

11 יוני, 2026
כ"ו סיוון, תשפ"ו

הגנת פרטיות בשימוש באמצעים לאימות גיל (Age assurance) במרחב המקוון

- טיוטה להערות הציבור -

1. "אימות גיל" (Age assurance) במרחב המקוון הוא מונח המיוחס לאמצעים מסוגים שונים, הננקטים במטרה לספק הערכה ברמת וודאות ודיוק משתנה בדבר גילם של משתמשים בשירותים מקוונים, וזאת, בין היתר, על בסיס עיבוד מידע אישי.¹
2. אימות גיל במרחב המקוון מתבצע לרוב לשלוש מטרות מרכזיות: מניעת גישת משתמשים לשירות מקוון מסוים על בסיס גילם; התאמת אופי שירות מקוון לגיל המשתמשים בו, כדוגמת אפליקציה המציגה סרטוני רשת המבקשת להתאים את אופי הסרטונים המוצגים בה לגיל המשתמשים;² ולשם ציות להוראות הדין, לרבות דיני הגנת פרטיות, ולהנחיות רגולטוריות.
3. נקיטת אמצעים לאימות גיל במרחב המקוון עשויה לתרום, בין היתר, לצמצום הגישה והחשיפה של ילדים לשירותים ולתכנים שאינם מותאמים להם, כמו גם לצמצום איסוף מידע על אודותיהם ברשת, ומכאן לחיזוק ההגנה על פרטיותם. מנגד, נקיטת הליכים שכאלו טומנת בחובה גם סיכונים פוטנציאליים משמעותיים לפרטיות משתמשים, ילדים ובגירים כאחד.
4. המסמך מיועד לארגונים הפועלים ברשת (כגון בעלי אתרי אינטרנט, רשתות חברתיות, חברות משחקים מקוונים, ונותני שירותים ברשת), המבקשים להשתמש באמצעים טכנולוגיים לאימות גיל במרחב המקוון, וליועצים המשפטיים וממוני הגנת הפרטיות של ארגונים אלו. המסמך יסקור את המתודות המרכזיות לאימות גיל, ינתח את הסיכונים המרכזיים לפרטיות העלולים להיגרם במסגרת נקיטת אמצעים לאימות גיל, ויצג הנחיות והמלצות לצמצום הפגיעה בזכות לפרטיות בעת נקיטת אמצעים שכאלו. אי-עמידה של ארגונים בהוראות הדין המחייבות עלולה, במקרים המתאימים, לגרור סנקציות מנהליות בדמות עיצומים כספיים מכוח חוק הגנת הפרטיות, לצד חשיפה לתביעות ולהליכים אזרחיים.

מתודות לאימות גיל במרחב המקוון – סקירה כללית

1. אמצעים לאימות גיל נועדו לאימות גילו של משתמש המבקש להשתמש בשירותים דיגיטליים, לקבל גישה לתכנים במרחב המקוון או, במקרה של קטינים, לשם אימות גיל הגורמים

¹ סעיף 3 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות') מגדיר "עיבוד" מידע אישי כ-"כל פעולה שמבוצעת על מידע אישי, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו".

² התאמת גיל משתמשים במקרים שכאלו עשויה להיעשות מטעמים שונים, כגון טעמים מסחריים ומטעמים של צמצום חשיפת ילדים צעירים לתכנים שאינם מותאמים להם, כגון תכנים אלימים או מיניים.

המאשרים את שימושם של הקטין בשירותים דיגיטליים או את גישתו לתכנים, כגון הוריו או אפוטרופוסים חוקיים אחרים (Verified parental consent).³

2. ככלל, ישנן שלוש מתודות מרכזיות לאימות גיל במרחב המקוון:⁴

א. **Age declaration – הצהרה עצמית**: מתודת אימות גיל המתבססת על הצהרה עצמית של משתמש בדבר גילו/מועד לידתו, אשר מוצגת, על-פי רוב, בעת כניסה לאתר, הורדת אפליקציה, או רישום לשירות מקוון,⁵ וללא צורך בראיות תומכות נוספות. מתודה זו נחשבת, כשלעצמה, כקלה לעקיפה ומכאן כפחות יעילה למניעת שימוש שאינו מותאם-גיל בשירותים מקוונים.

ב. **Age estimation – הערכת גיל**: מתודת אימות גיל שנועדה לספק הערכה בדבר גילו של משתמש, או את הימצאותו בטווח גילאים מסוים (כגון 8 עד 12 או 14 עד 18), וזאת על יסוד תהליכים טכנולוגיים שונים, כגון:

- עיבוד בזמן אמת של מידע ביומטרי (כגון תווי פניו של המשתמש, קולו, ואופן תנועתו);
- עיבוד מידע הנגזר מפרופיל חשבון משתמש, ממידע גלוי הנמצא על אודותיו ברשת, או מפעילותו בפלטפורמה מקוונת מסוימת, לרבות מידע על התנהגותו בפלטפורמה (Behavioral data), תחומי העניין שלו, זהות וגיל חבריו, ואופן השימוש שלו בשפה;
- עריכת מבדקים לבחינת רמת הידע הכללי והיכולות של המשתמש בהשוואה למשתמשים אחרים בעלי מאפיינים דומים.

ג. **Age verification – וידוא גיל**: מתודת אימות גיל המספקת אינדיקציה ברמת וודאות ודיוק גבוהה בדבר גיל המשתמש או היותו קטין או בגיר, וזאת תוך שימוש באחת או יותר מהטכניקות הבאות:

- אימות גיל משתמש על בסיס מסמכים רשמיים המהווים "מזהים קשיחים" (Hard identifiers) המועברים על-ידו, ובהם מוצגים תאריך לידתו ותמונתו – כגון תעודת זהות, רישיון נהיגה, ודרכון. התהליך עשוי לכלול לעיתים גם ביצוע השוואה בזמן אמת בין פניו של המשתמש לבין התמונה במסמכים שהוגשו על-ידו (Photo-ID matching);

³ החובה לשימוש באמצעים לאימות גיל במרחב המקוון מוסדרת, באופנים שונים, במספר הוראות דין והסדרים בינלאומיים. להרחבה ראו מרכז המחקר והמידע של הכנסת "מנגנונים לאימות גיל לצורך הגנה על קטינים בפלטפורמות דיגיטליות" (יוני 2024) (להלן: 'מסמך מרכז המחקר והמידע של הכנסת'); OECD, *The legal and Policy landscape of age assurance online for child safety and well-being – Technical paper*, (June, 2025).
⁴ להרחבה על המתודות השונות לאימות גיל במרחב המקוון ראו מרכז המחקר והמידע של הכנסת, לעיל ה"ש 3, וכן "Age assurance methods" שפורסמו על ידי רשות הגנת המידע הבריטית (ICO). לאופני חלוקה אחרים של מתודות אימות גיל ראו לדוגמה: Ofcom, *Guidance for service providers publishing pornographic content*, (Dec. 2023); CNIL, *Online age verification: balancing privacy and the protection of minors* (Sep. 2022).
⁵ ההצהרה בדבר גילו של משתמש עשויה להתקבל, בין היתר, באמצעות סימון ברובריקה בה המשתמש מצהיר כי הוא מעל גיל מסוים, או באמצעות הקלדת תאריך לידה.

