



25 בפברואר 2026
ח' באדר התשפ"ו

גילוי דעת בנושא הסכמה בדיני הגנת הפרטיות

הקדמה

1. עיקרון ההסכמה הוא עיקרון מרכזי בדיני הגנת הפרטיות הישראלים. מטרת גילוי הדעת היא להבהיר את עמדת הרשות להגנת הפרטיות (להלן: 'הרשות') בעניין יישום העיקרון בראי המציאות הדיגיטלית המתפתחת, וכן ביחס לתחולת חוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות' או 'החוק') בנושא. גילוי הדעת אינו עוסק במהותו בשאלה מתי ובאילו נסיבות חלה החובה לבקש את הסכמת נושא המידע לעיבוד מידע על אודותיו, אלא מציג את פרשנות הרשות ביחס לסוגיית אופן יישום החובה, קרי מה היא הסכמה תקפה על-פי דיני הגנת פרטיות, ומהם הכללים לאורם הסכמה שכזו צריכה להתקבל.
2. גילוי הדעת משקף את הפרשנות המשפטית שתשמש את הרשות בעת ולצורך הפעלת מגוון הסמכויות המסורות לה בחוק, לרבות הפיקוח על מילוי הוראות החוק והתקנות שמכוחו, יישום מאגר במרשם מאגרי המידע, והטלת עיצום כספי בגין הפרת הוראות החוק.¹

כללי

3. חוק הגנת הפרטיות קובע כי איסוף ושימוש במידע אישי (להלן גם: 'עיבוד') הכרוכים בפגיעה בפרטיות יכולים להיעשות מכוח הסכמה בדין או בהסכמת נושא המידע.²
4. עיקרון ההסכמה הוא עיקרון מרכזי בדיני הגנת הפרטיות. ככלל, על-פי עיקרון זה, עיבוד מידע מכוח הסכמתו של אדם יכול להיעשות רק בנסיבות בהן עומדת לו האפשרות להחליט איזה מידע הנוגע אליו ייחשף, למי, ולאילו מטרות.³
5. עיבוד מידע על אודות אדם ללא קבלת הסכמתו מהווה פגיעה באוטונומיה שלו וביכולתו לשלוט במידע הנוגע אליו.⁴ הסכמה משקפת אפוא את יכולת השליטה של אדם במידע שעל אודותיו.⁵

¹ פרשנות הרשות המוצגת בגילוי הדעת נסמכת על הוראות חוק הגנת הפרטיות, דברי ההסבר להוראות החוק, ופסיקת בתי המשפט ובתי הדין לעבודה. במקרים של סתירה בין פרשנות הרשות המוצגת בגילוי הדעת להוראות דין ספציפי החלות על גורמים שונים בנסיבות מסוימות, הוראות הדין הספציפי גוברות.

² יצוין כי סעיף 18 לחוק הגנת הפרטיות קובע כי במצבים מסוימים עשויה לעמוד הגנה משפטית לגורם הפוגע שלא כדין בפרטיותו של אדם. יובהר כי ההגנות הקבועות בסעיף 18 לחוק פורשו בפסיקה בצמצום רב והן כפופות גם לדרישות סטטוטוריות כגון חובת תום הלב ודרישת סבירות (ראו סעיף 20 לחוק). ראו לדוגמה רע"פ 4743/20 **מרדכי לייבל נ' מדינת ישראל** (נבו 21.7.2022). עוד יצוין כי בהתאם לפסיקת בית המשפט העליון, רשות מנהלית אינה רשאית להסתמך מראש על ההגנות שבסעיף 18 לחוק הגנת הפרטיות לצורך קביעת מדיניות כללית הכרוכה בפגיעה בפרטיות. לעניין זה ראו: רע"א 2558/16 **פלונית נ' קצין התגמולים – משרד הביטחון**, פסקה 59 לפסק הדין (נבו 5.11.2017).

³ תפיסה זו ידועה בשם "פרטיות כשליטה". להרחבה ראו מיכאל בירנהק **מרחב פרטי: הזכות לפרטיות בין משפט לטכנולוגיה**, 108-89 (2010).

