

18 ביולי 2022
י"ט בתמוז, התשפ"ב

חובת יידוע במסגרת איסוף ושימוש במידע אישי

נוסח מעודכן בעקבות תיקון 13

א. פתח דבר

להלן תוצג עמדת הרשות להגנת הפרטיות (להלן: 'הרשות') בנושא חובת היידוע באיסוף ושימוש במידע אישי. המסמך מציג את פרשנות הרשות בנושא ברמה הכללית, ותוך התייחסות לחובת יידוע במסגרת הליך קבלת הסכמה, וליידוע במסגרת שימוש במערכות לקבלת החלטות מבוססות אלגוריתם או בינה מלאכותית.

ב. חובת יידוע - כללי

1. הזכות לפרטיות היא זכות חוקתית נגזרת של כבוד האדם, כמו גם זכות אזרחית המבטאת, בין היתר, את החירות הבסיסית של האדם "להיעזב במנוחה", ואת זכותו לשלוט במידע אישי על אודותיו.¹
2. ככלל, הדין הישראלי מתיר איסוף, שימוש ועיבוד במידע אישי על אודות אדם בשני מצבים: האחד, מכוח הסכמת האדם נושא המידע, והשני, כאשר האיסוף והשימוש נעשים מכוח הסכמה שבדין.² כפי שיפורט בהמשך, בשני המצבים הדין מחייב את הגורם המבקש לאסוף ולהשתמש במידע (להלן: 'הגורם המבקש') ליידע את נושא המידע על כך, ולפרט בפניו נתונים הנוגעים לאיסוף ולשימוש במידע על אודותיו.³
3. חובת היידוע נובעת, בראש ובראשונה, מכוח הוראות **סעיף 11 לחוק הגנת הפרטיות**, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות' או 'החוק'). סעיף זה קובע כי פניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע **תלווה בהודעה שיצוינו בה המטרה אשר לשמה מבוקש המידע; האם חלה על נושא המידע חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו ובהסכמתו, ומהי תוצאת אי-ההסכמה למסירת המידע; למי יימסר המידע ומטרות המסירה; שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עימו; קיומן של זכות עיון במידע האישי לפי סעיף 13 לחוק,**⁴ ובדבר הזכות לבקש את תיקון המידע לפי סעיף 14 לחוק. על פרטים אלו להיות מדויקים. לפי סעיף 23 לחוק, מסירת פרטים לא נכונים בעת פנייה לאדם

¹ בג"ץ 6732/20 האגודה לזכויות האזרח בישראל נ' הכנסת (פורסם בנבו, 1.3.21), בפס' 10 ו-13 לפסק דינה של השופטת ברק-ארז.
² יצוין כי ישנה לכאורה גם אפשרות של איסוף מידע ממקורות גלויים וזאת ללא צורך בפנייה לנושא המידע ולקבלת הסכמתו המפורשת. סוגיה זו חורגת מתחולת מסמך זה.
³ יובהר כי חובת היידוע חלה ביחס לכל האופנים בהם יכולה להיערך הפנייה לנושא המידע, לרבות פנייה בעל-פה, באופן טלפוני או באמצעות הרשת.
⁴ להרחבה בעניין מימוש זכות העיון ראו הנחיית הרשות להגנת הפרטיות בנושא "[זכות העיון בהקלטות קול, וידאו ומידע דיגיטלי נוסף](#)" (ינואר 2017).

לקבלת מידע אישי לשם עיבודו במאגר מידע, בכוונה להטעותו באשר למסירת המידע האישי, מהווה עבירה פלילית.

4. לגישת הרשות, הוראות סעיף 11 חלות בכל מקום בו איסוף מידע אישי על אודות אדם נעשה על יסוד פנייה אליו לקבלת המידע, וזאת בין אם המידע נאסף מכוח הסכמת נושא המידע, ובין אם איסוף המידע נעשה מכוח הסמכה שבדין. כך עולה במפורש מלשון סעיף 11(1) לחוק, לפיו בעת פנייה לקבלת מידע על הפונה לציין אם חלה על נושא המידע חובה חוקית למסור את המידע. לפיכך, הסעיף מכיר במפורש באפשרות שפנייה ליידוע על איסוף מידע תיעשה במצב בו קיימת חובה חוקית למסירת המידע, קרי מכוח הסמכה שבדין.