- אימות גיל משתמש מול מאגר נתונים פומבי;
- בדיקת פרטי כרטיס אשראי של משתמש אשר מוזנים על-ידו לצורך וידוא כי הוא בגיל 18 ומעלה, או כחלק מביצוע תשלום עבור שירות. זיהוי זה יכול להיעשות גם באופן של זיהוי מבוסס ארנק דיגיטלי;
- אימות גיל על יסוד הצהרת גיל בנקאית, כגון מסמך אישור ניהול חשבון בנק;
- הסתייעות בצדדים שלישיים המציעים שירותי וידוא גיל אמינים (Trusted third party authentication services) על בסיס מידע הנאסף על אודות המשתמש ממקורות שונים, לרבות מהמשתמש עצמו, ושעל-פיו ניתן לקבוע את גילו מבלי לחשוף מידע אישי נוסף עליו.⁶ השימוש בשירות זה עשוי לאפשר לאמת את גיל המשתמש באופן המתאים לאופי השירות, מבלי שנותן השירות ייחשף לכל פרט נוסף.⁷ מתודה זו מתבססת ככלל על עיקרון ה"הוכחה באפס ידיעה" (Zero-knowledge proofs (ZKPs)).

דוגמה: אדם המבקש להירשם לשירות המיועד לבגירים פונה לחברה למתן שירותי וידוא גיל. על יסוד עיבוד מידע אישי המועבר לחברה על-ידי המשתמש ובהסכמתו, לרבות מידע כגון תעודת זהות, מידע ממקורות רשמיים/ממשלתיים או פרטי כרטיס אשראי, החברה מוודאת כי המשתמש הוא אכן בגיר. במצב שכזה החברה מייצרת אסימון (Token) המעיד כי המחזיק בו הוא אדם בגיר, וזאת באופן אנונימי ומבלי לכלול בו מידע אישי נוסף. האסימון מותקן במכשיר המשתמש, והוא מוצג על-ידו בעת רישום לכל שירות/אתר דיגיטלי המבקש לוודא כי הוא אינו קטין, מבלי שייאלץ לחשוף את זהותו בתהליך זה.

3. תהליך אימות גיל יכול להתבצע באמצעות שימוש באחת מהמתודות שפורטו לעיל, או תוך שימוש במספר מתודות באופן משולב (Waterfall techniques), וזאת כדי לספק תוצאה מצטברת עם רמת דיוק וודאות גבוהה יותר. שימוש משולב יכול להיות רלוונטי במיוחד בהקשר של אימות גילם של קטינים, ובמצבים בהם מתעורר חשש כי אימות גיל על יסוד מתודה אחת אינו מעניק את רמת הודאות הנדרשת בנסיבות העניין.

⁶ מתודה זו היא המומלצת על-ידי הרשות הצרפתית להגנת הפרטיות (CNIL). ראו ה"ש 4.
⁷ שימוש בארנק הזהות הדיגיטלית של האיחוד האירופי (EUDI Wallet) לצרכי אימות גיל מבטא יישום של המתודה האמורה. להרחבה ראו The European Commission, [The Age Verification Manual](#).

לדוגמה, משחק רשת המציג אלימות גרפית והמיועד לבגירים מגיל 18 ומעלה ביצע הליך של הערכת גיל שבסופו הגיע למסקנה כי גילו של משתמש מסוים עשוי לנוע בין הגילאים 16 עד 20. לפיכך, ולאור רצונו של מפעיל המשחק למנוע גישה של קטינים מתחת לגיל 18 לתכני המשחק, התבקש המשתמש לעבור גם תהליך של וידוא גיל על מנת לקבל חיווי מדויק ומוחלט בדבר גילו.

4. תהליך אימות הגיל יכול להתבצע באופן חד פעמי (כגון בנקודת הכניסה של משתמש לאתר או בעת רישום לשירות) או באופן מתמשך ובנקודות זמן נוספות.

לדוגמה, רשת חברתית, אשר קיבלה אינדיקציה כי גילו של משתמש שונה מהגיל עליו הוא הצהיר בעת רישומו לשירות, החליטה לנקוט אמצעי להערכת גילו של המשתמש על יסוד ניתוח התוכן אותו הוא צרך ופרסם ברשת החברתית בחודש שקדם למועד קבלת האינדיקציה. לאור ממצאי הבדיקה, ולאחר שנמצא כי התוכן שהמשתמש צרך ופרסם ברשת החברתית תאם לתוכן הצפוי והמקובל עבור משתמשים בטווח גילאים הכולל את הגיל עליו הוא הצהיר בעת הרישום לשירות, הופסק השימוש באמצעי לאימות הגיל.

5. עד כאן סקירת המתודות המרכזיות לאימות גיל. יש לציין כי במקביל למתודות אלו עשויים להיות כלים נוספים ששימוש בהם עשוי להביא להשגת מטרת צמצום הגישה של אוכלוסיות מסוימות (כגון קטינים) לתכנים ושירותים שאינם תואמים לגילם, וזאת שלא על יסוד איסוף ועיבוד מידע אישי. דוגמה מרכזית בעניין זה היא שימוש באמצעים **לסינון תכנים**, אשר בהתאם לדרישות מוגדרות מראש, מאפשרים "לחסום" גישת משתמשים לאפליקציות ואתרים המסווגים כפוגעניים, כגון אתרי פורנו ואתרי הימורים.⁸ אמצעים שכאלו יכולים לכלול גם **כלים לזיהוי וניתוח תכנים ספציפיים** (כגון תמונות או סרטונים פוגעניים, המועברים באמצעות רשתות חברתיות או אפליקציות להעברת מסרים מיידים) ולמנוע את הגישה לתכנים אלו. האמצעים יכולים להיות מותקנים על-גבי הרשת הביתית וכן באופן מקומי, במכשירי הקצה, כגון בטלפונים ובמכשירים החכמים ששימוש ילדים.

אפשרות נוספת היא לעצב את אופן השימוש בשירות בצורה שתייתר, או לכל הפחות תצמצם, את הצורך בשימוש באמצעים לאימות גיל. כך לדוגמה, חברה לשיווק ומכירת מוצרים ברשת יכולה להציג בפני משתמשים את הדרישה לאימות גיל רק כאשר מערכת ההזמנות שלה מזהה ניסיון לרכישה של מוצרי אלכוהול וטבק, וזאת במובחן מהאפשרות להצגת הדרישה עם הכניסה לאתר.

⁸ ספקיות תקשורת בישראל מחויבות לספק למנוייהם שירות סינון אתרים ותכנים פוגעניים ללא תשלום, וכן מחויבות להציע שירות זה באופן יזום ולאפשר הצטרפות לשירות זה בדרך קלה ומהירה. להרחבה ראו [כאן](#).

אימות גיל במרחב המקוון – סיכוני פרטיות

6. מרבית המתודות לאימות גיל במרחב המקוון מבוססות במהותן על איסוף ועיבוד של מידע אישי מסוגים שונים, לרבות מידע בעל רגישות מיוחדת, שלאורם מתקבלת החלטה בדבר גילו המשוערך או המדויק של אדם.⁹

7. כתלות במתודת ההליך, המידע האישי הנאסף ומעובד לצרכי אימות גיל עשוי לכלול את סוגי המידע הבאים:

- מסמכים רשמיים של המשתמש כגון תעודת זהות, רישיון נהיגה ודרכון, המכילים בין היתר מידע אישי רב, לרבות: שם המשתמש, תאריך לידתו, ארץ לידתו, שמות הוריו, חתימתו; הלאום אליו הוא משתייך, ועוד. כמו כן, המידע עשוי לכלול את תאריך הנפקת התעודה המשמש לעיתים כנתון מזהה לקבלת שירותי ציבוריים;

- מידע ביומטרי מסוג תמונתו של המשתמש או קולו;¹⁰

- מידע על אודות משתמש העשוי להיגזר מניתוח התנהלותו ברשת (בכלל או בפלטפורמה מסוימת), ובכלל זה מידע אישי על אודות דעותיו הפוליטיות, אמונותיו הדתיות והשקפת עולמו, מצבו הבריאותי או נטייתו המינית.