⁴ לעניין זה ראו לדוגמה את דברי הנשיאה חיות בבג"ץ 2109/20 **שחר בן מאיר נ' ראש הממשלה** (נבו, 26.4.2020), שם ציינה הנשיאה, בפס' 38 לפסק דינה, כי: "הסכמת הפרט לאיסוף המידע מהווה 'בריח התיכון' של ההגנה על הזכות לפרטיות. זאת, משום שכאשר הרשות אוספת מידע אודות הפרט בלא שמתקבלת לכך הסכמתו, מופקעת למעשה יכולת האוטונומית לשלוט בורם המידע אודותיו".

⁵ מיכאל בירנהק **פרטיות חוקתית** (2023), בעמ' 252.



6. דרישת ההסכמה נכללת מפורשות בחוק הגנת הפרטיות. סעיף 1 לחוק קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". משמעות הוראה זו היא כי על הפוגע בפרטיותו של אדם, באחת הדרכים המנויות בסעיף 2 לחוק, מבלי שניתנה לכך הסמכה בדין, מוטל הנטל לשכנע באופן פוזיטיבי כי הפגיעה נעשתה בהסכמה.⁶

7. רכיב ההסכמה מצא מקומו גם בסעיף 11(1) לחוק, שם נקבע כי בעת פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע, על מבקש המידע להציג בפניו נתונים שונים ובכלל זה, האם חלה עליו חובה חוקית למסור את המידע או האם מסירת המידע תלויה ברצונו ובהסכמתו, ומהי תוצאת אי-ההסכמה.

8. רכיב ההסכמה בא לידי ביטוי גם בסעיף 8(ב) לחוק, הקובע כי לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין.⁷ בהיעדר הסמכה בדין, וכאשר המידע נאסף מכח הסכמת נושא המידע, שימוש במידע למטרה מסוימת יכול להיעשות רק על יסוד ההסכמה שניתנה למטרה זו.

9. בתיקון מס' 13 לחוק הגנת הפרטיות נחקק בין היתר סעיף 8(ד1), המבהיר כי חל איסור על עיבוד מידע אישי במאגר אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע". למען הסר ספק יובהר כי **הוראה זו תחול על מידע אישי שנאסף אגב פגיעה בפרטיות שלא מתוקף הסכמה תקפה לפי החוק, אלא אם קיימת הסמכה בדין לאיסופו.**

10. חוק הגנת הפרטיות מגדיר, בסעיף 3, כי על הסכמה לעיבוד מידע אישי הכרוך בפגיעה בפרטיות להיות "מדעת", בין אם מתקבלת "במפורש" או נלמדת "מכללא". להלן נפרט על רכיבים מרכזיים אלו של דרישת ההסכמה בדיני הגנת הפרטיות, תוך התייחסות לרכיב הרצון החופשי בהסכמה, לסוגיית הפגיעה בפרטיות בהיעדר הסכמה, ולמתן האפשרות לחזרה מהסכמה.

הסכמה מדעת

11. הסכמה מדעת (informed consent) נועדה להבטיח כי הסכמתו של אדם לפגיעה בפרטיותו ניתנה מתוך בחירה אמיתית ואוטונומית.⁸

⁶ דרישת ההסכמה חלה במצבים המוגדרים כפגיעה בפרטיות על-פי סעיף 2 לחוק הגנת הפרטיות. עם זאת, הרשימה המפורטת בסעיף 2 אינה בהכרח רשימה סגורה של מצבי פגיעה בפרטיות. לעניין זה ראו בג"ץ 6650/04 פלונית נ' בית הדין הרבני האזורי בנתניה (נבו, 14.5.2006) (להלן: "עניין פלונית נ' ביה"ד הרבני"), סעיף 8 לפסק הדין; עסיק (ארצ'ל) 7541-04-14 הסתדרות העובדים הכללית החדשה מרחב המשולש הדרומי נ' עיריית קלנסווה (נבו, 15.3.2017), (להלן: "עניין קלנסווה"), סעיף 98 לפסק הדין. עם זאת יצוין, כי בתי המשפט לא קבעו עד כה אילו מצבים נוספים מוגדרים כפגיעה בפרטיות, מעבר לאלו המנויים, בסעיף 2 לחוק.

⁷ סעיף זה מבטא את עיקרון צמידות המטרה.