5. עמדת הרשות היא כי החובות הקבועות בסעיף 11 לחוק חלות גם כאשר הפנייה לאדם לקבלת מידע נעשתה בעקבות בקשתו של אותו אדם לקבלת שירות מסוים. כמו כן, יובהר כי חובת היידוע חלה רק בעת פנייה לנושא המידע לשם לאיסוף מידע על אודותיו, ולא בעת השימוש במידע או בעת העברתו. במובן זה, לגישת הרשות, סעיף 11 אינו חל על צדדים שלישיים שמידע אישי מועבר אליהם מתוקף הסכמת נושא המידע, ולא בעת העברת מידע בין גופים ציבוריים מתוקף הוראות פרק ד' לחוק הגנת הפרטיות.

6. חובת היידוע נובעת גם מהמאפיינים הייחודיים של הזכות לפרטיות. הזכות לפרטיות היא זכות שקשה להגדיר את מהותה וגבולותיה.⁵ כמו כן, בניגוד לזכויות חוקתיות אחרות – כגון זכות הקניין, חופש הביטוי או חופש התנועה – במקרים רבים הפגיעה בפרטיות והנזק הנגרם לאדם כתוצאה ממנה אינם מוחשיים, ולא ניתנים לזיהוי או לכימות אלא רק לאחר פרק זמן שבו השלכות הפגיעה באות לידי ביטוי.⁶

מאפיינים אלו מחדדים את החשיבות בעמידה בחובת היידוע וכן את הצורך בשקיפות אופן האיסוף והשימוש במידע לאורך זמן. ללא יידוע ושקיפות שכזו, לא יכול הפרט (והציבור בכללותו) לפקח ולבקר את תהליכי האיסוף והשימוש במידע הנוגע אליו. תהליכי פיקוח ובקרה לאורך זמן הם קריטיים בהקשרים של איסוף ושימוש במידע אישי, ואינם יכולים להתרחש ללא שקיפות ויידוע מספקים.

ג. חובת יידוע כחלק מהליך קבלת הסכמה

7. על-פי נוסחו של סעיף 11, הליך היידוע עשוי להיות מיושם בנפרד מהליך הפנייה לקבלת הסכמה לאיסוף מידע. במצב זה על אוסף המידע לפרט בפני נושא המידע את כלל הנתונים הנדרשים בהתאם להוראות הסעיף.

⁵ מיכאל בירנהק "מעגלים של פרטיות" זכויות הקהילה הגאה בישראל: משפט, נטייה מינית וזהות מגדרית 195, 198 (עינב מורגנשטיין, יניב לוינסקי ואלון הראל עורכים, 2016).

⁶ דניאל סולוב (Solove) ציין בעניין זה את הדמיון בין פגיעה בפרטיות לבין פגיעה בבריאות כתוצאה מזיהום ומזקק סביבתי. ראו: Daniel J. Solove, A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 487 (2006).

8. כמו כן, במקרים רבים הליך היידוע משולב דה-פקטו בהליך קבלת ההסכמה לאיסוף מידע, ומהווה מעין שלב מקדים לשלב קבלת ההסכמה. לגישת הרשות, במצב שכזה היקפה של חובת היידוע עשוי להיות מושפע מהדרישות הנדרשות לשם קבלת ההסכמה.

9. סעיף 3 לחוק הגנת הפרטיות קובע, בעקבות תיקון שנערך לחוק בשנת 2007, כי הסכמה לאיסוף ולשימוש במידע צריכה להיות "הסכמה מדעת" (informed consent).⁷ הדרישה להסכמה מדעת מחייבת את מבקש המידע להציג לאדם נתונים בנוגע לאיסוף המידע עליו והשימוש בו, כך שבפני נושא המידע תעמוד תמונה מלאה בטרם יחליט האם להסכים למסירת המידע אודותיו.⁸

10. היקף היידוע ותוכנו עשויים להיות מושפעים בהקשר זה מנתונים שונים, כגון זהות מבקש הבקשה, אופי מערכת היחסים שלו עם נושא המידע, וכן סוג ורגישות המידע.

