע ההמלצה ואת תוצאות המדידה שבאחריותו.

סיכום ההמלצות בנוגע להיבטים רוחביים:

1. מערך הדיגיטל הלאומי, בשיתוף כלל הגורמים הרלוונטיים, יפעל להעלאת האוריינות בתחומי העברות המידע והנתונים בקרב הגורמים השונים העוסקים בתחומי העברות המידע האישי.
2. משרד המשפטים, בשיתוף וסיוע של מערך הדיגיטל הלאומי, יפעל להגברת ההיכרות של המשפטנים במשרדי הממשלה ובגופים ציבוריים נוספים העוסקים בהעברות מידע אישי עם הדין בנושא.
3. מוצע להטיל על המנהלים הכלליים בגופים הציבורים (למעט בתי החולים הממשלתיים) למנות גורם אחראי לתחום העברות המידע האישי ותחומים משיקים בגוף הציבורי.
4. חידוש עבודתה של ועדת היגוי לנושא העברת מידע אישי בין גופים ציבוריים שהוקמה בהחלטת ממשלה מס׳ 1933 ובצרוף שותפים נוספים לשם לזיהוי חסמים וקשיים ביישום העברת המידע.
5. צוות בהשתתפות נציגי מערך הדיגיטל הלאומי, היועצת המשפטית לממשלה, מערך הסייבר הלאומי, הרשות להגנת הפרטיות, החשב הכללי והממונה על התקציבים במשרד האוצר ומשרד ראש הממשלה יגבש נוסח הסכם כללי מוצע להעברות מידע אישי בין גופים ציבוריים.
6. תיעדוף סוגית העברות המידע ברמה הארגונית והממשלתית באמצעות הפעולות הבאות:

   (1) בהמשך לסעיף 4, מוצע כי ועדת ההיגוי תשקף למנכ״לי משרדי הממשלה ויחידות הסמך את סטטוס העברות המידע ומשכי הזמן הממוצעים להעברות מידע אצלם בארגון, לפחות אחת לשנה.

   (2) מוצע כי משרד ראש הממשלה יעלה את סוגית העברות המידע בפורומים ממשלתיים באופן תדיר , בין היתר בפורום מנכ״לי משרדי הממשלה, פורום סמנכ״לי התכנון, המדיניות והאסטרטגיה.
7. מוצע כי הצוות יקיים ישיבות תקופתיות (אחת לחצי שנה, לתקופה של שנתיים מיום פרסום הדו״ח הסופי) במסגרתן יוצג סטטוס הביצוע של ההמלצות השונות וכן את תוצאות המדידה, בהתאם למדדים המפורטים בנספח א׳ לדו״ח.

פרק ה: נושאים מוצעים להמשך בחינה

1. הסדר להעברת מידע אישי בחירום:

א. החשיבות והתרומה שבמתן שירותים פיזיים ודיגיטליים לאזרחים ולתושבים גבוהות בעת שגרה, וגבוהות אף יותר בעת חירום. העברת מידע אישי בין גופים ציבוריים היא ציר מרכזי בהתנהלות הממשלה והשירות הציבורי בכללותו באירועי חירום, ובפרט לצורך מתן שירותים שחלקם קריטיים ואף עשויים להציל חיים.

ב. בשעת חירום ישנם מאפיינים ייחודים לעולם המידע. הנתונים משתנים באופן תדיר, ונדרשים באופן אקוטי על מנת להעניק שירותים מיטביים לאוכלוסייה בכללותה, ובפרט למי שנפגעו באופן ישיר או עקיף בשל מצב החירום. בעוד שהצורך והדחיפות בהעברת המידע האישי מתגברים, גם האתגרים המקשים על הגופים הציבוריים לבצע העברות מידע ביעילות בזמן שגרה, מתעצמים עוד יותר בשל נסיבות החירום. כך, למשל, עלולה להיפגע יכולתם של גופים מסוימים לתפקד באופן חלקי או מלא, ובשל כך הם מתקשים אף יותר מהרגיל לקיים כסדרו את הליך האישור להעברת המידע האישי. לדוגמה, רשויות מקומיות שאוכלוסייתן נפגעה בשל מצב החירום זקוקות יותר מתמיד לקבל מידע ממשרדי הממשלה לטובת סיוע לתושביהן, אך עשויות להתקשות במיוחד, בשל הפגיעה בהן, לקיים את הליך האישור להעברת המידע.

ג. קשיים אלו התגלו, הלכה למעשה, עם פרוץ מלחמת חרבות ברזל. בכדי לתת להם מענה מיידי, ניתנו שורה של חוות דעת פרטניות מטעם משרד המשפטים במטרה לאפשר ככל הניתן, במסגרת הוראות הדין, לבצע העברות מידע אישי שנדרשו בשל מצב החירום, תוך התאמת הליך האישור הנדרש לנסיבות החירום. עם התמשכות מצב החירום, ניתנה הנחיה רוחבית בנושא של המשנה ליועצת המשפטית לממשלה (משפט ציבורי – חוקתי) ליועצים המשפטיים למשרדי הממשלה ויחידות הסמך, ובה פרשנויות וכלים מעשיים שנועדו להקל ולזרז ככל הניתן, במסגרת הדין הקיים, את העברות המידע שנדרשו לטובת התמודדות עם מצב החירום.[68]

ד. לצד המענה המיידי שניתן לצורך הדחוף, סבר הצוות כי יש מקום לבחון גיבוש של הסדר קבוע בתחום העברות המידע האישי, לטובת התמודדות עם מצבי חירום עתידיים. זאת, בין היתר, בשים לב לתקנות שנקבעו לאחרונה מכוח חוק שוויון זכויות לאנשים עם מוגבלויות, התשנ״ח – 1998, במסגרתן הוסדר בפירוט רב תהליך העברת מידע, בשגרה ובחירום, שנועד לאפשר את מתן הסיוע לאנשים עם מוגבלויות במצב החירום.[69] בהתאם, במסגרת עבודת הצוות, הוקם צוות משנה בהובלת מערך הדיגיטל הלאומי, אשר קיים מספר רב של דיונים ללימוד הנושא ולגיבוש טיוטת מתווה להסדר ייחודי להעברת מידע אישי בחירום. במסגרת עבודת צוות המשנה, נבחנו בין השאר התאמה של מסלולי העברת המידע המומלצים בדו״ח זה לנסיבות ולצרכים הצפויים במצב חירום, הסדרה של העברות מידע אישי בשגרה שנועדו לאפשר מענה מיידי לצורך במידע עם קרות מצב החירום, וקביעה של חובה, בנסיבות מסוימות, להעברת מידע לטובת סיוע לאוכלוסיה בחירום. צוות המשנה טרם השלים את עבודתו, אשר לאחרונה שולבה בה גם רשות החירום הלאומית

---

[68] מכתבה של המשנה ליועצת המשפטית לממשלה (משפט ציבורי-חוקתי) ליועצים המשפטיים של משרדי הממשלה ויחידות הסמך בנושא ״העברת מידע בין גופים ציבוריים בנסיבות הקשורות לאירועי החירום הנוכחיים״ מיום 20.12.2023.

[69] תקנות שוויון זכויות לאנשים עם מוגבלות (מאגר מידע לסיוע לאנשים עם מוגבלות בחירום), התשפ״ד-2024.

(רח"ל).