⁸ רע"פ 10141/09 אברהם בן חיים נ' מדינת ישראל (נבו, 6.3.2012) (להלן: "עניין בן חיים"), בפס' 27 לפסק דינה של הנשיאה (בדימי) ד' ביניש. לפי בירנהק, את הביטוי "הסכמה מדעת" יש לקרוא ולפרש על רקע הבנה של הפרטיות כשליטה. לגישתו, מימוש שליטתו של אדם ביחידה האוטונומית שלו אפשרי רק כאשר הוא יודע ומבין את משמעות הפעולה המבוקשת. בירנהק, לעיל הי"ש 3, בעמ' 100.



12. מקורו של מושג זה הוא בהקשר הרפואי, ולפיו, על מטפל למסור למטופל את כל המידע הרפואי הנדרש לו, באורח סביר, לשם קבלת החלטה ביחס לטיפול רפואי אותו הוא מבקש או נדרש לעבור.⁹

13. בדיני הגנת הפרטיות, משמעות הדבר היא שבעת בקשה לקבלת הסכמה לפגיעה בפרטיות, אדם צריך להיות מודע לזכותו לסרב לבקשה (לרבות מודעות להשלכות החלטתו),¹⁰ לאחר שהובא בפניו כל המידע הדרוש לו, באורח סביר ובצורה מובנת, כדי לקבל החלטה בנושא.¹¹

14. בעניין קרן אביב, בו קיבל בית המשפט המחוזי (מרכז) בקשה לאישור תובענה כתובענה ייצוגית בגין שימוש בשמות ותמונות משתמשים לשם רווח ללא קבלת הסכמה מדעת, ציין בית המשפט כי: "... על מנת שתתקיים הסכמה מדעת, נדרש שבידי האדם שניתנת הסכמתו, יהיה המידע הדרוש לו, באורח סביר, כדי להחליט אם להסכים. כמו כן, נדרש כי המידע יימסר לו בצורה ברורה. עוד צוין מפורשות בדברי ההסבר כי דרישת ההסכמה מדעת היא בעלת חשיבות מיוחדת, וזאת במיוחד בעידן האינטרנט, כאשר הסכמי הוויתור על פרטיות לעיתים אינם גלויים כלל לעין האדם אשר פרטיותו נפגעת. הסכמה מדעת משמעותה ש'ההסכמה לפגיעה בפרטיותו של אדם צריכה להינתן רק לאחר שהאדם יודע ומבין את משמעות הפעולה המתבקשת, את הפגיעה הצפויה בעטייה ואת השלכותיה. הכוונה היא למתן הסכמה לא רק על בסיס ידיעה, אלא גם על בסיס הבנה עמוקה של המצב והשלכותיו".¹²

15. עיקרון ההסכמה, כמו גם חובת היידוע שבסעיף 11 לחוק הגנת הפרטיות, מחייבים את מבקש ההסכמה לספק ולהציג לאדם נתונים שונים על אודות איסוף המידע והשימוש בו, ובכלל זה פירוט בדבר מטרת איסוף המידע ובדבר זהות הגורמים אליו הוא עשוי להיות מועבר.¹³

16. תוקף ההסכמה והיקפה תלויים, במידה רבה, במידע שהועבר לאדם נושא המידע, ושעל-פיו הוא נתן את הסכמתו.

⁹ עיקרון זה קבוע בסעיף 13(ב) לחוק זכויות החולה, התשנ"ו-1986, הקובע כי "לשם קבלת הסכמה מדעת, ימסור המטפל למטופל מידע רפואי הדרוש לו, באורח סביר, כדי לאפשר לו להחליט אם להסכים לטיפול המוצע". להרחבה ראו ע"א 2781/93 דעקה נ' בית החולים "כרמל" חיפה, פ"ד נג' (4) 526 (1999).

¹⁰ עניין בן חיים, לעיל ה"ש 8, בפס' 27.