11. דוגמה לכך ניתן לראות בפסיקת בית הדין הארצי לעבודה בעניין קלנסווה, אשר עסק בבקשת רשות מקומית לאיסוף מידע ביומטרי של עובדיה. במקרה זה קבע בית הדין הארצי כי הרשות המקומית לא סיפקה לעובדים מידע מספק בדבר איסוף המידע הביומטרי ואופן השימוש בו, ומכאן שבמקרה זה לא התקיים יסוד ההסכמה מדעת:

"קודם לבקשת הסכמתן של עובדות החינוך היה על העירייה להציג להן מידע מקיף ומפורט, ובכלל זה (ולא כרשימה ממצה): הסבר מפורט מה 'ניטל' מהן; מי הם ה'טכנאים' שייטלו מהן את טביעות האצבע ומה הכשרתם; האם טביעות האצבע נשמרות ב'מאגר'; מי אחראי על המאגר ולמי יש גישה אליו ואל המידע האצור בו; האם המידע שנשמר, נשמר בצמידות לפרטי זיהוי אישיים אחרים; מהן דרכי האבטחה של אותו מידע; מהן הסכנות האפשריות; האם לגורמים חיצוניים יש אפשרות להתחבר ל'מערכת' מבחון או שמא מדובר במערכת 'מבודדת'; האם ניתן להעתיק את טביעת האצבע מיחידות הקצה (הסורקים) – בין בצורה דיגיטאלית ובין בצורה אחרת; מי בודק ומתי האם מידע זה נשמר או שמא נעשה ניסיון שלא כדין לגשת אליו; כיצד ומתי מוחקים מידע מאותו מאגר; מי הממונה בעירייה על כל אלה ומי אמון על מתן תשובות לשאלות, תהיות וכיוצא ב'ב' בקשות לקבלת מידע".⁹

⁷ סעיף 3 לחוק הגנת הפרטיות מגדיר הסכמה כ"הסכמה מדעת, במפורש או מכללא". מכללא – באופן שאינו מפורש אך משתמע מתוך התנהגות וכדומה. ראו חוק הגנת הפרטיות (תיקון מס' 9), התשס"ז-2007.

⁸ בת"א (ירושלים) 3213-09 פלונית נ' פלוני (פורסם בנבו, 11.10.11), שעסק בפגיעה בפרטיות במסגרת פרסום ספר, קבע ביהמ"ש המחוזי בירושלים כי: "הסכמתו של אדם לפגיעה בפרטיותו יכולה להיות מפורשת או מכללא, אולם הסכמה זו צריכה להיות 'הסכמה מדעת' (ס' 3 לחוק). 'הסכמה מדעת' הוא מונח השאוב מתחום דיני הרשלנות הרפואית, ומשמעותו היא כי 'בידי האדם שנתונה לו זכות לפרטיות (מושא המידע) היה המידע הדרוש לו באורח סביר כדי להחליט אם להסכים למסירת המידע ולשימושים שיעשו בו, ובכלל זה להעברתו לצדדים שלישיים' (מ' בירנהק, שם, בע' 100). לפיכך, על מנת שהסכמה תהא מדעת, יש צורך ב'ידיעה, בהבנה ובהסכמה' (שם). נטל הוכחת ההסכמה הוא על הנתבע" (פס' 58 לפסק דינה של השופטת כנפי-שטייניץ). כמו כן, לפי פרופ' בירנהק, "את הביטוי 'הסכמה מדעת' יש לקרוא ולפרש על רקע הבנת הפרטיות כשליטה. מימוש שליטתו של אדם ביחידה האוטונומית שלו אפשרי רק כאשר האדם יודע ומבין את משמעות הפעולה המבוקשת". ראו מיכאל בירנהק מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה 100 (התשע"א).

⁹ עס"ק (ארצי) 7541-04-14 הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי - עיריית קלנסווה (פורסם בנבו, 15.3.17), (להלן: 'עניין קלנסווה'), פס' 144 לפסק דינו של השופט איתח.

12. על היותה של חובת היידוע חלק מעיקרון ההסכמה מדעת ניתן ללמוד גם מעמדתו של היועץ המשפטי לממשלה שהוגשה לבית הדין הארצי בהליך בעניין קלנסווה, ולפיה: "על המעסיק חלה חובת יידוע כלפי העובדים בדבר מאפייניה של המערכת, משמעות התקנתה במקום העבודה, הסיכונים הכרוכים בה, טיב שיטת אבטחת המידע הננקטת והאפשרות להפסיק את השימוש במערכת. יתר על כן, על היידוע להיות מפורש וספציפי, שכן ללא מידע ספציפי וברור בנוגע לפגיעה שעלולה להיגרם לפרטיותו ואף ביחס לחוסר הוודאות בה היא מתאפיינת, לא ניתן לייחס להסכמת העובד את יסוד ה'דעת' ... טיבה ואיכותה של ההסכמה מבוססים, אם כן, על קיומו של יידוע ברור בהיקפו ... **ההסכמה מדעת כוללת שני ראשים: האחד נוגע לחובת היידוע עליה עמדנו לעיל, והשני נוגע לעמידה במבחני המידתיות**..." (ההדגשה אינה במקור).¹⁰

ד. יידוע בדבר תוצאת אי-קבלת ההסכמה

13. על-פי נוסחו של סעיף 11, על אוסף המידע לפרט בפני נושא המידע את כלל הנתונים הנדרשים בהתאם להוראות הסעיף, **לרבות תוצאת אי-קבלת ההסכמות**.