8. לאור כך, ביצוע הליכי אימות גיל במרחב המקוון כרוך בסיכוני פרטיות מסוגים שונים, כגון:

- איסוף מידע בעל רגישות מיוחדת, כגון מידע ביומטרי, או מידע רגיש אחר העשוי להיאסף ולהיות מעובד במסגרת ניתוח התנהלותו של משתמש ברשתות חברתיות (כדוגמת מידע על מצבו הרפואי של המשתמש, נטייתו המינית, מוצאו וכו'), אשר עשוי להילמד, בין היתר, מתוך האתרים בהם המשתמש מבקר, התכנים אותם הוא צורך, והפרסומים אותם הוא בוחר לשתף ברשת;¹¹

- דלף המידע האישי אשר נאסף ומעובד במסגרת הליכי אימות הגיל, וחשיפתו ברבים;¹²

⁹ חוק הגנת הפרטיות מגדיר "מידע בעל רגישות מיוחדת", בין היתר, כ"מידע אישי על צנעת חיי המשפחה של אדם, על צנעת אישיותו ועל נטייתו המינית"; מידע אישי המתייחס ל"מצב בריאותו של אדם"; מידע שהוא "מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב"; מידע על אודות "דעותיו הפוליטיות של אדם, אמונותיו או השקפת עולמו"; מידע שהוא "נתוני מיקום ונתוני תעבורה"; ומידע "על פעילותו הפיננסית".

¹⁰ חוק הגנת הפרטיות מגדיר "מזהה ביומטרי" – כ"נתון ביומטרי המשמש לזיהוי אדם או לאימות זהותו, או אמצעי ביומטרי שניתן להפיק ממנו נתון כאמור". המושג "ביומטרי" מוגדר בחוק כ"מאפיין אנושי, פיזיולוגי או התנהגותי, ייחודי, הניתן למדידה ממוחשבת".

¹¹ לעניין עצם האיסוף של מידע אישי כחלק מהזכות לפרטיות יפים דבריה של השופטת ברק-ארז בבג"ץ 6732/20 האגודה לזכויות האזרח בישראל נ' הכנסת (נבו, 1.3.2021) (להלן: "עניין האגודה לזכויות האזרח") בפסקה 12 לפסק דינה: "ראוי להדגיש כי הזכות לפרטיות כוללת בחובה לא רק הגנה מפני "גילוי" מידע הנוגע לאדם לצדדים שלישיים. ההגנה על זכות זו חייבת להתייחס גם לפעולות הקודמות לגילוי במישור הזמן – איסוף המידע ... הטלת הגבלות על איסוף מידע הנוגע לאדם ועל אגירתו באופן אלקטרוני היא חלק אינטגרלי מהזכות לפרטיות אף כאשר הוא אצור במאגר המידע ואינו נחשף בפני כול".

¹² סיכון זה הוא סיכון מרכזי בשל כך שאמצעים לאימות גיל מופעלים במקרים רבים בעת כניסה לאתרים ולשירותים שבמסגרתם עשוי להיאסף מידע בעל רגישות מיוחדת על אודות המשתמשים בהם, כגון אתרי הימורים ואתרי פורנוגרפיה. בשל כך, חשיפת מידע המעיד כי משתמשים מסוימים בילו באתרים אלו, או אף מידע רגיש יותר כגון תמונות או סרטונים של משתמשים שצולמו בעת שימושם באתרים אלו, עשוי לפגוע בפרטיותם של המשתמשים.

- שימוש במידע שנאסף לצרכי אימות גיל למטרות אחרות, כגון פרסום מותאם אישית, פרופילינג, וכדומה;¹³
 - איסוף ועיבוד מידע אישי לצרכי אימות גיל ללא יידוע המשתמש וקבלת הסכמתו לכך,¹⁴ או במצבים בהם אין בידי המשתמשים אפשרות סבירה לסרב להעניק הסכמתם;¹⁵
 - איסוף ועיבוד מידע עודף, שאינו נדרש למטרת אימות גיל המשתמש;¹⁶
 - שימוש במידע שנאסף לצרכי אימות גיל על-ידי גורמים לא מורשים.
9. מעבר לסיכונים אלו, שימוש נרחב מידי ולא מאוזן באמצעים לאימות גיל לשם מניעת גישת קטינים לאתרים ולתכנים מסוימים ברשת עלול לפגוע לא רק בפרטיותם של קטינים (פגיעה העלולה להיגרם, לדוגמה, במצב בו אתרי משחקים מקוונים המיועדים לקטינים מגיל 16 מפעילים אמצעי אימות גיל למניעת גישה של קטינים בגילאים צעירים יותר), אלא גם באינטרסים שונים הקשורים לשימושם ברשת.¹⁷
10. בראייה רחבה יותר, לשימוש אתרים ושירותים מקוונים באמצעים לאימות גיל עלולה להיות השפעה רחבה על היקף המידע האישי הנאסף במסגרת שימוש ברשת, ומכאן גם על מידת האנונימיות העומדת לכלל המשתמשים במרחב המקוון. כך, ככל שהשימוש באמצעים לאימות גיל במרחב המקוון יהפוך נרחב יותר, יגדל היקף המידע הרגיש שייאסף ויעובד על אודות כלל משתמשי הרשת, קטינים ובגירים כאחד, לרבות מידע אישי שמקורו מ"מזהים קשיחים" (כגון תעודות זהות) ומידע בעל רגישות מיוחדת, כגון מידע ביומטרי.
- משתמשים אשר יבקשו להיכנס לאתר מסוים או להוריד אפליקציה מסוימת יידרשו לתת הסכמתם לאיסוף ולעיבוד מידע בעל רגישות מיוחדת על עצמם, באופן אשר עלול להעניק לארגונים ולרשויות ציבוריות גישה נרחבת יותר למידע מזוהה על אודותיהם, להתיר להם לעבד ולהצליב מידע על אודות המשתמשים ממקורות שונים ועלומים, ולפגוע קשות במידת האנונימיות העומדת כיום למשתמשים ברשת. מצב עניינים זה עלול להוות צעד נוסף להפיכתו

¹³ ככלל, שימוש ללא הסכמה במידע אישי שלא למטרה שלשמה נמסר או למטרת המאגר בו הוא שמור מהווה הפרה של סעיפים 9(2) ו-8(ב) לחוק הגנת הפרטיות, בהתאמה.

¹⁴ מצב זה עלול להתרחש בנסיבות בהן אמצעים לאימות גיל מופעלים באופן סמוי או כאשר תהליכי היידוע וקבלת ההסכמה לעיבוד המידע לצרכי אימות גיל אינם מיושמים כנדרש ובהתאם להוראות הדין.

¹⁵ מצב זה עלול להתרחש בהקשר של אתרים או אפליקציות של שירותים חיוניים (כגון אתר אינטרנט של חברת חשמל) או כאלו המופעלים על-ידי גופים ציבוריים (כגון אתר אינטרנט של רשות מקומית או אפליקציה של קופת חולים). יישום אמצעים לאימות גיל באתרים ובשירותים כאלו עלול ליצור מצב בו אדם יהיה **מחויב** למעשה להסכים לאיסוף ועיבוד מידע רגיש על אודותיו לשם אימות גילו, וזאת בלי ברירה, ושלא מתוקף רצונו החופשי.