ה. לאור האמור, מוצע כי מערך הדיגיטל ורח"ל, בשיתוף יתר הגורמים החברים בצוות, ישלימו את עבודת המטה לבחינת ההסדר הראוי להעברת מידע לצורך סיוע לאוכלוסייה ואספקת שירותים ציבוריים במצב חירום. זאת, בין היתר, בשים לב לעקרונות הבאים:

1. הצורך לקבוע בעל תפקיד בממשלה המרכז את נושא העברות המידע הנדרשות לצורך סיוע לאוכלוסייה ולאספקת שירותים ציבוריים במצב חירום (להלן – סיוע בחירום) שיהיה אחראי על יישום ההסדר.
2. הצורך לבחון את ההגדרה המתאימה למצבי החירום, בהם יחול ההסדר בנושא והתנאים להפעלת ההסדר במצבי חירום אלו.
3. הצורך לקבוע מסלולים נוספים שיאפשרו העברת מידע אישי בין גופים ציבוריים במצב חירום, וביניהם:

(א) הרחבה של האפשרות להעביר מידע בסיסי לפרטי מידע נוספים מעבר לאלה הנכללים במסלול המידע הבסיסי המוצע במצב שגרה בין גופים ציבוריים לצורך סיוע בחירום, ביחס לאזור החירום והאוכלוסייה המושפעת ממצב החירום.

(ב) קביעה בחקיקת משנה של פרטי מידע אישי נוספים על המידע האמור בסעיף קטן (א), שיועברו לטובת סיוע בחירום בין גופים ציבוריים מסוימים.

(ג) בחינת האפשרות להעביר באופן יזום מידע אישי כאמור, בהתאם להסדרה מתאימה של העברת המידע שתיערך מבעוד מועד לפני תחילת מצב החירום, ובלבד שיקבעו אמצעים משפטיים וטכנולוגיים שיבטיחו כי השימוש במידע יעשה רק לצורך מתן שירות בשעת חירום.

(ד) היבטי אבטחת מידע והגנת סייבר בהעברת מידע אישי בחירום יקבעו בהתייעצות עם מערך הסייבר הלאומי, יה"ב והרשות להגנת הפרטיות.

ו. ככל שעבודת המטה האמורה תושלם עד להגשת מסקנות הצוות, יהיה מקום לבחון את שילוב מסקנות עבודת המטה בהמלצות הצוות.

ז. מבלי לקבוע מסמרות בנושא, ההסדרים הנבחנים לגבי העברת מידע אישי בחירום צפויים לדרוש קביעה של ההסדר בחקיקה ראשית.

2. <u>האפשרות לקבוע במקרים המתאימים חובה להעברת מידע אישי:</u>

ח. כמפורט לעיל, פרק ד' לחוק הגנת הפרטיות **מתיר**, בתנאים מסוימים, להעביר מידע אישי בין גופים ציבוריים. בהתאם, דו"ח זה עוסק בתנאים בהם יהיה מותר להעביר מידע אישי בין גופים ציבוריים, ולא בקביעת חובות להעברת מידע כאמור. לצד זאת, מוצע לבחון את השאלה האם בנסיבות מסוימות ראוי לקבוע במסגרת ההסדר **חובה** להעביר מידע אישי בין גופים ציבוריים.[70] נסיבות שעשויות להיות מתאימות, על פניו, לקביעת חובה להעברת מידע אישי הן כאשר האדם מסכים ואף מבקש להעביר את המידע אודותיו וכן בנסיבות של העברת מידע בחירום, במסגרת ההסדר שיגובש

[70] כפי שצוין לעיל, במקביל להסדרה הכללית להעברת מידע בין גופים ציבוריים בפרק ד' לחוק הגנת הפרטיות, ישנם דברי חקיקה המסדירים העברות מידע מסוימות בין גופים ציבוריים. בניגוד להסדר הכללי, העוסק כאמור בהיתר להעברת מידע, בהסדרים פרטניים העוסקים בהעברות מידע מסוימות, נקבעו בחקיקה חובות שונות להעברת מידע.

בהתאם לסעיף קטן (1).

ט. קביעת חובה להעברת מידע אישי בין גופים ציבוריים כאשר נושא המידע מסכים להעברתו מעוררת שאלות מורכבות. העברת המידע האישי בהסכמה עולה בקנה אחד עם מושכלות יסוד בדיני הגנת הפרטיות, לפיהן האדם הוא בעל השליטה במידע אודותיו, והסכמתו לפעולות שונות במידע אינן פוגעות בזכויותיו, אלא מגשימות אותן.[71] פעמים רבות, הסכמה של אדם להעברת מידע אודותיו משרתת נאמנה את הרצונות והאינטרסים שלו, כגון פישוט וייעול הליכים בירוקרטיים שונים מול גופים ציבוריים, בהם האדם מתבקש להמציא מידע שמקורו בגופים ציבוריים אחרים.

אולם, ישנם היבטים רבים שכמפורט לעיל נדרש לבחון בעת אישור העברת מידע אישי בין גופים ציבוריים, שאינם נוגעים לעצם הסכמתו של האדם עליו מועבר המידע. כך, בין היתר, נבחנת מידתיות העברת המידע, ובמסגרתה שהמידע המבוקש אכן נדרש, שמועבר ונשמר רק המידע המזערי הנחוץ להגשמת המטרה, ושהגישה למידע מתאפשרת רק למי שהמידע נחוץ לו לשם מילוי תפקידו. כן מוסדר אופן העברת המידע ואבטחתו. כל אלה נבחנים, בהתאם למסלולי האישור השונים, בשיח בין הגופים הציבוריים, ולא נקבעים חד צדדית על ידי הגוף המבקש את המידע. קביעת חובה למסירת מידע אישי, עלולה לגרוע מאפשרות הגוף מוסר המידע להפעיל את שיקול דעתו ולעמוד על כך כי הסדרים מתאימים יקבעו בנושא. יתר על כן, כאשר אדם מסכים להעברת מידע עליו, נדרש, כבכל הסכמה לפגיעה בפרטיות, כי ההסכמה תהיה מדעת.[72] אולם, שלל הנושאים האמורים, מעצם טבעם, אינם מצויים בידיעתו של האדם עליו מועבר המידע. אדם העומד מול רשות שלטונית המבקשות ממנו להסכים להעברת מידע אודותיו, זכאי להניח כי הרשות פועלת כנאמן הציבור, ומשכך דואגת לכל אותם היבטים המבטיחים את מידתיות העברת המידע האישי.

מענה אפשרי לפער בין הסכמת האדם לבין הצורך בהסדרה בין הגופים הציבוריים המעבירים ביניהם מידע אישי יכול להתקבל על ידי הסדרה של כלל היבטי העברת המידע בחקיקה, והדבר אף נעשה בחקיקה בשנים האחרונות ביחס להעברת מידע פיננסי ומידע רפואי (לאו דווקא בין גופים ציבוריים).[73] אולם, כפי שניתן לראות בהסדרים אלה, מדובר בחוקים המסדירים העברת מידע מסוג מסוים מאוד לגופים מסוג מסוים, וכוללים פירוט רב, בין היתר של פרטי המידע שיועברו, השימוש בהם, תקופת שמירתם ואופן קבלת ההסכמה והתנאים לה. כן נדרש לפי חוקים אלה קיומו של מאסדר המעניק היתרים ומפקח על העברת המידע בין אותם גופים ואשר מוסמך לקבוע לגביה הוראות שונות. נראה כי הסדרה כה מפורטת מתאימה להעברת מידע בנסיבות פרטניות, ולא כהסדר כללי להעברת מידע אישי בין גופים ציבוריים.