14. ידוע בדבר תוצאת אי-קבלת ההסכמה משמעותו שעל מבקש המידע לציין בפני נושא המידע, בטרם קבלת ההסכמה, מה תהיה המשמעות של אי-קבלת ההסכמות לאיסוף ועיבוד המידע. **תוצאה שכזו יכולה להיות, בין השאר, העדר אפשרות לחתום על הסכם, מניעת אפשרות השימוש בשירותים מסוימים (לדוגמה, במצבים בהם איסוף המידע מתחייב לשם עצם מתן השירותים), סיום התקשרות בין צדדים, או הגבלת אופן היישום של שירות מסוים (כגון הגבלת האפשרות לקבלת שירות באופן מקוון)**. בתוך כך, על מבקש המידע לציין את החלופות העומדות בפני נושא המידע אם לא יסכים למסירת המידע, והכל בהתאם לנסיבות העניין וזהות הצדדים.

לדוגמה, על רשות מקומית המבקשת לספק לתושביה שירותים ציבוריים באופן מקוון (כגון רישום למסדות חינוך), ולצורך כך מבקשת לאסוף מידע אישי הנוגע אליהם, ליידע את התושבים כי סירוב למסירת המידע עלול למנוע מהם את האפשרות לקבלת השירותים באופן מקוון, ובד בבד לציין כי שירותים אלו יעמדו לתושבים באופן פיזי במשרדי הרשות.

15. במקרים בהם בקשה לאיסוף מידע עלולה להשפיע על זכויות נושא המידע או להיתפס ככזו, **יידוע בדבר תוצאת אי-קבלת ההסכמה צריך לכלול התייחסות גם להשלכות הסירוב למסירת המידע על זכויות נושא המידע**.

כך לדוגמה, על קופת חולים המבקשת לאסוף מידע אישי לצרכי מחקר רפואי וולונטרי להבהיר למטופליה כי סירובם למסירת המידע לא יביא לפגיעה בזכויותיהם, לרבות זכותם לקבלת טיפול רפואי מטעם קופת החולים.

¹⁰ פסי' 65-66, ו-78 לעמדת היועץ המשפטי לממשלה בעניין קלנסווה.

ה. חובת יידוע במערכות לאיסוף מידע וקבלת החלטות מבוססות אלגוריתם או בינה מלאכותית

16. העידן הדיגיטלי מאופיין באיסוף מידע אישי רב ובשימוש במידע זה למטרות שונות. בצד יתרונותיו, העידן הדיגיטלי מאתגר את יכולתו של הפרט לשמור על פרטיותו, ולשלוט על אופן השימוש במידע הנוגע אליו.

17. עיבוד מידע במערכות טכנולוגיות נעשה כיום על בסיס שימוש באלגוריתמים – רכיבים המתוכננים לנתח מידע המוזן אליהם (קלט) על יסוד קריטריונים מוגדרים מראש (rule-based), ולמטרות מוגדרות (פלט).¹¹

18. ברם, עיבוד זה נעשה, במקרים רבים, באופן שאינו שקוף דיו, כלומר ללא פירוט והסבר בדבר אופן פעולת האלגוריתם, הקריטריונים שהוגדרו לו, והמידע המוזן אליו. מצב זה הוא בעייתי במיוחד במערכות טכנולוגיות המשתמשות לקבלת החלטות על אודות אדם.

19. כך לדוגמה, חברת ביטוח המשתמשת באלגוריתם לחישוב גובה פרמיות שעל מבוטחים לשלם עלולה לקבוע בהגדרות האלגוריתם כי מבוטחים ממוצא אתני כלשהו, המתגוררים באזור מסוים, יידרשו לשלם פרמיות גבוהות יותר מאשר מבוטחים אחרים. ללא יידוע מספק יידרשו המבוטחים לשאת בתשלומים האמורים וזאת מבלי שהם יודעים איזה שימוש נעשה במידע על אודותיהם, ועל יסוד אילו שיקולים או נתונים התקבלה ההחלטה.