¹⁶ כך לדוגמה, הליך וידוא הגיל בהתבסס על איסוף ועיבוד מידע מתוך מסמכים רשמיים של משתמש (כגון תעודת זהות ודרכון), עלול להביא לאיסוף מידע שאינו נדרש לשם וידוא גיל המשתמש, כגון ארץ מוצאו, שמות הוריו, הסטאטוס המשפחתי שלו ועוד. להרחבה בעניין זה ראו גילוי הדעת של הרשות להגנת הפרטיות בנושא "איסוף מספרי תעודות זהות וצילום תעודות זהות" (2024). גילוי הדעת זמין [כאן](#).

¹⁷ להרחבה על חשיבותה של הזכות לפרטיות עבור קטינים ולסוגיית צמצום המרחבים השונים הרלוונטיים לחייהם בעידן הדיגיטלי כתוצאה משימוש בכלים למעקב אחר התנהלותם ברשת ובכלל, ראו סאני כלב "מרחבי ילדות? פרטיות, מעקב וצמצום המרחב הפרטי של קטינים בעידן הדיגיטלי" **משפט, חברה ותרבות** ב' 279 (2019).

של המרחב המקוון למרחב מנוטר שבו קל ופשוט יותר להתחקות אחר צעדיו של אדם במרחב זה, ולייצר תחושה של מעקב מקוון בקרב משתמשי הרשת בישראל.¹⁸

בעניין זה יפים דבריו של המשנה לנשיאה (בתוארו אז) א' ריבלין בעניין **רמי מור**, אשר ציין כי:

"האנונימיות היא גם חלק מן הזכות לפרטיות – מן החשובות שבזכויות ... חשיבותה של האנונימיות באינטרנט בולטת גם בהקשר של הזכות לפרטיות ... מקום שבו עושה אדם שימוש באינטרנט, בין שהוא מפרסם דבר-מה, בין שהוא משוטט באתרים לפי בחירתו, נוצר לגביו – לעיתים שלא בטובתו – מידע. לאורך זמן ניתן לומר כי נוצר לגביו מעין "מאגר מידע" הכולל פרטים רבים: החל מן הכתובת שבה הוא דר, דרך מספר כרטיס האשראי שבו הוא עושה שימוש, וכלה בתחומי העניין שלו ובעמדותיו בסוגיות שונות. משמעות הדבר היא שלצד הפלטפורמות באינטרנט המעניקות אנונימיות למשתמש, עלול האינטרנט לאיין את האנונימיות של מי שהפך חלק ממאגר המידע העצום האצור בו. אם בעבר לא הייתה מצויה בדרך-כלל גישה המונית למידע אישי ורגיש על הפרט, ומעשים בין ארבעת כתלי ביתו נותרו נסתרים מעיניהם של אחרים, בא האינטרנט ואפשר, בדרכים ישירות ועקיפות, לחדור אל תוך נבכי נפשו של היחיד. ניפוץ 'אשליית האנונימיות', במציאות שבה תחושת הפרטיות של הגולש היא מיתוס, עלול לעורר אסוציאציות של 'אח גדול'. פגיעה זו בפרטיות ראוי למזער. בגבולות ראויים ראוי לשמר את מקלטי האנונימיות כחלק מתרבות הגלישה באינטרנט. ניתן לומר כי במידה רבה האנונימיות עושה את האינטרנט למה שהוא, ובלעדיה ייגרע מן החופש במרחב הווירטואלי".¹⁹

בנוסף לכל האמור יש לזכור כי בעוד שהפגיעה בפרטיות בשימוש באמצעים לאימות גיל היא, על-פי רוב, ברורה ומובהקת, הגם שעוצמתה משתנה בין המתודות השונות, הרי שיעילותם של אמצעים אלו, **בכל מתודה שהיא**, נמצאת במחלוקת ואף מוטלת בספק.²⁰

ניתוח המתודות והאמצעים לאימות גיל בראי הפגיעה בפרטיות

11. שימוש באמצעים לאימות גיל כרוך במהותו בפגיעה בפרטיות. מידת הפגיעה בפרטיות העלולה להיגרם כתוצאה משימוש באמצעים לאימות גיל תלויה במספר משתנים שונים, וביניהם:

- רגישות המידע הנאסף והמעובד לצרכי אימות הגיל;

¹⁸ השוו: פסקה 18 לפסק דינה של הנשיאה חיות בעניין **האגודה לזכויות האזרח**, לעיל ה"ש 11, שם נקבע, בהקשר לשימוש בכלי שירות הביטחון הכללי למעקב אחר מגעים של חולי קורונה לשם למניעת התפשטות הנגיף, כי: "איסוף המידע, לצד היעדר השקיפות בנוגע לסוג המידע שנאסף ולאופן השימוש בו, יש בהם כדי ליצור תחושת מעקב אשר 'לעצם קיומה' [...] יש אפקט מצנן' ואשר גורמת לפגיעה קשה בזכות לפרטיות".

¹⁹ רע"א 4447/07 **רמי מור נ' ברק אי.טי.סי.** [1995] **החברה לשרותי בזק בינלאומיים בע"מ** (נבו 25.03.2010) (להלן: "עניין רמי מור"), פסקאות 13 ו-16 לפסק דינו של המשנה לנשיאה ריבלין.

²⁰ ראו לדוגמה: James Titcomb, [The VPNs allowing youngsters to bypass Online Safety Act rules](#), THE TELEGRAPH (31.7.2025).

- היקף המידע המעובד ;
- מטרת השימוש באמצעים, ובכלל זה האם השימוש נעשה לשם קבלת הערכה בדבר גיל המשתמשים או לשם וידוא גילם המדויק ;
- כמות, מגוון וסוגי מקורות המידע בהם נעשה שימוש להערכת גילם של משתמשים, ובכלל זה האם המידע נאסף אך ורק מהמשתמש עצמו, ממספר מקורות ספציפיים, קבועים וידועים, או שמא גם ממקורות נוספים ומשתנים כגון מקורות מידע פומבי ברשת ;
- זהות הגורם המבצע, קרי האם עיבוד המידע מתבצע על-ידי הארגון עצמו או באמצעות גורמים שלישיים (ספקי חוץ) ;
- כמות וזהות הגורמים להם עומדת הרשאת גישה למידע האישי המעובד במסגרת ההליך, ובכלל זה האם המידע נשמר אך ורק בידי הגורם המבצע את אימות הגיל או שמא הוא מועבר גם לידי גורמים נוספים, לרבות הארגונים המבקשים את ביצוע הליך אימות הגיל ;
- נקודות זמן איסוף המידע, ובכלל זה האם המידע נאסף רק פעם אחת ובנקודת הכניסה לאתר/שירות או שמא גם בנקודות זמן נוספות או באופן מתמשך, כגון בעת גלישה באתר ובמסגרת שימוש בשירות ;
- מספר האמצעים והמתודות לאימות גיל בהם נעשה שימוש, קרי האם נעשה שימוש באמצעי/מתודה אחד/ת או בשילוב של מגוון אמצעים ומתודות ;
- האם הליך אימות הגיל מבוצע באמצעות טכנולוגיה מוכרת ומבוססת או באמצעות טכנולוגיה חדשה ;
- קיומן של חובות משפטיות או רגולטוריות, לרבות חובות המחייבות שימוש באמצעים לאימות גיל.

12. בחינת שיקולים אלו ואחרים עשויה לסייע לארגונים בניתוח וסיווג אמצעי אימות הגיל השונים בראי פגיעתם בפרטיות, ומכאן לסייע להם בבחירת האמצעי בו הם יעשו שימוש, ובדבר המנגנונים שעליהם לנקוט לצמצום הפגיעה בפרטיות העלולה להיגרם כתוצאה משימוש זה.