י. יצוין, כי בהחלטת ממשלה 1933 נקבעה חובה על משרדי הממשלה ויחידות הסמך להעביר ביניהם מידע אישי כאשר הוא דרוש לצורך שיפור השירות לציבור ויישום מדיניות שאל פעם אחת. חובה זו אינה מותנית בקבלת הסכמה, אולם, היא כפופה להשלמת הליך הבחינה של חוקיות העברת המידע, במסגרתו נבחנים כיום בידי הוועדות להעברת מידע כל השיקולים שפורטו לעיל.[74] בהתאם, החובה הקבועה כיום נתונה למעשה לשיקול דעת הוועדות להעברת מידע.

---

[71] לעניין מעמד ההסכמה בדיני הגנת הפרטיות ר' סעיף 1 לחוק הגנת הפרטיות: "לא יפגע אדם בפרטיות זולתו ללא הסכמתו"; סעיף 7(ב) לחוק יסוד: כבוד האדם וחירותו: "אין נכנסים לרשות היחיד של אדם שלא בהסכמתו". ר' גם סעיף 20 ל – GDPR המעגן את הזכות ל – data portability.

[72] ר' הגדרת הסכמה בסעיף 3 לחוק הגנת בפרטיות.

[73] ר' חוק ניוד מידע רפואי, התשפ"ד-2024 וחוק חוק שירות מידע פיננסי, התשפ"ב-2021.

[74] ר' סעיף 1(א) להחלטת ממשלה מס' 1933.

יא. לאור המורכבות שפורטה לעיל, מוצע שהצוות ימשיך ויבחן את האפשרות לקבוע חובה להעברת מידע אישי בין גופים ציבוריים וימליץ על קידום תיקוני חקיקה ככל שהדבר יידרש.

פרק ו: סיכום המלצות הצוות

להלן יובא ריכוז המלצות הצוות, כפי שהן מפורטות בדו"ח זה:

א. המלצות לשלב גילוי ואיתור המידע האישי:

1. בניית קטלוג מידע ממשלתי על ידי מערך הדיגיטל הלאומי, והקצאת המשאבים הנדרשים לפיתוחו.
2. הטמעת הקטלוג בגופים ציבוריים מרכזיים, על ידי הגופים בסיוע מערך הדיגיטל הלאומי, והקצאת המשאבים נדרשים לכך.
3. יצירת עזרים ומדריכים לחיפוש במידע הממשלתי.

ב. המלצות לשלב אישור העברת המידע האישי:

1. קביעה של מסלולים נוספים לאישור תהליכי העברות מידע אישי, בהתאם לתנאים המפורטים לעיל:
   (א) מסלול להעברת מידע בסיסי (Basic Data);
   (ב) מסלול להעברת מידע על סמך אישור מבקש המידע;
   (ג) הסכמי העברות מידע;
   (ד) ועדה מרכזית לאישור העברות מידע אישי בין גופים ציבוריים;
   (ה) מנגנון התממה טכנולוגי דוגמת "קופסה שחורה";
   (ו) שימור המסלול הקיים של הועדות להעברת מידע .
2. קביעת היבטים כלליים שנדרש להסדיר בכל אחד ממסלולי האישור המפורטים לעיל:
   (א) המאפיינים הבסיסיים של העברת המידע;
   (ב) היבטים הנוגעים לממשק העברת המידע ולאבטחת המידע לאחר העברתו;
   (ג) קביעת חובת יידוע על העברת מידע ביומטרי.
3. הבהרת הדין ביחס לתחולת ההסדר.
4. עיגון הסדרים אלה בתיקון לתקנות הגנת הפרטיות, אשר במסגרתו יכללו גם עיקרי ההסדרים שהוצעו בטיוטת התיקון שהוכנה בעקבות החלטת הממשלה מס' 1933.
5. פיתוח מערכת לניהול תהליך אישור העברת המידע (מערכת ציטה).

ג. ההמלצות לשלב מימוש העברת המידע:

1. מערך הדיגיטל יכין תכנית עבודה לחיבור גופים ציבוריים לתשתיות העברת המידע המרכזיות.
2. להקים צוות ייעודי במערך הדיגיטל הלאומי שיסייע לגופים הציבוריים לפתח את הממשקים הדרושים לשם קישור מאגרי המידע המרכזיים שלהם לתשתיות העברת המידע המרכזיות ולשימוש בהן.
3. יצירת ממשקים בין התהליך איתור המידע, קבלת אישור להעברת המידע (באמצעות מערכת ציטה) והעברת המידע בפועל.
4. מערך הדיגיטל הלאומי ישלים את פיתוחן של מערכות אנליזה משלימות לטובת הפקת סטטיסטיקה ואיסוף מידע לצורך קבלת החלטות מבוססות נתונים: רשת לקידום מדעי

הנתונים (פלטפורמת רקמ״ה) ותשתית מחשוב לשאילתות מבוזרות (מערכת מחל״ף). בנוסף, המערך ירכז בחינה רוחבית של טכנולוגיות ומתודולוגיות קיימות להתממת מידע במשרדי הממשלה.

ד. ההמלצות בנוגע לסטנדרטיזציה של היבטי אבטחת המידע:

1. לאמץ את מסמך הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים.
2. עדכניות ההוראות במסמך ההנחיות תיבחן מעת לעת על ידי ממערך הסייבר הלאומי, הרשות להגנת הפרטיות ויה״ב, ולכל הפחות אחת לשנתיים או בעת הטמעת מערכת מרכזית חדשה להעברת מידע בין גופים ציבוריים.

ה. סיכום ההמלצות למדיניות כלכלית ותקציבית בהעברת מידע בגופים ציבוריים

1. שינוי מודל התשלומים עבור העברות מידע על ידי החלטת ממשלה מעודכנת בהתאם למפורט לעיל:
   (א) יהיה ניתן לגבות עלות ישירה בכפוף לשקיפות מלאה של התעריף, תיעוד התשלומים, ורק כאשר עלות ההפקה מאותו גוף מבקש עוברת את הסכום של 200 אלפי ש״ח במצטבר בשנה קלנדרית.
   (ב) יש להימנע מחיוב כפול עבור מידע שכבר הופק, תוך עידוד שימוש חוזר וחסכוני במידע קיים.
   (ג) יוקם מנגנון פיקוח על התעריפים שנגבים על ידי משרדים ממשלתיים. החשב הכללי יהיה רשאי לבחון, לבקר ובמקרה הצורך לשנות תעריפים שנעשו לפי חישוב מוגזם של עלויות.
   (ד) במקרים שבהם המידע נדרש לטובת מדיניות חירום או מטרות לאומיות בנסיבות חריגות, הועדה המרכזית להעברות מידע תהיה רשאית להחליט כי העברת המידע תעשה ללא חיוב.
   (ה) יוחרג מהמודל מידע שמשרד רשאי לקבל מתוקף חוק מגוף ציבורי אחר הנדרש לצורך ביצוע תפקידו ועד היום הועבר ללא גביית תשלום בגין העברתו.
2. איתור על ידי מערך הדיגיטל בתיאום עם אגף ממשל וחברה ואגף תקציבים של ״מוקדי ערך״ אשר השקעה חד פעמית תוזיל את העלויות של כלל הממשלה ולחברתם לתשתיות שיתוף המידע המפורטות לאורך מסמך זה.

ו. ההמלצות בנוגע להיבטים רוחביים:

1. מערך הדיגיטל הלאומי, בשיתוף כלל הגורמים הרלוונטיים, יפעל להעלאת האוריינות בתחומי העברות המידע והנתונים בקרב הגורמים השונים העוסקים בתחומי העברות המידע האישי.
2. משרד המשפטים, בשיתוף וסיוע של מערך הדיגיטל הלאומי, יפעל להגברת ההיכרות של המשפטנים במשרדי הממשלה ובגופים ציבוריים נוספים העוסקים בהעברות מידע אישי עם הדין בנושא.