¹¹ השינוי בהגדרת "ההסכמה" בחוק הגנת הפרטיות, לפיו הסכמה לפגיעה בפרטיות צריכה להיות "מדעת", התקבל במסגרת חוק הגנת הפרטיות (תיקון מס' 9), התשס"ז-2007. בדברי ההסבר לתיקון צוין כי "התיקון המוצע נועד להבטיח כי ההסכמה הניתנת לפגיעה בפרטיות תהיה הסכמה מדעת. היינו, שבידי האדם המסכים לפגיעה בפרטיות יהיה מידע, הדרוש לו, באורח סביר, כדי להחליט האם להסכים או לא, והמידע יימסר לו בצורה מובנת" (ה"ח הממשלה 230, 232). פרשנות זו של המונח מצאה מקומה בפסיקת בתי המשפט. ראו לדוגמה: עמר"מ (מחוזי-מרכז) 13028-04-09 אליה נ' עיריית טבריה (נבו, 11.3.2010) (להלן: 'עניין אליהו'), פס' 26 לפסק הדין; ת"צ (מרכז) 25669-04-21 קרן אביב נ' Meta platforms. Inc (נבו, 9.7.2025), (להלן: 'עניין קרן אביב'), בפס' 60 לפסק הדין.

¹² עניין קרן אביב, שם, בפסקאות 60 ו-61 לפסק דינה של השופטת איריס רבינוביץ ברון.

¹³ את הרציונל לדברים ניתן למצוא, ביו היתר, בדברי השופטת ברק-ארז, אשר ציינה כי: "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". לעניין זה ראו בג"ץ 6732/20 האגודה לזכויות האזרח בישראל נ' הכנסת (נבו, 1.3.2021), בפס' 12 לפסק דינה של השופטת ברק-ארז.



כך למשל, רשת מרכולים המשתמשת בתמונת לקוח במסגרת מסע פרסום נרחב על-גבי חלונות ראווה, אוטובוסים ובעיתונות, תיחשב כפוגעת בפרטיות הלקוח אם מתוך המידע שנמסר לו במועד קבלת הסכמתו לצילום לא ניתן היה ללמוד על הסכמה שהתמונה תפורסם באמצעי מדיה רחבים יותר מפרסום בחלונות הראווה בסניפים.¹⁴

17. בקשת הסכמה שאינה כוללת את נתוני המידע הנדרשים לגיבוש רכיב ההסכמה "מדעת" עלולה להביא לכך שההסכמה שניתנה לא תיחשב הסכמה תקפה.

בנוגע לציון הגורמים אליהם עשוי המידע להיות מועבר – גישת הרשות היא כי ניתן להסתפק לשם כך במידע המציין בפני נושא המידע את סוג הגורמים מבחינת השיוך המקצועי שלהם (כגון "חברות פרסום" או "רשויות אכיפת חוק"), ואין הכרח לצייין פרטי זיהוי ספציפיים כגון שם החברה וכו'. עם זאת, ציון כללי מידי של סוג הגורם אליו יועבר המידע, אשר אין בו כדי ללמד על השימוש שייעשה בו על-ידי אותו גורם (כגון "חברות טכנולוגיה"), עלול להיחשב כאי-עמידה בדרישת רכיב ה"מדעת".

בכל הנוגע לסוגי המידע הנאסף ומטרות איסוף והמשך עיבוד המידע – על בעל שליטה להציג בפני נושא המידע פירוט בדבר כלל סוגי המידע וכלל מטרות עיבוד המידע, באופן שיאפשר לנושא המידע להבין איזה מידע אישי נאסף על בסיס הסכמתו, ולאילו שימושים. **ככלל, הצגה חלקית של פרטי מידע אלו (לרבות תוך שימוש בביטויים כגון "וכיו"ב" ו-"בין היתר") אינה עונה על דרישת ההסכמה מדעת.**

18. סוג המידע שעל אוסף המידע לספק לאדם לשם קבלת הסכמתו, והיקפו, תלויים בהקשר הפנייה.

לדוגמה ממשפט העבודה, בעניין קלנסווה קבע בית הדין הארצי לעבודה כי מעסיקה לא קיבלה הסכמה מדעת לאיסוף מידע ביומטרי של עובדות לצרכי רישום נוכחות במקום העבודה, וזאת, בין היתר, משום שלא הציגה בפני העובדות פרטים רלוונטיים באשר לטיב ולאופן השימוש בשעון ביומטרי, לא פרסמה מדיניות ברורה, גלויה ומידתית בנושא, ולא שיתפה את העובדות (או נציגיהן) בקביעת מדיניות זו.¹⁵

¹⁴ ת"יא (ירושלים) 20901-08 רומן מינקין נ' קו אופ ישראל רשת סופרמרקטים בע"מ (נבו, 20.2.2011).