13. יובהר כי השפעתם של השיקולים האמורים על מידת הפגיעה בפרטיות העלולה להיגרם כתוצאה משימוש באמצעים לאימות גיל עשויה להשתנות ביחס לאופן יישומם בכל מקרה ומקרה.

כך לדוגמה, שימוש באמצעים להערכת גיל נחשב ככלל כפוגעני פחות לפרטיות משימוש באמצעים לוידוא גיל (כגון כאלו המתבססים על איסוף ועיבוד מידע אישי ממסמכים רשמיים), וזאת מהטעם שאמצעים אלו לא נועדו לאסוף, לעבד ולליצר (Generate) מידע מדויק על אודות גילו של אדם, אלא רק מידע מוערך בנוגע להשתייכותו לקבוצת גיל מסוימת.

עם זאת, ישנם מצבים בהם שימוש באמצעים להערכת גיל עלול להיחשב כפוגעני יותר לפרטיות מאשר שימוש באמצעים לוודא גיל. כך לדוגמה, כאשר הערכת גילו של אדם מתבססת על שימוש במידע הביומטרי שלו (שעצם איסופו וכן האפשרות לזליגתו או לשימוש בו לשם זיהויו של אדם הופכים אותו לבעל פוטנציאל לפגיעה קשה בפרטיות), או כאשר השימוש באמצעים להערכת גיל כולל ניטור מתמשך, מעמיק ורציף של התנהלותו של אדם ברשת – הרי שהשימוש באמצעים אלו להערכת גילו של אדם עשוי להיחשב פוגעני יותר לפרטיות, לעומת אמצעים לוודא גיל המתבססים למשל על איסוף חד-פעמי של מסמכים רשמיים כגון תעודת זהות.

במובן זה, אופן השימוש באמצעים לאימות גיל, והמנגנונים בהם נעשה שימוש לצמצום הפגיעה בפרטיות (אשר חלקם יפורטו בהמשך), עשויים להשפיע רבות על הסיכון לפגיעה בפרטיות הכרוך בשימוש באמצעים אלו, וזאת מעבר לשאלת סוג האמצעי בו נעשה שימוש.

14. בהמשך לאמור, ועל יסוד כל שפורט עד כה, ניתן לסווג באופן כללי את האמצעים המרכזיים לאימות הגיל לשלוש קבוצות, וזאת על יסוד מידת הפגיעה האפשרית שלהם בפרטיות משתמשים:

❖ **אמצעים שפגיעתם בפרטיות נחותה** – אמצעים המעבדים מידע אישי מועט, שאינו בעל רגישות מיוחדת, הנמסר ישירות מהמשתמש עצמו, ואשר אינם מצליבים ומאמתים מידע זה מול מידע ממקורות נוספים.

תחת קבוצה זו ניתן ככלל לציין אמצעים מסוג המתודה של "הצהרה עצמית", אשר אוספים נתונים מעטים על אודות משתמשים על יסוד הצהרתם (כגון תאריך לידתם) ואינם כרוכים באיסוף מידע אישי נוסף לוודא אמיתות הנתונים. כאמור, אמצעים אלו נחשבים כקלים לעקיפה וכפחות יעילים למניעת שימוש לא מותאם גיל בשירותים מקוונים.

❖ **אמצעים שפגיעתם בפרטיות בינונית/מתונה** – אמצעים המעבדים מידע אישי שאינו בעל רגישות מיוחדת, שמקורו במשתמש עצמו ובמקורות ספורים, ספציפיים ורשמיים.

תחת קבוצה זו ניתן לציין אמצעים להערכת גיל מסוג עריכת מבדקים לבחינת רמת הידע הכללי והיכולות של המשתמש בהשוואה למשתמשים אחרים בעלי מאפיינים דומים, וכן אמצעים לוודא גיל מסוג אימות גיל משתמש מול מאגר נתונים פומבי; בדיקת פרטי כרטיס אשראי של משתמש; הצהרה בנקאית; ואמצעים מסוג הסתייעות בצדדים שלישיים המציעים שירותי וידוא גיל אמינים.

❖ **אמצעים שפגיעתם בפרטיות גבוהה** – אמצעים המעבדים מידע אישי בעל רגישות מיוחדת, הנאסף מתוך מספר רב ומשתנה של מקורות (לרבות מזהים קשיחים).

תחת קבוצה זו ניתן לציין אמצעים מסוג "עיבוד בזמן אמת של מידע ביומטרי של משתמשים"; אמצעים להערכת גיל על יסוד "עיבוד מידע הנגזר מפרופיל חשבון משתמש או מפעילות ברשת או בפלטפורמה מקוונת מסוימת"; ואמצעים לאימות גיל משתמש על

בסיס מסמכים רשמיים המהווים "מזהים קשיחים" (Hard identifiers) המועברים על-ידו, ובהם תאריך לידתו, ארץ מוצאו ותמונתו (כגון תעודת זהות, רישיון נהיגה, ודרכון).

15. כאמור, פוטנציאל ומידת הפגיעה בפרטיות בשימוש באמצעים השונים לאימות גיל עשויים להיות מושפעים גם משיקולים שונים (כגון אלו שפורטו קודם לכן), מאופן יישומם בפועל של האמצעים, וכן מהמנגנונים וההסדרים הננקטים לצמצום הפגיעה בפרטיות הכרוכה בשימוש בהם, אשר חלקם יפורט בהמשך מסמך זה.

16. בנוסף לאמצעים שפורטו לעיל יצוין כי שימוש באמצעים לסינון תכנים, אשר מציעים מניעת גישה לתכנים מסוימים בהתאם להגדרה קבועה מראש (כדוגמת סינון תכנים בעלי אופי פוגעני בשעות בהן ילדים נוטים לצרוך תכנים ברשת), אינו מבוסס על איסוף ועיבוד מידע אישי של משתמשים, ומכאן ששימוש בו אינו כרוך בפגיעה בפרטיות כלל.

אימות גיל במרחב המקוון – הנחיות והמלצות

17. הליך אימות גיל הוא הליך הכרוך, על-פי רוב, בעיבוד מידע אישי. ארגונים המשתמשים באמצעים לאימות גיל, ובמסגרת זו אוספים ומעבדים מידע אישי, בעצמם או באמצעות גורמים שלישיים, מחויבים בהתאם לכך בעמידה בהוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו. להלן יפורטו הנחיות והמלצות הרשות בנושא:

בחינת ובחירת אמצעי ומתודה לאימות גיל

18. על בעלי אתרים, אפליקציות וארגונים המציעים שירותים דיגיטליים ברשת, אשר בוחנים הטמעה ושימוש באמצעים לאימות גיל, לשקול במסגרת כלל שיקוליהם גם את פוטנציאל ומידת הסיכון לפגיעה בפרטיות משתמשים העלולה להיגרם כתוצאה מנקיטת אמצעים אלו.²¹ בארגונים בהם חלה חובת מינוי של ממונה הגנה על הפרטיות (כפי שיפורט בסעיפים 37-38 למסמך זה), בחינה זו צריכה להתבצע כחלק מתפקידו של הממונה.²²

19. הבחינה צריכה להיעשות, בין היתר, ביחס לחובות משפטיות ורגולטוריות החלות ביחס לשימוש באמצעים לאימות גיל (ככל שאלו קיימות), לסיכונים העלולים להיגרם כתוצאה מגישת משתמשים בגילאים מסוימים לשירותים ולתכנים שאינם מותאמים להם, למידת הפגיעה בפרטיות וסיכוני אבטחת מידע הכרוכים בשימוש בשירותים שכאלו, ועוד.