3. מוצע להטיל על המנהלים הכלליים בגופים הציבורים (למעט בתי החולים הממשלתיים) למנות גורם אחראי לתחום העברות המידע האישי ותחומים משיקים בגוף הציבורי.
4. חידוש עבודתה של ועדת היגוי לנושא העברת מידע אישי בין גופים ציבוריים שהוקמה בהחלטת ממשלה מס׳ 1933 ובצרוף שותפים נוספים לשם לזיהוי חסמים וקשיים ביישום העברת המידע.
5. צוות בהשתתפות נציגי מערך הדיגיטל הלאומי, היועצת המשפטית לממשלה, מערך הסייבר הלאומי, הרשות להגנת הפרטיות, החשב הכללי והממונה על התקציבים במשרד האוצר ומשרד ראש הממשלה יגבש נוסח הסכם כללי מוצע להעברות מידע אישי בין גופים ציבוריים.
6. תיעדוף סוגית העברות המידע ברמה הארגונית והממשלתית באמצעות הפעולות הבאות:
   (א) בהמשך לסעיף 4, מוצע כי ועדת ההיגוי תשקף למנכ״לי משרדי הממשלה ויחידות הסמך את סטטוס העברות המידע ומשכי הזמן הממוצעים להעברות מידע אצלם בארגון, לפחות אחת לשנה.
   (ב) מוצע כי משרד ראש הממשלה יעלה את סוגית העברות המידע בפורומים ממשלתיים באופן תדיר , בין היתר בפורום מנכ״לי משרדי הממשלה, פורום סמנכ״לי התכנון, המדיניות והאסטרטגיה.
7. מוצע כי הצוות יקיים ישיבות תקופתיות (אחת לחצי שנה, לתקופה של שנתיים מיום פרסום הדו״ח הסופי) במסגרתן יוצג סטטוס הביצוע של ההמלצות השונות וכן את תוצאות המדידה, בהתאם למדדים המפורטים בנספח א׳ לדו״ח.

ז. סיכום ההמלצות למדיניות כלכלית ותקציבית בהעברת מידע בין גופים ציבוריים:

1. שינוי מודל התשלומים עבור העברות מידע על ידי החלטת ממשלה מעודכנת בהתאם למפורט לעיל:
   (א) יהיה ניתן לגבות עלות ישירה בכפוף לשקיפות מלאה של התעריף, תיעוד התשלומים, ורק כאשר עלות ההפקה מאותו גוף מבקש עוברת את הסכום של 200 אלפי ש״ח במצטבר בשנה קלנדרית.
   (ב) יש להימנע מחיוב כפול עבור מידע שכבר הופק, תוך עידוד שימוש חוזר וחסכוני במידע קיים.
   (ג) החשב הכללי יקים מנגנון פיקוח על התעריפים שנגבים על ידי משרדים ממשלתיים. הוא יהיה רשאי לבחון, לבקר ובמקרה הצורך לשנות תעריפים שנעשו לפי חישוב מוגזם של עלויות.
   (ד) במקרים שבהם המידע נדרש לטובת מדיניות חירום או מטרות לאומיות בנסיבות חריגות, הועדה המרכזית להעברות מידע תהיה רשאית להחליט כי העברת המידע תעשה ללא חיוב.
   (ה) לא יגבה תשלום עבור מידע שמשרד רשאי לקבל מתוקף חוק מגוף ציבורי אחר הנדרש לצורך ביצוע תפקידו ועד היום הועבר ללא גביית תשלום בגין העברתו.
2. תקצוב ייעודי של ההמלצות הנוגעות לפיתוח הכלים הטכנולוגיים המפורטים בדו״ח, קטלוג המידע ממשלתי, והחיבור בין המערכות לניהול תהליך האישור להעברות מידע, התשתית להעברה עצמה והמערכת המשלימות.

3. איתור על ידי מערך הדיגיטל בתיאום עם אגף ממשל וחברה ואגף תקציבים של "מוקדי ערך" אשר השקעה חד פעמית בהם תוזיל את העלויות להעברת מידע של כלל הממשלה ולחברתם לתשתיות שיתוף המידע המפורטות לאורך מסמך זה, ובהמשך לכך לתקצב השקעה כאמור בהתאם לסדר עדיפויות שיקבע.
4. החזון המוצע על ידי הצוות הוא כי לאחר הפיתוח וההטמעה של המערכות הממשלתיות הרוחביות להעברת מידע, לא יגבה תשלום עבור העברת מידע באמצעותן שלא תדרוש פעולות עיבוד מיוחדות על ידי הגוף המוסר את המידע.

נספחים

נספח א' – מדדים ליישום ההמלצות ולהצלחתן

נספח ב' –הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים

נספח א׳: מדדים ליישום ההמלצות ולהצלחתן

מטרת המדידה היא לעקוב אחרי השפעת שינויי המדיניות המוצעים בדו״ח בשני מישורים מרכזיים:

- **מישור התפוקה** – במישור זה תיבחן מידת יישום ההמלצות בדו״ח על-ידי הגופים הציבוריים האמונים על ביצוע ההמלצות.
- **מישור התוצאה** – בחינה של מדדים כגון זמני העברה מידע, על מנת לבחון קיצור בזמנים ובטווחי מתן השירות. נוסף על כך, מוצע למדוד את ״נפח העברות המידע״ בין הגופים, במטרה להעריך האם המדיניות מובילה לעלייה בהיקפי העברות המידע בין גופי המגזר הציבורי, והאם נעשה בה שימוש על-ידי מגוון גופים.

תפיסת השינוי של הצוות גורסת כי ישנו קשר חיובי בין עמידה במדדי התפוקה לעמידה במדדי התוצאה. מדידה בשני המישורים תאפשר בקרה אפקטיבית לאורך זמן, כמו גם איתור חסמים ובעיות במימוש המדיניות.

<u>המדדים המוצעים:</u>

מדד	סוג המדד	ערך בסיס 2025	ערך מתוכנן	מועד סיום מדידה	אחריות מדידה
ממוצע ימי העברה מ״קצה לקצה״ מיום דרישת המידע ועד העברתו בפועל	מדד תוצאה	240 ימים (לשלב האישור בלבד)	שנה ממועד פרסום הדו״ח: 120 ימים. שנה ממועד תיקון התקנות: 90 ימים.	שנתיים ממועד תיקון התקנות	מערך הדיגיטל הלאומי
גופים המחוברים לשדרת המידע	מדד תוצאה	45 משרדי ממשלה ויחידות סמך	שנה ממועד פרסום הדו״ח: כל משרדי הממשלה ויחידות הסמך (100%). 85% מהרשויות	שנה ממועד פרסום הדו״ח	מערך הדיגיטל הלאומי

מדד	סוג המדד	ערך בסיס 2025	ערך מתוכנן	מועד סיום מדידה	אחריות מדידה
			המקומיות.[75]		
שיעור השירותים המיישמים מדיניות ask once	מדד תוצאה (ימדד מדגם מצומצם של שירותים)	מדידה חדשה[76]	עליה בשיעור של 25% בשנה שלאחר פרסום הדו"ח ביחס לשירותים שימדדו במדגם. עליה בשיעור של 50% בשנה שלאחר תיקון התקנות ביחס לשירותים שימדדו במדגם.	שנה ממועד תיקון התקנות	מערך הדיגיטל הלאומי
הסכמי שיתוף מידע בין גופים ציבורים	מדד תוצאה	-	3 הסכמים בשנה החל משנה לאחר תיקון התקנות.	שנתיים מתיקון התקנות	מערך הדיגיטל הלאומי

[75] מתוך 259 רשויות מקומיות.
[76] המדד מפותח כיום וישמש כבסיס למדידת העלייה.