20. **איסוף ועיבוד מידע אישי על-ידי מערכות לקבלת החלטות מבוססות אלגוריתמים, הנעשים ללא יידוע מספק, ומבלי שנושא המידע יכול להבין מה נעשה עם המידע הנוגע אליו ולאילו מטרה, מהווים פגיעה ביכולתו לשלוט במידע האמור. על יסוד הגישה הרואה בשליטה במידע מאפיין מרכזי של הזכות לפרטיות, שימוש זה במידע אישי עלול להוות פגיעה בפרטיות.**

21. מעבר לכך, בשנים האחרונות גובר השימוש במערכות בינה מלאכותית (AI) לקבלת החלטות אוטומטיות (להלן: 'מערכות אוטומטיות'). מערכות אלו נועדו לעבד מידע ממגוון רב של מקורות (לרבות מאגרי מידע), וזאת באופן "עצמאי", משתנה, ושלא על-פי קריטריונים מוגדרים מראש. לאלגוריתמים במערכות אלו היכולת לשנות את הקריטריונים והנסיבות שעל בסיסם הם מקבלים החלטות, וזאת בין היתר, על סמך החלטות קודמות או מידע סטטיסטי. אופן פעולתן של המערכות האמורות הוא מורכב ומשתנה, ומשכך עשוי להיות לא שקוף לציבור, לנושאי המידע, ולעיתים אף לגורמים המתכננים את המערכות האמורות. אלגוריתמים מסוג זה הוגדרו לא פעם כ'קופסה שחורה'.¹²

¹¹ הכוונה כאן היא לאלגוריתמים המבטיחים שקלט מוגדר יוביל לפלט מוגדר. להבחנה בין סוגי האלגוריתמים השונים ראו סיון תמיר "בינה מלאכותית בשירותי ממשל: הטמעת מערכות לקבלת החלטות מבוססות אלגוריתם בשירותי הרווחה", המכון הישראלי למדיניות טכנולוגיה 9 (2020).

¹² המושג 'קופסה שחורה' מתייחס למנגנון אשר הקלט והפלט שלו ידועים, אולם דרך פעולתו לא ידועה. ראו: נתי פרל "החלטה על קיומו של 'חשד סביר' בעולם ה-Big-Data: מהנמקה אנושית לאלגוריתם לחיזוי פשיעה" **דין ודברים** יד 237, 253 (2019). פרל ז"ל ניתח במאמרו את השימוש באלגוריתמים לומדים לחיזוי פשיעה, אשר מבססים את תחזיותיהם על ניתוח ועיבוד של מאגרי מידע וזאת לצורך זיהוי והרתעה על עברייני פוטנציאלי החשוד כי בכוונתו לבצע עבירה ספציפית.

22. מצב עניינים זה עלול להביא לכך שנושא מידע - שהחלטה לגביו מתקבלת על-ידי מערכות שכאלו - יתקשה מאד להבין איזה מידע נאסף עליו על-ידי המערכות, איזה שימוש נעשה בו, איזה מידע עובד ביחד עם המידע על אודותיו, ולאילו מטרות. מצב שכזה מקשה על אדם לשלוט על אופן השימוש במידע על אודותיו. העדר השקיפות עלול לפגוע גם ביכולת הבקרה והפיקוח על פעילות המערכות וההחלטות המתקבלות במסגרתן.¹³

23. במקרים מסוימים איסוף המידע עצמו נעשה על-ידי מערכות אוטומטיות מבוססות בינה מלאכותית. מערכות שכאלו, כדוגמת "בוטים", פונות לאדם ומבקשות ממנו לשתף ולמסור מידע על אודותיו וזאת, לעיתים, מבלי ליידע אותו על מטרות איסוף המידע ולמי המידע יימסר.

24. אתגרים אלו מחדדים את הערך שבשיקוף מידע בדבר המערכות ואופן פעולתן, ואת חשיבות ההסבר בדבר תהליך קבלת ההחלטות שלהן - קרי מדוע המערכת פעלה והחליטה כפי שהחליטה בנושא מסוים (עניין זה מוגדר כמובנות או הסברתיות של החלטות).¹⁴

25. לאור כל האמור הרשות מבקשת להדגיש כי הוראות סעיף 11 לחוק הגנת הפרטיות מטילות חובת יידוע **בשלב איסוף המידע** גם על גורמים האוספים מידע אישי באמצעות מערכות לקבלת החלטות מבוססות אלגוריתם (לרבות מערכות מבוססות בינה מלאכותית (AI)) וגם על גורמים האוספים מידע אישי לשם שימוש בו במסגרת מערכות שכאלו. כלומר, **על גורמים האוספים מידע אישי מאדם על-ידי המערכות הללו או לשם עיבודו במסגרת מערכות שכאלו, מוטלת החובה ליידע את נושא המידע ולספק לו מידע על אודות מטרות השימוש ולמי יימסר המידע, והכל בהתאם למפורט בחלקים ב' ו-ג' למסמך זה.**¹⁵