20. לגישת הרשות, שקלול נכון של הדברים צריך להתבטא ביצירת מדרג המאזן בין אופי השירות ומידת הסיכון הכרוכה בו למשתמשים (כגון הסיכון בחשיפת ילדים לתכנים שאינם מותאמים

²¹ בחינה זו רצוי שתיעשה במסגרת הליך "עיצוב לפרטיות" (Privacy by Design). דגש מיוחד רצוי לשים בהקשר זה על עריכת תסקיר השפעה על פרטיות. להרחבה ראו "תסקיר השפעה על פרטיות – מדריך עזר מתודולוגי" (2022).

²² בארגונים בהם חלה חובת מינוי ממונה הגנה על הפרטיות על הממונה לקדם הטמעה של עיקרון העיצוב לפרטיות בארגון, ולהיות מעורב באופן אפקטיבי בניתוח השלכות השימוש בטכנולוגיות חדשות ובהערכת סיכוני הפרטיות הנובעים מפעילות הארגון. להרחבה בעניין זה ראו טיוטת גילוי דעת הרשות להגנת הפרטיות בנושא "מינוי ממונה על הגנת הפרטיות בארגון לפי דרישות תיקון 13 לחוק הגנת הפרטיות" (יולי 2025).

להם, לרבות סיכוני אבטחת מידע) ולארגון (לדוגמה, במצב של הפרת הוראות דין האוסרות על פרסומת ושיווק המכוונים לקטינים או מכירת אלכוהול וטבק לקטינים), לבין מידת הפגיעה בפרטיות משתמשים הכרוכה בשימוש באמצעים שכאלו.

בהתאם לכך, עמדת הרשות היא כי שימוש באמצעי אימות גיל שפגיעתם בפרטיות גבוהה יחרוג על-פי רוב במידה משמעותית מהנחוץ לצורך מטרת אימות גיל משתמשים, וכי השימוש באמצעים שכאלו עשוי להיות מוצדק רק במצבים הבאים:

א. **כאשר קיימת הוראה חוקית או רגולטורית המחייבת שימוש באמצעים שהוגדרו ככאלו שפגיעתם בפרטיות גבוהה;**²³

ב. **כאשר ניתן להצביע על סיכון מוחשי ומשמעותי העלול להיגרם למשתמשים קטינים המצדיק את השימוש באמצעים שכאלו, חרף הפגיעה הקשה בפרטיות הכרוכה בו.**

במצבים בהם תנאים אלו אינם מתקיימים, וכאשר שימוש באמצעים שפגיעתם בפרטיות בינונית/מתונה או נמוכה עשוי להיות מתאים לאופי השירות ולמידת הסיכון הנובע ממנו – יש לתת עדיפות לשימוש באמצעים אלו, ולהימנע משימוש באמצעים שפגיעתם בפרטיות גבוהה.

21. גופים שעליהם חלה חובת המידתיות מכח המשפט הציבורי המבקשים להשתמש באמצעים לאימות גיל, נדרשים לעמוד לשם כך בשלושת מבחני המידתיות, ובכלל זה לוודא שהאמצעי הנבחר על-ידם תואם להשגת המטרה לשמה נעשה שימוש באמצעים אלו (מבחן הקשר הרציונאלי); לבחור באמצעי לאימות גיל המשיג מטרה זו תוך פגיעה מינימלית בפרטיות משתמשים (מבחן הפגיעה הפחותה); וכי התועלת בשימוש באמצעי עולה על הפגיעה בפרטיות הנגרמת כתוצאה מהשימוש בו (מבחן המידתיות במובן הצר). **ביחס לגופים אלו, שימוש באמצעים לאימות גיל שפגיעתם בפרטיות גבוהה, ללא הצדקה מספקת לכך, ובנסיבות שגם אמצעים שפגיעתם מתונה יותר עשויים להשיג את אותה התכלית, עלול להיחשב שימוש שאינו מידתי.**

צמידות המטרה (הגבלת עיבוד המידע)

22. סעיף 9(2) לחוק הגנת הפרטיות קובע כי שימוש בידעיה על עניניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה, מהווה פגיעה בפרטיות. על-פי סעיף 8(ב) לחוק הגנת הפרטיות, על בעלי שליטה ומחזיקים במידע חל איסור לעבד מידע אישי במאגר מידע "אלא למטרת המאגר שנקבעה לו כדין".

23. לאור האמור, **על ארגונים האוספים ומעבדים מידע אישי למטרת אימות גיל משתמשים (אם בעצמם ואם באמצעות צדדים שלישיים), להשתמש במידע שנאסף אך ורק למטרה זו.**

²³ נכון למועד פרסום המסמך, לא מוכרות לרשות הוראות חוקיות או רגולטוריות מסוג זה.

כך לדוגמה, עיבוד מידע ביומטרי למטרת הערכת גיל משתמש יכול להתבצע אך ורק למטרה זו. שימוש במידע הביומטרי לכל מטרה אחרת שלא ניתנה לגביה הסכמת המשתמש, כגון לצרכי זיהוי או אימות זהות שאינה נוגעת לאימות הגיל, יהווה הפרה של עיקרון צמידות המטרה ושל הוראות סעיפים (9)2 ו-8(ב) לחוק הגנת הפרטיות.²⁴

צמצום מידע עודף

24. **על ארגונים המבקשים להשתמש באמצעים לאימות גיל לבחון ולהגדיר את סוג והיקף המידע האישי המינימלי הנדרש לשם אימות גיל המשתמשים כתלות בשירות אותו הם מספקים, ולהימנע מאיסוף והחזקה של מידע עודף שאינו נדרש לשם מטרה זו.**

25. **על יסוד האמור, וכתלות בשירות אותו הם מספקים (ובדרישות חוקיות/רגולטוריות, ככל שכאלו קיימות), על ארגונים להקפיד להשתמש באמצעים לאימות גיל באופן אשר אינו מביא לאיסוף ועיבוד מידע עודף, שאינו נדרש לשם מטרת אימות גיל.**

כך לדוגמה, על אפליקציה לשירותי היכרויות לגיל השלישי, המבקשת לאמת את גיל המשתמשים בשירותה על יסוד מידע מתוך תעודות הזהות שלהם, לאסוף ולעבד אך ורק מידע המצוין בתעודה מתוכו ניתן ללמוד על גיל המשתמשים (כגון תאריך לידתם), ולהימנע מלאסוף, לאחסן או לעבד כל מידע אישי אחר המצוין בתעודה.

26. **על מנת לעמוד בעקרונות צמידות המטרה וצמצום המידע, כדי לצמצם את הסיכון לפגיעה שאינה מוצדקת בפרטיות משתמשים, ובתלות באופי השירות והחובות המשפטיות/רגולטוריות החלות עליהם, על ארגונים לפעול, ככל הניתן, על-פי כללי האצבע המפורטים להלן:**

א. **הימנעו משימוש במספר אמצעים לאימות גיל במקביל, אלא בנסיבות ובמצבים בהם קיימת הצדקה לכך, כגון במצבים בהם מתעורר חשש כי גילו האמיתי של משתמש אינו תואם לגיל שהוצהר על ידו בעת הרישום לשירות.**

ב. **השתמשו באמצעים לאימות הגיל באופן אשר יספק אינדיקציה ברמת הוודאות הנדרשת בדבר גיל המשתמשים, אך ללא מתן גישה למידע אישי נוסף שנאסף ועובד במסגרת ההליך.**

לדוגמה, שימוש באמצעי מסוג "הסתייעות בגופים שלישיים" יכול לאפשר לארגונים לקבל הערכה אמينة באמצעות גופים שלישיים בדבר גיל המשתמשים בשירותיהם, וזאת מבלי שמידע אישי על אודות משתמשים יועבר אליהם ויוחזק על-ידם.