מדד	סוג המדד	ערך בסיס 2025	ערך מתוכנן	מועד סיום מדידה	אחריות מדידה
הגשה לשר המשפטים של טיוטת התקנות לאישור לפרסום להערות הציבור	מדד תפוקה	-	V	2025	משרד המשפטים
ככל שיאושר פרסום התקנות להערות הציבור, הנחת טיוטת התקנות לאישור שר המשפטים	מדד תפוקה	-	V	2026	משרד המשפטים
כמות ההיתרים שניתנו ע״י הוועדה המרכזית	מדד תפוקה	-	שנה ממועד תיקון התקנות - לפחות 2 בשנה.	5 שנים מפרסום התקנות	מערך הדיגיטל הלאומי

מדד	סוג המדד	ערך בסיס 2025	ערך מתוכנן	מועד סיום מדידה	אחריות מדידה
פרסום נוסח הסכם כללי מוצע להעברות מידע בין גופים ציבוריים	מדד תפוקה	-	V	3 חודשים מיום תיקון תקנות	מערך הדיגיטל הלאומי
פרסום קטלוג מרכזי	מדד תפוקה	-	V	4/2025[77]	מערך הדיגיטל הלאומי
הגופים המחוברים לקטלוג המרכזי	מדד תפוקה	מדידה חדשה	שנה ממועד פרסום הדו״ח – 5 גופים. שנתיים ממועד פרסום הדו״ח – 10 גופים.	שנתיים ממועד פרסום הדו״ח	מערך הדיגיטל הלאומי

[77] בהתאם למועד הקבוע בסעיף 13 להחלטת ממשלה 2273.

מדד	סוג המדד	ערך בסיס 2025	ערך מתוכנן	מועד סיום מדידה	אחריות מדידה
פיתוח מערכת רקמ״ה	מדד תפוקה	-	עלית גרסה ראשונית לאוויר (MVP).	10/2025[78]	מערך הדיגיטל הלאומי
פיתוח מערכת מחל״ף	מדד תפוקה	-	Proof of Concept [79]	06/2025	מערך הדיגיטל הלאומי
משרדי ממשלה ויחידות סמך שמינו ממונה לשיתוף מידע	מדד תפוקה	מדידה חדשה	40 משרדי ממשלה ויחדות סמך מינו ממונה שיתוף מידע. [80]	12/2025	מערך הדיגיטל הלאומי

[78] בהתאם למועד הקבוע בסעיף 2ד13 להחלטת ממשלה 2273.
[79] מסגרת ה- POC תיבדק מידת הישימות של מוצר הקיים בתעשייה בתחום ה Secured Collaboration לפי מדדי ההצלחה שהוגדרו.
[80] מתוך 50 גופים המונחים על ידי מערך הדיגיטל הלאומי.

מדד	סוג המדד	ערך בסיס 2025	ערך מתוכנן	מועד סיום מדידה	אחריות מדידה
פריסת מערכת צ'יטה	מדד תפוקה	מדידה חדשה	שנה מפרסום הדו"ח: 15 משרדי ממשלה ויחידות סמך מחוברים למערכת.[81] 25 רשויות מקומיות מחוברות למערכת. שנתיים ממועד פרסום הדו"ח: 25 משרדי הממשלה ויחידות הסמך מחוברים למערכת. 65 רשויות מקומיות מחוברות למערכת.[82]	שנתיים ממועד פרסום הדו"ח.	מערך הדיגיטל הלאומי

[81] מתוך 50 גופים המונחים על ידי מערך הדיגיטל הלאומי.

[82] חיבורם של גופים ציבוריים נוספים למערכת תבחן בהתאם לתדירות והיקפי העברות המידע של הגופים, ובהתאם לתיעדופים שייקבעו על ידי מערך הדיגיטל הלאומי.

נספח ב׳: הנחיות אבטחת המידע והגנת הסייבר בהעברת מידע אישי בין גופים ציבוריים

<u>הנדון: הנחיות אבטחת מידע והגנת סייבר בהעברת מידע בין גופים ציבוריים[83] – סיכום עבודת תת-הצוות המקצועי במסגרת הצוות הבין-משרדי להעברות מידע אישי בין גופים ציבוריים</u>

<u>רקע</u>

בהתאם להחלטת הממשלה בנושא ייעול המגזר הציבורי: האצת השירות הדיגיטלי לאזרח ויצירת תשתיות דיגיטליות וכלי מדיניות תומכים, ובהמשך לעקרונות שהוצגו בדיון הצוות הבין-משרדי להעברות מידע מיום 8.10.24, מובאת להלן הצעה לסטנדרטיזציה של היבטי אבטחת המידע והגנת סייבר ביחס להעברת מידע בין גופים ציבוריים אשר מטרתה לפשט את הליכי הסדרת היבטים אלה בין הגופים מוסרי המידע ומקבלי המידע.[84]

התוצר גובש בתהליך משותף של אנשי טכנולוגיה ומשפטנים ממערך הסייבר הלאומי, הרשות להגנת הפרטיות והיחידה להגנת הסייבר במערך הדיגיטל הלאומי (יה״ב) במסגרת עבודת תת הצוות הבין-משרדי בנושא היבטי אבטחת מידע והגנת סייבר בהעברות מידע בין גופים ציבוריים. מסמך זה מתייחס הן להעברת מידע אישי והן להעברת נתונים שאינם מידע אישי ומפרט את ההנחיות המחייבות בעת העברת מידע בין גופים ציבוריים בהיבטי אבטחת מידע והגנת סייבר.

<u>בכל הנוגע למידע אישי,</u> ההוראות המפורטות במסמך זה הן הוראות הנובעות ישירות מתקנות הגנת הפרטיות (אבטחת מידע), התשע״ז – 2017, למעט ההוראה לעניין סינון מידע טרום העברה, ובהתאם הן מחייבות את כלל הגופים הציבוריים בהעברת מידע אישי ביניהם.

מסמך זה כולל את כל ההוראות המחייבות לפי הדין הכללי בהיבטי אבטחת מידע והגנת הסייבר בקשר להעברת מידע אישי בין גופים ציבוריים. המסמך לא גורע מחובות אחרות בהיבטי אבטחת מידע והגנת הסייבר החלות על גופים ציבוריים שלא בקשר להעברת מידע אישי ביניהם, או מהוראות דין פרטניות החלות על גופים מסוימים או על העברות מידע מסוימות.

בעת העברת מידע בין גופים ציבוריים, יצהיר הגוף מקבל המידע בפני הגוף מוסר המידע על עמידה בהוראות מסמך זה בצירוף המסמכים והמידע הנדרשים כמפורט במסמך (ככל שהם נדרשים), תוך פירוט החלופה המותרת אותה בחר ליישם, כאשר קיימות חלופות לבחירה. מוסר המידע רשאי, מטעמים מיוחדים, לדרוש ממקבל המידע לבחור בחלופה מסוימת מבין החלופות המותרות. כאשר מדובר בחלופה שמעצם טיבה נדרש סנכרון לגביה בין הגופים (כגון תווך העברת המידע), בחירת החלופה תיעשה בתיאום בין שני הגופים.

---

[83] מסמך זה מתייחס למידע לא מסווג ביטחונית.
[84] יצוין כי אין בהנחיות אלו כדי לגרוע מהוראות כל דין.