26. להרחבה נוספת בעניין חובת היידוע ביחס לשימוש במידע אישי במערכות בינה מלאכותית, ראו טיוטת הנחיית הרשות להגנת הפרטיות "תחולת הוראות חוק הגנת הפרטיות על מערכות בינה מלאכותית" (אפריל 2025), שפורסמה להערות הציבור.¹⁶

ו. חובת יידוע – הנחיות והמלצות הרשות להגנת הפרטיות

27. לאור כל האמור במסמך זה, הרשות להגנת הפרטיות מבקשת להדגיש כי :

א. חובת היידוע הקבועה בהוראות סעיף 11 לחוק הגנת הפרטיות חלה בכל מקום בו איסוף מידע אישי על אודות אדם נעשה על יסוד פנייה אליו, וזאת בין אם המידע נאסף מכוח הסכמת נושא המידע, ובין אם איסוף המידע נעשה מכוח הסמכה שבדין. חובה זו חלה גם

¹³ לאורך השנים התגלו מקרים רבים בהם מערכות אוטומטיות קיבלו החלטות שגויות ומפלות. במקרה מפורסם נמצא כי מערכת אוטומטית לקביעת זכאות לדמי אבטלה שהופעלה במדינת מישיגן קבעה בטעות ש- 34 אלף איש הונו את המערכת (unemployment fraud). רק לאחר שנתיים נמצא כי הניתוח היה שגוי. [Robert N. Charette, Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold, IEEE SPECTRUM \(Jan, 24, 2018\)](#). להרחבה בנושא ראו גם: מעיין פרל "פרטיות, שליטה ופיקוח בעידן של נתוני עתק: חובת הנמקה על החלטות אלגוריתמיות" **משפט, חברה ותרבות** ב' 167 (2019).

¹⁴ להרחבה בנושא זה ראו "המיזם הלאומי למערכות נבונות בטוחות להעצמת הביטחון הלאומי והחוסן המדעי-טכנולוגי: אסטרטגיה לאומית לישראל - דו"ח מיוחד לראש הממשלה, חלק ב", פרק 8, בעמ' 172-208.

¹⁵ להנחיות והמלצות בנושא יישום חובת יידוע במערכות אוטומטיות ראו סעיף 23 למסמך זה.

¹⁶ סעיף 6 לטיוטת ההנחיה, זמינה [כאן](#).

כאשר הפנייה לאדם לקבלת מידע נעשתה בעקבות בקשתו של אותו אדם לקבלת שירות מסוים.

ב. על-פי הוראות סעיף 11, גורם המבקש לאסוף מידע אישי מאדם צריך לפרט, בעת הפניה לאותו אדם, איזה מידע יאסף עליו, למי המידע עשוי להיות מועבר, לשם איזו מטרה, ומהי תוצאת אי הסכמתו למסירת המידע. בנוסף, על הגורם המבקש לאסוף את המידע לציין את שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עימו, וליידע על קיומן של זכות עיון במידע האישי לפי סעיף 13 לחוק, ובדבר הזכות לבקש את תיקון המידע לפי סעיף 14 לחוק.

ג. לפי סעיף 23 לחוק, מסירת פרטים לא נכונים בעת פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע, בכוונה להטעותו באשר למסירת המידע האישי, מהווה עבירה פלילית, שהעונש המירבי בצדה הוא 3 שנות מאסר.

ד. ככלל, איסוף מידע מאדם ושימוש בו ללא יידוע מספק של נושא המידע, משליך על תוקף ההסכמה מדעת, ועשוי להוות הפרה של הוראות חוק הגנת הפרטיות.¹⁷

במצבים בהם חובת היידוע מיושמת כחלק מהליך קבלת ההסכמה מדעת, היקפה של חובת היידוע עשוי להיות מושפע מהדרישות לשם קבלת ההסכמה. כך, נתונים שונים כגון זהות מבקש הבקשה, אופי מערכת היחסים שלו עם נושא המידע ומידת יכולתו של נושא המידע להתנגד לבקשה, וכן סוג ורגישות המידע, עשויים להביא להרחבה של חובת היידוע הנדרשת.