¹⁵ עניין קלנסווה, לעיל ה"ש 6, בפס' 144 לפסק דינו של השופט איטח. במסגרת עמדת היועץ המשפטי לממשלה, שהוגשה בהליך זה, צוין בנוסף כי: "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 עובד את יסוד ה"דעת" (פס' 65 לעמדת היועץ המשפטי לממשלה). לעניין זה ראו גם ע"ע (ארצי) 90/08 טלי איסקוב ענבר - מדינת ישראל - הממונה על חוק עבודת נשים ואח' (נבו, 8.2.2011), (להלן: "עניין איסקוב"), בפס' 30 של השופטת ארד.



בעניין **סמל**, אשר עסק בפרסום תמונות עירום ללא הסכמה, קבע בית משפט השלום כי לשם קבלת הסכמה מדעת בהקשר זה היה על המפרסם לספק למצולם מידע הדרוש לו לשם קבלת החלטתו, לרבות בדבר פרסומו של המידע המצולם ודרך פרסומו.¹⁶

דוגמה נוספת ניתן למצוא בעניין **ברובצ'יוק**, בו קבע בית הדין האזורי לעבודה בתל-אביב כי מעסיקה פגעה באופן בלתי מידתי בפרטיות עובדת כאשר גרמה לה לעבור בדיקת פוליגרף בלא לקבל הסכמה מדעת. בקביעתו זו הסתמך בית הדין, בין היתר, על כך שלעובדת לא ניתן כל הסבר לגבי מהות הבדיקה, לגבי הספקות הקיימים ביחס לרמת תקפותה ומהימנותה, ביחס לאופן שבו היא מתבצעת, ביחס לשימוש שיש בכוונת הנתבעת לעשות בתוצאותיה, או ביחס לזהות הגורם אשר יבצע את הבדיקה והכשרתו.¹⁷

19. רכיב ההסכמה "**מדעת**" וסבירותו נבחנים לא רק ביחס לסוג והיקף פירוט הנתונים המוצגים לנושא המידע לשם קבלת הסכמתו, אלא גם ביחס לאופן הצגתם. מתוך כך שהסכמה חייבת להיות "מדעת" הרי שהסכמה שניתנה מבלי שלאדם הייתה האפשרות הסבירה להבין את משמעות הסכמתו והשלכותיה, לא תיחשב הסכמה תקפה. לכן, יש להקפיד כי תוכן ההסכמה והמידע הנלווה לה יוצגו באופן ברור, נגיש, פשוט ומובן.

כך למשל, אתר אינטרנט, אשר מסמך תנאי השימוש ומדיניות הפרטיות שלו אינו נגיש בצורה סבירה למשתמשים בו, או אשר מציג את האמור בהם בצורה מסורבלת, ארוכה וקשה להבנה, עשוי להיחשב כאתר שאינו עומד בתנאים הנדרשים לביסוס הסכמה מדעת לאיסוף ושימוש במידע אישי של המשתמשים בו.

20. לעניין זה ראו לדוגמה את החלטת בית המשפט המחוזי מרכז-לוד בעניין **קרן אביב**, בו נקבע כי: "... על מנת לבחון האם ניתן לאדם, בצורה ברורה, המידע הנדרש לו באורח סביר כדי להחליט אם להתיר פעולה שאחרת באה בגדר פגיעה בפרטיות, יש לערוך בחינה כפולה. תחילה, יש לבחון האם במסגרת תנאי השימוש של המשיבה, הפרקטיקה האמורה מקבלת ביטוי גלוי וברור, כך שאדם סביר יכול להבין מקריאתם את השימוש נושא בקשת האישור. בנוסף, יש לבחון את אופן מתן ההסכמה לתנאי השימוש – דהיינו, כיצד המשיבה מפנה משתמש פוטנציאלי למסמך תנאי השימוש שלה, וכיצד בפועל הוא נדרש לאשר אותו".¹⁸

21. **איסוף מידע למטרות שונות מתכלית העסקה העיקרית**: במקרים של שירות המבקש לאסוף מידע למטרות השונות באופן מהותי מתכלית העסקה העיקרית, או המבקש לאסוף ולעבד מידע בעל רגישות מיוחדת באופן שסביר כי אינו תואם לציפייה של לקוחותיו, יש לתת לכך ביטוי

¹⁶ בפסק הדין נקבע כי "משמעותה של הסכמה מדעת בהקשר זה הינה כי בידי האדם היה במועד מתן ההסכמה את המידע הדרוש לו באורח סביר כדי להחליט אם להסכים למסירת המידע, פרסומו, דרך פרסומו ולשימושים שייעשו בו, ובכלל זה להעברתו לצדדים שלישיים". ראו ת"א (הרצליה) 14-07-21945-07 פלוני נ' אריאל סמל (נבו), 31.1.2016, פסי' 42 לפסק דינו של השופט סלע.