עקרונות

- שפה אחידה – תיאום הגדרות ממשלתי
- הנחיות בסטנדרט אחיד לכלל הגופים הציבוריים, בהתאם לסוג המידע וסיווגו
- סטנדרטיזציה של פרקטיקות מקובלות הקבועות בין השאר בדין ובהנחיות, מבלי להחמיר מעבר לנדרש
- תוצר פשוט, ברור ופרקטי
- התייחסות לתשתיות מרכזיות רוחביות קיימות להעברת המידע בין גופים ציבוריים

סיווגי מידע – טבלת המרה[85]

	סיווג המידע			
מקור/קטגוריה	**א**	**ב**	**ג**	**ד**
חוק הגנת הפרטיות	נתונים שאינם מידע אישי לפי חוק הגנת הפרטיות	מידע אישי, לרבות Basic data	מידע בעל רגישות מיוחדת	
הנחיית יהה"ב	פומבי	פנימי	פנימי – מוגבל	פנימי – חסוי
הגדרות מסי"ל	פומבי	רגיש	חסוי	חסוי ביותר

הנחיות אבטחת מידע והגנת סייבר ביחס למסלולי העברות המידע לפי דוח הצוות הבין-משרדי להעברות מידע בין גופים ציבוריים

[85] אף שהתוצר רלוונטי לעבודת הצוות הבין משרדי ביחס להעברת מידע אישי בלבד בין גופים ציבוריים, עבודת תת הצוות המקצועי בנושא היבטי אבטחת מידע והגנת סייבר הייתה רחבה ומוצע בהתאמה להשלים את עבודת המטה הממשלתית ביחס להעברות מידע שאינו מידע אישי בין גופים ציבוריים.

מסלולים					
מסלול	1 **ללא מידע אישי**	2 **מסלול מידע בסיסי**	3 **מסלול באישור עצמי**	4 **הסכמי העברת מידע + ועדות**	5 **ועדה מרכזית**
מסלול העברת המידע בהיבטי אבטחת מידע וסייבר	ככלל א *אלא אם יש צבר מידע	ב *בחירום- מסלול ב, ג או ד בהתאם לסוג המידע	ב *ג או ד ביחס למידע בעל רגישות מיוחדת אשר עבר התממה לא מלאה	ב, ג או ד	ב, ג, או ד

- ביחס להעברת מידע בחירום – לאחר סיום עבודת תת-צוות העברות מידע בחירום, תתבצע בחינה נוספת של הנחיות אבטחת מידע והגנת סייבר ביחס להעברת מידע בחירום, ביחד עם תת-צוות חירום.
- יובהר כי גם ביחס להעברת מידע בין גופים ציבוריים שאינה מתבצעת לפי הוראות פרק ד' לחוק הגנת הפרטיות, הנחיות אבטחת המידע יקבעו בהתאם לסיווג המידע.
- כאשר מתאפשרים מספר מסלולים נדרש לסווג את הנתונים בהתאם לסוג המידע והיקפו לצורך בחינת מסלול העברת המידע בהיבטי אבטחת מידע וסייבר.

הנחיות אבטחת מידע והגנת סייבר ביחס להעברות מידע בין גופים ציבוריים[86]

במסלולי העברות המידע

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** **(הדרישות בכל קבוצה חליפיות אחת לשנייה)**	**א**	**ב**	**ג**	**ד**	
סינון ובדיקת מידע טרום העברה[88]	1. ללא סינון ובדיקת המידע 2. תהליך ידני לווידוא העברת מידע רלוונטי בלבד. 3. השחרה טכנולוגית של מידע שאינו רלוונטי.	1, 2, 3	2, 3	2, 3	3	הנחיית שדרת המידע דורשת משני המשרדים, המקבל והמוסר, לבצע הליך סינון והלבנה.[89]
אריזת המידע[90]	4. ללא אריזה כלל. **הכנסת המידע לתוך:** 5. File Document סטנדרטי (word ,csv וכיו״ב). 6. בסיס נתונים סטנדרטי (SQL, MDB ,DBF וכיו״ב). 7. Web File (html, php וכיו״ב).	18–4	4 (בתנאי שישנה הצפנה מקובלת) 18–5	17–5 18 במקרה של בלדרות מאובטחת	5, 6, 9, 10, 16–11 18 (במקרה של בלדרות מאובטחת	בדיקת מרכיב זה מבוצעת אוטומטית בכל העברה בשדרת המידע,[91] MFT (כספות או Go Anywhere), גוגל דרייב ענני,[92] ודוא״ל ממשלתי.[93]

---

[86] מובהר כי אין באמור כדי לגרוע מהנחיות הקצין המוסמך לפי החוק להסדרת הביטחון בגופים ציבוריים, התשנ״ח- 1998.
[87] יצוין כי לא מדובר ברשימה ממצה וקיימות תשתיות מדינה נוספות.
[88] ההוראה לעניין סינון מידע לפני העברתו תחול כהוראה מחייבות את הגופים הכפופים להנחיית מערך הסייבר הלאומי ויה״ב, ותהווה בגדר המלצה מקצועית (Best Practice) לגבי יתר הגופים הציבוריים. יצוין כי סעיף 23ה בחוק הגנת הפרטיות העוסק במידע עודף מתיר מסירת מידע עודף בין גופים ציבוריים, ובלבד שנקבעו נהלים שיבטיחו מניעת שימוש כלשהו במידע עודף שנתקבל וכי בתקנה 6 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ״ו-1986, נקבעה חובה על הגוף המקבל מידע להפריד מיד עם קבלת הנתונים את המידע העודף ולמחוק אותו מיד
[89] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן.
[90] תק׳ 14(ב) לתקנות הגנת הפרטיות (אבטחת מידע), התשע״ז-2017 (להלן: ״**תקנות אבטחת מידע**״) עוסקת באבטחת תקשורת וקובעת כי העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות. עמדת הרשות להגנת הפרטיות היא כי המונח שיטות הצפנה מקובלות בתקנה זאת כולל במקרים המתאימים, אריזה של המידע, הצפנה של המידע בעת העברתו וכן הצפנה של תוך ההעברה.
[91] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן.
[92] הנחיית יה״ב 5.32 שימוש מאובטח ב google meet – התייחסות ל-Drive.
[93] הנחיית יה״ב 5.6 אבטחת דואר אלקטרוני.

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** **(הדרישות בכל קבוצה חליפיות אחת לשנייה)**	**א**	**ב**	**ג**	**ד**	
	8. קבצי הרצה (EXE, DMG וכיו״ב). 9. GIS File. 10. Medical Imaging File (כגון Dicom). **העלאת המידע על מדיות כגון:** 11. Hard Drive. 12. SSD. 13. USB Flash Drive. 14. Optical Disc. 15. Memory Card. 16. NAS storage. **מידע שמקורו בענן הציבורי** 17. Cloud Storage. 18. תדפיס.					
סניטציה של המידע בגוף המוסר	19. ללא סניטציה. 20. ביצוע בדיקת True Type 21. הלבנה.	19, 20, 21	20, 21	20, 21	21	בדיקת מרכיב זה מבוצעת אוטומטית בכל העברה בשדרת המידע,[95] MFT (כספות או Go

[95] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן; הלבנה מתבצעת אוטומטי ברכיב L7 ו-DataPower. יודגש שב-APGEE שירות ההלבנה לא ניתן באופן רוחבי ועל המשרד ליישם באופן עצמאי.