ה. על-פי נוסחו של סעיף 11, על אוסף המידע לפרט בפני נושא המידע את כלל הנתונים הנדרשים בהתאם להוראות הסעיף, לרבות תוצאת אי-קבלת הסכמתו. תוצאת אי-ההסכמה למסירת מידע אישי יכולה להיות, בין היתר, הגבלת או מניעת שירות מסוים שלמטרתו מתבקשת מסירת המידע האישי, העדר אפשרות לחתום על הסכם או סיום ההתקשרות בין הצדדים. כמו כן, על אוסף המידע לציין את האפשרויות והחלופות העומדות בפני נושא המידע אם לא יסכים למסירת המידע, והכל בהתאם לנסיבות העניין וזהות הצדדים. במקרים בהם בקשה לאיסוף מידע עלולה להשפיע על זכויות נושא המידע או להיתפס ככזו, היידוע צריך לכלול גם התייחסות להשלכות אי-קבלת ההסכמה על זכויות נושא המידע.

¹⁷ בת"פ (ת"א) 6955-98 מדינת ישראל נ' שחם שמואל (פורסם בנבו, 10.12.01) הרשיע בית משפט השלום בת"א חברה להשכרת טלפונים וטלוויזיות לחולים המאושפזים בבתי חולים ואת מנהלה (ובעל המניות בה) בהפרת סעיפים שונים בחוק הגנת הפרטיות, לרבות הוראות סעיף 11 לחוק. במקרה זה, חולים שאושפזו בבית חולים וביקשו לשכור מהחברה הנאשמת טלוויזיה או טלפון, נדרשו למסור את פרטיהם האישיים, ולאחר מכן אף נתבקשו לחתום על 'טופסי ויתור', בהם צוין כי הם מתירים מסירתם פרטיהם, לכאורה לשם קבלת הצעות בתחום הבריאות. בית המשפט קבע כי הנאשמים מכרו את שמותיהם של חולים לגורמים שונים מבלי שאלו הביעו את הסכמתם לכך, וכי במרבית המקרים הם כלל לא יידעו את החולים באשר לשימוש שיעשה בשמותיהם. בעניין טופסי הויתור ציין בית המשפט כי הם אינם עומדים בהוראות סעיף 11 לחוק הגנת הפרטיות. בהקשר של דיני הגנת מידע באירופה, בחודש ספטמבר 2021 הודיעה נציבות הגנת המידע האירית (Data Protection Commission, DPC) על הטלת קנס בסך 225 מיליון אירו על חברת וואטסאפ בגין הפרה של חובת השקיפות הקבועה בתקנות הגנת המידע האירופיות (GDPR) בהקשרים של אופן עיבוד המידע והעברתו לחברות אחרות השייכות לחברות פייסבוק.

ו. היידוע צריך להיות בשפה ברורה, פשוטה ונגישה,¹⁸ להינתן בד בבד עם הפניה לאדם, ומומלץ כי יכלול פירוט בדבר אופן שמירת המידע (כגון זהות מורשי הגישה למידע). ככל שהשירות מופנה לציבור מובחן מבחינה מסוימת (כגון גיל, ארץ מוצא או מוגבלות), חשוב ששפת היידוע תהיה מותאמת, ככל האפשר, והדבר יכול להשליך גם על תוקף ההסכמה מדעת.¹⁹ עם זאת יובהר כמובן שבמצב בו קיימים הסדרים חוקיים או רגולטוריים סותרים בנוגע לאופן יישום חובת היידוע בנסיבות ספציפיות או ביחס לגורמים ספציפיים (כגון בנקים וכו'), הסדרים אלו עשויים לגבור, ואפשר שיהיה על הגורמים הרלוונטיים לפעול לפיהם.

ז. ככל שהמידע הנאסף הוא "מידע בעל רגישות מיוחדת" כהגדרתו בסעיף 3 לחוק הגנת הפרטיות (כגון מידע אישי שהוא מזהה ביומטרי המשמש או המיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב), ובנסיבות בהן קיים חשש אינהרנטי כי הסכמת נושא המידע עלולה להיות מוגבלת, רצוי לכלול במסגרת היידוע פרטים נוספים הנוגעים לאיסוף המידע, ולאופן ומטרות השימוש בו.