²⁴ איסוף ועיבוד מידע ביומטרי בהליכים להערכת גיל נועדו לאפשר שימוש במאפיינים ביומטריים של אדם על מנת להעריך את גילו (לדוג' באמצעות ניתוח קמטים המופיעים על פניו של אדם וכו'). לפיכך, שימוש במידע ביומטרי שנאסף לצרכי הערכת גיל למטרת זיהוי של אדם או לצרכי אימות זהות, שלא לצורך הערכת הגיל, לדוגמה באמצעות השוואת תכונות תווי הפנים לתמונות המצויות במאגר נתונים, מהווה שימוש שלא למטרה במידע.

ג. לאחר בחירת אמצעי לאימות גיל, בחרו במקורות מידע אשר במסגרת האמצעי הנבחר מצמצמים את האפשרות לאיסוף, עיבוד וחשיפה של מידע עודף, שאינו נדרש לשם אימות גיל המשתמשים, והשתמשו בטכנולוגיות מגבירות פרטיות (PETs) לצמצום הסיכונים הכרוכים בהחזקת המידע.²⁵

לדוגמה, בהליך אימות גיל על יסוד מידע ממסמכים רשמיים – עצם כך שמשתמש מחזיק ברישיון נהיגה עשוי להעיד, ברמת וודאות גבוהה, כי הוא מעל גיל 16. בנסיבות שאימות ברמה זו הוא מספק, קשה לראות צורך באיסוף מידע נוסף המפורט ברישיון הנהיגה או באיסוף מסמכים רשמיים אחרים בהם מפורט מידע אישי נוסף שאינו נדרש, כדוגמת תעודת זהות.

ד. לאחר ביצוע הליך אימות הגיל בנוגע למשתמש מסוים, הקפידו להחזיק ולאחסן רק את המידע המינימלי הדרוש לשם המשך מתן השירות לאותו המשתמש, ולמחוק כל מידע אחר שנצבר במסגרת ההליך ושאינו עוד הצדקה להחזיקו.

לדוגמה, בנסיבות בהן אין חובה או הצדקה לשמור מידע על אודות גילם המדויק של משתמשים במאגרי המידע של הארגון (ככל שמידע שכזה נאסף במסגרת הליך אימות הגיל) – ניתן לשמור אך ורק מידע בינארי המבטא את השתייכותם של משתמשים לקבוצות גיל שונות (כגון: קטין/בגיר; משתמש מעל גיל 40/משתמש מתחת לגיל 40).

יודגש: אחסון מידע אישי בו נעשה שימוש לצרכי אימות גיל במאגר מידע, בנסיבות בהן אחסון זה אינו נדרש לביצוע המטרה שלשמה הוא נאסף, עלול להיחשב הפרה של עקרונות צמידות המטרה וצמצום המידע, ושל הוראות הדין המבטאים עקרונות אלו.

27. נזכיר כי על-פי תקנה 2(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'תקנות אבטחת מידע'), על ארגונים לבחון, אחת לשנה, האם קיים מידע עודף במאגריהם. אם מתברר לארגון כי הוא מחזיק במאגריו מידע אשר נאסף ועובד לצרכי אימות גיל משתמשים, וכי שמירתו של המידע האמור אינו נדרשת עוד לשם מטרה זו, עליו לפעול לצמצמו, לרבות באמצעות מחיקתו.²⁶

28. כמו כן, וכפי שיפורט גם בהמשך, על ארגון המתקשר עם גורם חיצוני לקבלת שירות מסוג אימות גיל להתייחס במסגרת התקשרות זו גם להיבט מחיקת המידע בו נעשה שימוש למטרה זו. בהתאם לעיקרון צמצום המידע, ובתלות בחובות משפטיות ואחרות, מומלץ כי ארגונים ינחו

²⁵ להרחבה ראו מדריך הרשות להגנת הפרטיות בנושא "טכנולוגיות מגבירות פרטיות (PETs)" (פברואר 2025). ככל שאמצעי אימות הגיל בהם נעשה שימוש הם אמצעים מבוססים בינה מלאכותית, מומלץ לבחון גם שימוש בטכנולוגיות מגבירות-פרטיות במערכות בינה מלאכותית. להרחבה ראו הרשות להגנת הפרטיות "מדריך ליישום טכנולוגיות מגבירות-פרטיות במערכות בינה מלאכותית (PETs AI)" (דצמבר 2025).

²⁶ להרחבה ראו טיוטת גילוי הדעת של הרשות להגנת פרטיות בנושא "צמצום מידע (Data Minimization) – מסמך מדיניות".

את הגורמים החיצוניים הפועלים מטעמם למחוק את המידע ששימש אותם לביצוע הערכת הגיל, לאחר העברת תוצאת ההליך לידיהם.

יידוע, הסכמה והגנות סעיף 18

29. **על ארגונים המבקשים לאסוף ולעבד מידע אישי על אודות משתמשים למטרת ביצוע הליך של אימות גיל, ליידע את המשתמשים על כך, ובכלל זה לציין בפניהם את פרטי המידע הבאים:**²⁷

- האם חלה עליהם חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונם ובהסכמתם ומהי תוצאת אי-ההסכמה;
- המטרה אשר לשמה מבוקש המידע;
- שמו של בעל השליטה במאגר המידע, ודרכי ההתקשרות עימו; למי יימסר המידע ומטרות המסירה;
- קיומן של זכות עיון במידע האישי לפי סעיף 13 ושל זכות לבקש תיקון של המידע האישי לפי סעיף 14 לחוק הגנת הפרטיות.

30. **איסוף ועיבוד מידע אישי למטרת אימות גיל יכולים, ככלל, להיעשות רק על יסוד הסכמה בדין או הסכמת נושאי מידע.** כתלות באמצעי בו נעשה שימוש, ביצוע פעולות לאיסוף ועיבוד מידע אישי למטרת אימות גיל ללא קבלת הסכמה עלול, בנסיבות מסוימות, להיחשב כפגיעה בפרטיות על יסוד הוראות סעיפים 1(2), 2(3), 2(6), 2(9) ו-11(2) לחוק הגנת הפרטיות.

בעניין זה יובהר כי על-פי סעיף 8(ד1) לחוק הגנת הפרטיות, חל איסור על עיבוד מידע אישי במאגר מידע, אשר נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק הגנת הפרטיות או להוראות כל דין אחר המסדיר עיבוד מידע.

31. **בנסיבות שאיסוף המידע והשימוש בו למטרת אימות גיל נעשים מכח הסכמת המשתמש – על ארגונים לוודא כי הסכמה זו הינה הסכמה תקפה על-פי דיני הגנת הפרטיות, קרי שהיא ניתנת מדעת ועל בסיס רצון חופשי של המשתמשים.**²⁸

32. לשם כך, על ארגונים להציג בפני משתמשים את כלל הנתונים הנדרשים, באופן סביר, לשם קבלת החלטתם בעניין, ולעשות כן בצורה ברורה, פשוטה להבנה, ותמציתית.

בשימוש באמצעים לאימות גיל האוספים ומעבדים מידע על אודות משתמש ממקורות שונים ברשת, יש לפרט בפני נושא המידע את מקורות המידע מהם עשוי המידע להיות מחולף ומעובד, וזאת בטרם הוא מעניק את הסכמתו לביצוע תהליך אימות הגיל.

²⁷ ראו סעיף 11 לחוק הגנת הפרטיות.

²⁸ ראו גילוי הדעת של הרשות להגנת הפרטיות בנושא "הסכמה בדיני הגנת הפרטיות" (פברואר 2025).