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** **(הדרישות בכל קבוצה חליפיות אחת לשנייה)**	**א**	**ב**	**ג**	**ד**	
לאיתור פוגענים[94]						Anywhere), גוגל דרייב ענני,[96] ודוא״ל ממשלתי.[97]
הצפנת המידע הגולמי במנוחה[98]	22. ללא צורך בהצפנה. 23. התממת מידע. 24. הצפנה סיסמה. 25. הצפנה מקובלת. 26. הצפנה ממלכתית.	22, 23	24, 25, 26	25, 26	25, 26	בדיקת מרכיב זה מבוצעת אוטומטית בכל העברה בשדרת המידע,[99] MFT (כספות או Go Anywhere), גוגל דרייב ענני,[100] דוא״ל ממשלתי,[101] ואתרי אינטרנט ממשלתיים.[102]
תווך העברת המידע בין הארגונים[103]	27. רשתות חברתיות (כגון – Facebook, LinkedIn ועוד). 28. דוא״ל ארגוני. 29. דוא״ל מאובטח. 30. פלטפורמות קולבורציה ושיתוף מידע (כגון – slack,	27 עד 45	28 עד 45	33 עד 45	33 עד 45	ראו פירוט מטה של התשתיות הרוחביות המרכזיות שקיימות.

[94] תקנה 13(א) לתקנות אבטחת מידע העוסקת בניהול ותפעול תקין של מערכות המאגר, מחייבת בין היתר לבצע סניטציה לאיתור פוגענים בגוף המוסר והמקבל בעת העברת מידע בין גופים ציבוריים. כמו כן, החובה לבצע סניטציה בגוף המוסר והמקבל לאיתור פוגענים מעוגנת בהנחיות יה״ב.
[96] הנחיית יה״ב 5.32 שימוש מאובטח ב google meet – התייחסות ל-Drive ; הלבנה אוטומטית על בסיס הספק.
[97] הנחיית יה״ב 5.6 אבטחת דואר אלקטרוני.
[98] תקי' 14(ב) לתקנות אבטחת מידע – ראו התייחסות לעיל.
[99] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן.
[100] הנחיית יה״ב 5.32 שימוש מאובטח ב google meet – התייחסות ל-Drive.
[101] הנחיית יה״ב 5.6 אבטחת דואר אלקטרוני.
[102] הנחיית יה״ב 5.17 בנושא אבטחת אתרי אינטרנט ממשלתיים.
[103] תקי' 14(ב) לתקנות אבטחת מידע – ראו התייחסות לעיל.

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** **(הדרישות בכל קבוצה חליפיות אחת לשנייה)**	**א**	**ב**	**ג**	**ד**	
	Teams, Meet, Monday.com ועוד). 31. משתמש ארגוני בפלטפורמות לניהול פרויקטים (כגון – Jira, Trello ועוד). 32. משתמש ארגוני Cloud Services (כגון- Google Drive, Drobox, OneDrive ועוד). 33. אתר אינטרנט מאובטח (כגון GOV.il). 34. כספת מידע 35. File Transfer Protocols (כגון – SFTP, FTPS). 36. SSLVPN. **ממשקים טכנולוגיים מאובטחים** 37. Rest API. 38. SOAP. 39. Direct Database Connection (כגון ODBC, JDBC). **קווי תקשורת ישירים** 40. תמסורת פרטית מוצפנת (כגון בזק מטרו ועוד). 41. S2SVPN. 42. Cloud Peering. 43. Blockchain.					

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** **(הדרישות בכל קבוצה חליפיות אחת לשנייה)**	**א**	**ב**	**ג**	**ד**	
	בלדרות 44. בלדרות רגילה. 45. בלדרות מאובטחת.					
סניטציה של המידע בגוף המקבל לאיתור פוגענים[104]	46. ביצוע בדיקת True Type 47. הלבנה.	46, 47	46, 47	47	47	בדיקת מרכיב זה מבוצעת אוטומטית בכל העברה בשדרת המידע,[105] MFT (כספות או Go Anywhere), גוגל דרייב ענני,[106] ודוא״ל ממשלתי.[107]
סינון המידע בעת קבלתו[108]	48. ללא סינון המידע בעת קבלתו. 49. סינון המידע בעת קבלתו.	48, 49	49	49	49	

[104] תקנה 13(א) לתקנות אבטחת מידע העוסקת בניהול ותפעול תקין של מערכות המאגר, מחייבת בין היתר לבצע סניטציה לאיתור פוגענים בגוף המוסר והמקבל בעת העברת מידע בין גופים ציבוריים. כמו כן, החובה לבצע סניטציה בגוף המוסר והמקבל לאיתור פוגענים מעוגנת בהנחיות יה״ב.
[105] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן; הלבנה מתבצעת אוטומטי ברכיב L7 ו-DataPower.
[106] הנחיית יה״ב 5.32 שימוש מאובטח ב google meet – התייחסות ל-Drive; הלבנה אוטומטית על בסיס הספק.
[107] הנחיית יה״ב 5.6 אבטחת דואר אלקטרוני.
[108] תקנה 6 לתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ״ו-1986 קובעת כי מקבל מידע שקיבל מידע לפי תקנות אלה יפריד מיד עם קבלת הנתונים את המידע העודף וימחק אותו מיד.

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** (**הדרישות בכל קבוצה חליפיות אחת לשנייה**)	**א**	**ב**	**ג**	**ד**	
רמת אבטחת המידע בגוף המקבל[109]	50. רמת אבטחה מוצהרת. 51. רמת אבטחה מוצהרת ומוכחת - ביחס למידע אישי הצהרה על עמידה בתקנות הגנת הפרטיות (אבטחת מידע) לרבות אישור על ביצוע סקר סיכונים ומבדקי חדירות (ביחס למאגרים ברמת אבטחה גבוהה). 52. רמת אבטחה נבדקת מטעם הגוף המוסר כולל הוכחות (מבדקי חוסן, עמידה בתקן, בודק מוסמך).	50, 51	51	51	52	בכל העברה בשדרת המידע,[110] MFT (כספות או Go Anywhere), גוגל דרייב ענני,[111] דוא״ל ממשלתי,[112] ואתרי אינטרנט ממשלתיים,[113] בדיקת מרכיב זה מבוצעת אוטומטית בגופים מונחי יה״ב או מס״ל.
הרשאות גישה למידע (מידור)[114]	53. ללא מידור כלל. 54. ביצוע מידור לפי מדיניות הארגון המקבל. 55. ביצוע מידור בהתאם לסוג בעלי תפקידים, להם נדרש המידע לתכלית מסוימת, לצורך מילוי תפקידם. 56. ביצוע מידור לפי בעל תפקיד מסוים או מספר מצומצם של	53, 54	54, 55	55	56	בכל העברה בשדרת המידע,[115] MFT (כספות או Go Anywhere), גוגל דרייב ענני,[116] דוא״ל ממשלתי,[117] ואתרי אינטרנט ממשלתיים,[118]

[109] לגבי מידע אישי – תקנות 5(ג)-5(ד) לתקנות אבטחת מידע מטילות חובה על בעלי מאגרי מידע ברמת אבטחה גבוהה לבצע סקר סיכונים ומבדקי חדירות. מאגרים ברמת אבטחה גבוהה הם מאגרים כאמור בפרט 1(1) או (3) בתוספת הראשונה לתקנות אבטחת מידע שיש בהם מידע על אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה עולה על 100.

[110] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן.

[111] הנחיית יה״ב 5.32 שימוש מאובטח ב google meet – התייחסות ל-Drive.

[112] הנחיית יה״ב 5.6 אבטחת דואר אלקטרוני.

[113] הנחיית יה״ב 5.17 בדבר אבטחת אתרי אינטרנט ממשלתיים.