ח. כאשר בעל שליטה במאגר מידע מתקשר עם גורם חיצוני לצורך קבלת שירות במסגרת 'מיקור חוץ' בהתאם להוראות תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'תקנות אבטחת מידע'), והגורם החיצוני מבקש להשתמש במידע האישי שנאסף על-ידו במסגרת מתן השירות למטרות השונות ממטרת השירות המקורי, על הגורם החיצוני ליידע את נושא המידע על כך, ולבקש את הסכמתו.²⁰

28. בהקשר של מערכות אוטומטיות (AI), הרשות מציינת כי:

א. כאשר איסוף המידע נעשה באמצעות מערכות אוטומטיות (כגון "בוטים") יש לוודא כי במסגרת זו יוצגו לנושא המידע כל הפרטים הנדרשים בהתאם להוראות סעיף 11 לחוק.

ב. כאשר עיבוד המידע נערך באמצעות מערכות אוטומטיות - על הליך היידוע לפרט על אופן פעולת המערכות האמורות, **ככל שהדבר רלוונטי לגיבוש ההסכמה** וככל שפירוט זה אפשרי מבחינה משפטית, טכנולוגית, ומסחרית.

ג. מומלץ כי יוסבר לנושא המידע על אודות פרטי המידע בהם עשויות המערכות להשתמש במסגרת השימוש במידע הנוגע אליו, והמקור של פרטי מידע אלו.

¹⁸ לעניין זה מומלץ לשקול שימוש בשפה גרפית (ציורים, סימנים) לפישוט ההסברים. פרופ' בירנהק ציין בעניין כי "ההסבר אינו צריך להיות ארוך, משפטי או מסורבל. להפך, הסברים מסורבלים מקשים את ההבנה, בוודאי בעסקות שגרתיות, פשוטות, נקודתיות וקצרות כמו רכישה בסופרמרקט. ההסבר צריך להיות כזה שאדם יוכל להחליט בעצמו אם למסור את המידע מבלי להשקיע עלויות בבדיקה". מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" משפט וממשל יא 9, 53 (תשס"ח).

¹⁹ כך לדוגמה, חברת משחקי רשת לילדים בגילאי העשרה, רצוי כי תפרט על מדיניות הפרטיות שלה ואופן השימוש שלה במידע אישי באופן ובשפה המותאמים גם לבני נוער.

²⁰ כך לדוגמה, בנסיבות בהן עירייה מתקשרת עם ספק חיצוני למתן שירות מסוג הפעלת אופניים חשמליים, ובמסגרת זו אוסף ספק השירות מידע על אודות תושבים לצרכים ולמטרות שאינן מיועדות למתן השירות (כגון לצרכי מחקר, פרסום, או ייעול שירותים אחרים הניתנים על-ידו), על הרשות המקומית החובה ליידע את התושבים על כך.



29. יובהר כי אין באמור במסמך זה בכדי לומר כי חובת היידוע מחייבת לחשוף את כלל הפרטים והנתונים הנוגעים לאיסוף ולשימוש במידע אישי. יתכנו מצבים בהם חשיפה שכזו תהיה בלתי אפשרית או מנוגדת לתכליות חוקיות או לאינטרסים לגיטימיים אחרים.²¹ **במצבים שכאלו על הגורם המבקש לאזן בין האינטרסים השונים.** עליו לבחון כיצד הוא מספק לנושא המידע את הנתונים המרכזיים הנוגעים לאיסוף המידע והשימוש בו (כגון נתונים שבלעדיהם אין לנושא המידע אפשרות להעניק הסכמה מדעת לאיסוף), תוך הימנעות מחשיפת נתונים אותם אין באפשרותו לחשוף.

30. יש לזכור כי היקף הפירוט במסגרת עמידה בחובת היידוע הוא תלוי הקשר. בנסיבות בהן איסוף המידע והשימוש בו כרוכים בפגיעה משמעותית בפרטיות, או כאשר ניתן להניח שנושא המידע עשוי שלא להיות מודע לעצם איסוף המידע או להשלכותיו, יש להקפיד כי היידוע יוצג באופן נקודתי אך מקיף ככל האפשר.

²¹ עיקרון זה מוסדר גם בהוראות סעיפים 8 ו-9 לחוק חופש המידע, התשנ"ח-1998, הקובעות מגבלות וסייגים שונים לחובת השקיפות החלה על רשויות וגופים ציבוריים. דוגמה לאינטרס לגיטימי לאי-חשיפת כלל המידע במסגרת חובת היידוע וקבלת ההסכמה עשויה להיות מצב בו חשיפה שכזו תביא לפגיעה קשה בסוד מסחרי מוגן של הגורם המבקש. גם אינטרסים של ביטחון המדינה, שלומו או ביטחונו של אדם, עשויים להיות כאלו המצדיקים אי-חשיפה של כלל המידע הנוגע לאיסוף ולשימוש במידע אישי.