33. במידה והשירות מיועד בעיקרו לאוכלוסיות מיוחדות (קטינים, אנשים עם מוגבלות, עולים) – יש להתאים את תוכן ההסכמה ואת אופן הצגתה למאפיינים הייחודיים של האוכלוסייה.

34. לאור הסיכון המשמעותי לפגיעה בפרטיות הכרוך בביצוע הליך לאימות גיל ורגישות המידע המעובד למטרה זו (בוודאי בשימוש באמצעים שפגיעתם גבוהה), ולאור כך שאיסוף המידע עשוי להתבצע במסגרת ההתנהלות הרשית היומיומית והשכיחה, קיים חשש כי הישענות על הסכמה מכללא של משתמשים לאיסוף ועיבוד מידע אישי למטרת אימות גיל עלולה שלא להיות מספקת לביסוס ותיקוף רכיבי ההסכמה הנדרשים (מדעת ורצון חופשי).

לפיכך, מומלץ שארגונים המבקשים להתבסס על הסכמת משתמשים לאיסוף ועיבוד מידע אישי לצרכי אימות גיל יפעלו לקבלת הסכמתם המפורשת של המשתמשים לכך, וימנעו, ככל האפשר, מהישענות על הסכמה משתמעת מצד משתמשים בעניין זה.

35. ארגונים המבקשים לנקוט אמצעים לאימות גיל שלא על יסוד הסכמת המשתמשים ותוך הסתמכות על ההגנות המנויות בסעיף 18 לחוק הגנת הפרטיות (כגון סעיפים 18(2)(ב) ו-18(2)(ג)), צריכים לעמוד בדרישת המידתיות (ראו סעיף 20(ב) לחוק). דהיינו, הם מחויבים להשתמש באמצעים לאימות גיל שפגיעתם בפרטיות המשתמשים היא הפחותה ביותר האפשרית בנסיבות העניין.

כמו כן, על ארגונים אלו להיות מסוגלים להצביע על הסיבות והאינטרסים הלגיטימיים המצדיקים, לגישתם, את הפגיעה בפרטיות המשתמשים ללא הסכמתם לכך, שאם לא כן הם עלולים להיות מוחזקים כמי שפגעו בפרטיות באופן לא מידתי לצורך האינטרסים להם ניתנה ההגנה בסעיף 18, וכמי שפעלו שלא בתום לב.

חובת מינוי ממונה על הגנה על פרטיות

36. עצם השימוש באמצעים לאימות גיל עשוי, בנסיבות מסוימות, להטיל על ארגונים חובה למנות ממונה על הגנת הפרטיות, לפי החוק.²⁹

37. חובה זו עשויה לחול על ארגונים שכחלק מביצוע עיסוקם העיקרי משתמשים באמצעים לאימות גיל הכרוכים בעיבוד מידע בעל רגישות מיוחדת בהיקף ניכר.³⁰ גם ארגונים שכחלק מביצוע עיסוקיהם העיקריים פועלים לניטור שוטף ושיטתי של משתמשים בהיקף ניכר לשם אימות גילם, עשויים להיות מחויבים במינוי ממונה על הגנת הפרטיות.³¹

לדוגמה, רשת חברתית המעבדת באופן שיטתי מידע אישי רב הנגזר מפעילותם הרציפה של משתמשים בפלטפורמה, לשם אימות גילם.

²⁹ להרחבה על חובת מינוי ממונה על הגנת פרטיות ראו טיוטת גילוי הדעת של הרשות להגנת הפרטיות, לעיל ה"ש 22.

³⁰ בהתאם לחלופה של חובת המינוי הקבועה בסעיף 17(א)(4) לחוק הגנת הפרטיות.

³¹ בהתאם לחלופה של חובת המינוי הקבועה בסעיף 17(א)(3) לחוק הגנת הפרטיות.

אבטחת מידע והתקשרות עם גורמים חיצוניים המספקים שירותי אימות גיל

38. ארגון שבעלותו אתר אינטרנט, אפליקציה, או כל שירות מקוון אחר, המשתמש באמצעים לאימות גיל משתמשים, מהווה בעל השליטה במאגר המידע בו מאוחסן המידע, וככזה חלות עליו כל חובות אבטחת המידע המוטלות על בעל שליטה מכח הוראות חוק הגנת הפרטיות ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'תקנות אבטחת מידע').³²

39. שימוש באמצעים לאימות גיל הכרוכים בעיבוד והחזקה של מידע אישי עשוי להשפיע על רמת האבטחה בה נדרש ארגון לעמוד בהתאם להוראות תקנות אבטחת מידע. לאור האמור, על ארגונים המשתמשים באמצעים לאימות גיל לבחון באופן ספציפי את רמת האבטחה הנדרשת, על פי התקנות, למאגרים בהם מוחזק מידע שנצבר במסגרת שימושם באמצעים אלו.

40. על ארגונים המתקשרים עם גורמים חיצוניים לשם הספקת שירותי אימות גיל לפעול בהתאם להוראות תקנה 15 לתקנות אבטחת מידע, המחייבת, בין היתר, את ביצוע הפעולות הבאות:

- לבחון, בטרם ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות עם הגורם החיצוני;
- לקבוע מפורשות בהסכם את המידע שהגורם החיצוני רשאי לעבד לשם אימות גיל, וכי עיבוד המידע יכול להיעשות רק למטרה זו;
- לקבוע בהסכם את סוגי העיבוד והפעולות שהגורם החיצוני רשאי לנקוט לצורך ביצוע הליך אימות הגיל, ובכלל זה המתודה שבה הוא מתבקש לפעול למטרה זו;
- לקבוע בהסכם את משך ההתקשרות, ובכלל זה גם את החובה למחיקת המידע בו נעשה שימוש לשם ביצוע הליך אימות הגיל, והדיווח על מחיקתו.
- להתייחס בהסכם לאופן יישום החובות בתחום אבטחת המידע שהגורם החיצוני חייב בהן בהתאם לתקנות אבטחת מידע;
- לנקוט אמצעי פיקוח ובקרה על הגורם החיצוני – בהיקף ההולם את הסיכונים הספציפיים הנובעים מההתקשרות עמו.

לשימוש של ארגונים בספקים חיצוניים למטרת ביצוע הליכי אימות גיל עשויות להיות משמעותיות משפטיות, עסקיות וטכנולוגיות. לאור כך יובהר כי קיימת חשיבות עצומה בעמידה בהוראות תקנה 15 לתקנות אבטחת מידע, ובהנחיות הרשות בנושא.³³

41. כמו כן, ארגונים המפתחים מוצרי תוכנה לאימות גיל תוך הטמעת קוד פתוח במוצריהם (באופן מלא או חלקי), ארגונים המשתמשים במוצר תוכנה של גורם חיצוני אשר מוטמע בו קוד פתוח,

³² יצוין כי "אבטחת מידע" מוגדרת בסעיף 3 לחוק הגנת הפרטיות כ"הגנה על שלמות המידע האישי או הגנה על המידע האישי מפני עיבוד, ללא רשות כדין".

³³ להרחבה ראו מדריך הרשות להגנת הפרטיות בנושא "פעולה להתקשרות עם ספקי מיקור חוץ - תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע)" (ספטמבר 2023).



וכן ארגונים המתקשרים עם גורם חיצוני לקבלת שירותי אימות גיל על בסיס מוצר תוכנה בו מוטמע קוד פתוח, להקפיד על יישום עקרונות לניהול סיכוני אבטחת מידע המתקיימים כתוצאה משימוש זה.³⁴

³⁴ להרחבה ראו הרשות להגנת הפרטיות "עקרונות לניהול סיכוני אבטחת מידע בעת שימוש בקוד פתוח במערכות המאגר" (אפריל, 2024).