[114] לגבי מידע אישי – תקנות 8–9 לתקנות אבטחת מידע מקימות חובה להטמיע מנגנון הרשאות למידע במאגר המבוסס על ״הצורך לדעת״ וכן חובה על בעל המאגר לקבוע הרשאות גישה של בעלי הרשאות למאגר בהתאם להגדרות התפקיד, ובמידה הנדרשת לביצוע התפקיד, כמו גם לנקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו כדי לוודא כי הגישה למאגר ולמערכותיו נעשית בידי בעל ההרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקופות.

[115] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן.

[116] הנחיית יה״ב 5.32 שימוש מאובטח ב-google meet – התייחסות ל-Drive.

[117] הנחיית יה״ב 5.6 אבטחת דואר אלקטרוני.

[118] הנחיית יה״ב 5.17 בדבר אבטחת אתרי אינטרנט ממשלתיים.

		סיווג המידע				תשתיות רוחביות קיימות אפשריות[87]
הנחיות	**דרכי מימוש** **(הדרישות בכל קבוצה חליפיות אחת לשנייה)**	**א**	**ב**	**ג**	**ד**	
	בעלי תפקיד, להם נדרש המידע לתכלית מסוימת, לצורך מילוי תפקידם.					בדיקת מרכיב זה מבוצעת אוטומטית בגופים מונחי יה״ב או מס״ל.
העברת המידע לצד ג' ונותני שירותים (שאינם גופים ציבוריים)[119]	57. מותר. 58. מותר לאחר שאלון ספקים תקין.[120] 59. מותר בכפוף לנקיטת אמצעי ביצוע בקרה ופיקוח בהתאם להוראות תקנה 15(א)(4) לתקנות אבטחת מידע.[121] 60. מותר לאחר קבלת אישור הגוף המוסר. אזור הנחיתה הממשלתי בנימבוס אינו נחשב לצד ג' לעניין זה.	57, 58	59	59	60	

<u>פירוט תשתיות מרכזיות רוחביות להעברת מידע בין גופים ציבוריים</u>[122]

1. **שדרת מידע**[123] – תשתית זו מתאימה לביצוע העברות של כל סיווגי המידע (א'-ד') בין גופים ציבוריים. בכל העברה באמצעות תווך שדרת המידע הממשלתית, בדיקת המרכיבים הבאים המבוצעת אוטומטית:
   a. אריזת המידע
   b. הצפנת המידע
   c. הלבנה – מתבצעת אוטומטי ברכיב L7 ו-DataPower. **יודגש שב-APIGEE שירות ההלבנה לא ניתן באופן רוחבי ועל המשרד ליישם באופן עצמאי.**

---

[119] יצוין כי העברת המידע לצד ג' ונותני שירותים שאינם גופים ציבורים תתבצע בכפוף להנחיות המפורטות במסמך זה. לגבי מידע אישי – תקנה 15 לתקנות אבטחת מידע מסדירה את אופן ההתקשרות בין הארגון לבין כל גורם חיצוני המספק לארגון שירות הכרוך במתן גישה למאגר המידע שלו.

[120] כגון שאלון הספקים לפי תקנה 15 לתקנות אבטחת מידע בנספח למדריך הפעולה להתקשרות עם ספקי מיקור חוץ בקישור: https://www.gov.il/BlobFolder/reports/guide_section_15/he/guide-section%2015.pdf או שאלון הספקים של מערך הסייבר בקישור https://www.gov.il/he/pages/querysupply.

[121] בהתאם לתקנה 15(ד) לתקנות אבטחת מידע הקובעת כי בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים.

[122] קיימות מערכות נוספות הפועלות במשרדים השונים, במידת הצורך תערך בהמשך בחינה של מערכות נוספות אלו והתאמתן לדרישות אבטחת מידע והגנת סייבר המפורטות במסמך זה.

[123] הנחיית יה״ב 5.21 שדרת המידע, והנחיית יה״ב 5.33.4 שדרת המידע בענן.

d. רמת אבטחת המידע בגוף המקבל – מתבצעת אוטומטית במצבים שמדובר בגופים מונחי יה"ב או מס"ל.
e. מידור המידע - מתבצעת אוטומטית במצבים שמדובר בגופים מונחי יה"ב או מס"ל.

2. **MFT (CyberArk או Go Anywhere)** – תשתית זו מתאימה לביצוע העברות של כל סיווגי המידע (א'-ד') בין גופים ציבוריים. בכל העברה באמצעות תווך מערכת הכספות Go Anywhere, בדיקת המרכיבים הבאים המבוצעת אוטומטית:
a. אריזת המידע
b. הצפנת המידע
c. תווך המידע
d. הלבנה
e. רמת אבטחת המידע בגוף המקבל – מתבצעת אוטומטית במצבים שמדובר בגופים מונחי יה"ב או מס"ל.
f. מידור המידע - מתבצעת אוטומטית במצבים שמדובר בגופים מונחי יה"ב או מס"ל.

3. **גוגל דרייב ענני**[124] – תשתית זו מתאימה לביצוע העברות של סיווגי המידע א'-ב' בין גופים ציבוריים. בכל העברה באמצעות תווך גוגל דרייב בחשבון הארגוני, בהינתן אישור ועדת הענן הממשלתית, בדיקת המרכיבים הבאים מבוצעת אוטומטית:
a. אריזת המידע
b. הצפנת המידע
c. תווך המידע
d. הלבנה אוטומטית על בסיס הספק
e. רמת אבטחת המידע בגוף המקבל – מתבצעת אוטומטית במצבים שמדובר בגופים מונחי יה"ב או מס"ל.
f. מידור המידע - מתבצעת אוטומטית בגופים מונחי יה"ב או מס"ל.

4. **דוא"ל ממשלתי**[125] - תשתית זו מתאימה לביצוע העברות של סיווגי המידע א'-ב' בין גופים ציבוריים. בכל העברה באמצעות תווך דוא"ל ממשלתי, בדיקת המרכיבים הבאים מבוצעת אוטומטית:
a. אריזת המידע
b. הצפנת המידע
c. הלבנת המידע
d. רמת אבטחת המידע בגוף המקבל – מתבצעת אוטומטית כאשר מדובר בגופים מונחי יה"ב או מס"ל.
e. מידור המידע - מתבצעת אוטומטית במצבים שמדובר בגופים מונחי יה"ב או מס"ל.

5. **אתרי אינטרנט ממשלתיים**[126] - תשתית זו מתאימה לביצוע העברות של מידע המסווג בסיווג א' בלבד בין גופים ציבוריים. בכל העברה באמצעות תווך אתר אינטרנט ממשלתי, בדיקת המרכיבים הבאים מבוצעת אוטומטית:
a. הצפנת המידע
b. רמת אבטחת המידע בגוף המקבל – מתבצעת אוטומטית בגופים מונחי יה"ב או מס"ל.
c. מידור המידע - מתבצעת אוטומטית בגופים מונחי יה"ב או מס"ל.

[124] הנחיית יה"ב 5.32 שימוש מאובטח ב google meet – התייחסות ל-Drive.
[125] הנחיית יה"ב 5.6 אבטחת דואר אלקטרוני.
[126] הנחיית יה"ב 5.17 אבטחת אתרי אינטרנט ממשלתיים.

בדיקה תקופתית – עדכניות ההוראות במסמך זה תיבחן מעת לעת על ידי ממערך הסייבר הלאומי, הרשות להגנת הפרטיות ויה״ב, ולכל הפחות אחת לשנתיים, או בעת הטמעת מערכת מרכזית חדשה להעברת מידע בין גופים ציבוריים.