¹⁷ סע"ש (תל אביב-יפו) 14-11-51013-11 ויקטוריה ברובצ'יוק - טופ טן אביזרי אופנה בע"מ (נבו), 15.12.2016, בפסי' 15 לפסק דינה של השופטת רות.

¹⁸ עניין קרן אביב, לעיל ה"ש 11, בפסי' 62 לפסק דינה של השופטת רבינוביץ ברון.



ובולטות במסגרת הצגת מטרות השימוש, ככל הניתן בנפרד משאר רכיבי ההתקשרות, בטרם מתן ההסכמה.

כך למשל, חברה המשווקת מזון בריאות אוספת ממשתמשים הנרשמים לאתר או לאפליקציה שלה נתונים על אודות המיקום ומסלולי התנועה שלהם, וזאת גם בעת שהאפליקציה אינה פועלת. לאור רגישות המידע ולאור ההנחה שמרבית המשתמשים אינם מצפים כי רכישת מזון במסגרת מתן השירות תביא לאיסוף נתוני המיקום שלהם בצורה זו, הרי שהסתפקות החברה בציון הדברים אך ורק במסמכי מדיניות הפרטיות ותנאי השימוש, ללא הצגת הדברים באופן בולט ומודגש, עלולה שלא להספיק לביסוס רכיב ה"מדעת". הדגשת הדברים במסמך תנאי השימוש, בעמוד הבית הראשי או בהודעה "קופצת" בעת הרישום, יכולים להביא להעלאת מודעות המשתמשים, ולסייע לחברה בביסוס רכיב ה"מדעת".

22. הנגשה לאוכלוסיות ייחודיות: במקרים ששירות מסוים מופנה בעיקרו לאוכלוסייה בעלת מאפיינים ייחודיים, כגון אנשים עם מוגבלות, יש לתת על כך את הדעת במסגרת אופן הצגת המידע הנדרש לצורך קבלת ההסכמה, ואופן קבלתה.¹⁹

כך למשל, על אפליקציות חדשות שמכוונות לאוכלוסייה של ליקוי ראייה להציג את המידע הרלוונטי לקבלת ההסכמה לשימוש באפליקציה (לרבות איזה מידע נאסף בעת השימוש באפליקציה, למי הוא עשוי להיות מועבר ולאילו מטרה), ככל הניתן באופן שיהיה נגיש עבורם, למשל תוך שימוש בכיתוב בגודל פונט מתאים, באמצעים קוליים או באמצעים ויזואליים (תמונות, אימוג'ים) העשויים לסייע להם להבין את משמעות הסכמתם.

חובת היידוע בסעיף 11 לחוק הגנת הפרטיות בראי רכיב ההסכמה מדעת

23. כאמור, ביטוי ספציפי של רכיב ההסכמה מדעת ניתן למצוא בסעיף 11 לחוק הגנת הפרטיות, הקובע כי בעת פנייה לאדם לשם איסוף מידע שנועד להיכלל במאגר מידע, יש לפרט בפני נושא המידע אם חלה עליו חובה חוקית למסור את המידע או שמסירת המידע תלויה בהסכמתו, את המטרה שלשמה מבוקש המידע, וכן למי הוא יימסר ולשם איזו מטרה.²⁰ במסגרת תיקון מס' 13 לחוק הגנת הפרטיות נקבע כי חובת היידוע לפי סעיף 11 כוללת גם את החובה להודיע לאדם מהי "תוצאת אי-ההסכמה", וכן לציין בפניו את זכותו לבקש לעיין במידע על אודותיו לפי סעיף 13 לחוק, או לבקש לתקנו או להביא למחיקתו, אם מצא כי אינו נכון, שלם, ברור או מעודכן, לפי סעיף 14 לחוק.

24. סעיף 11 מבטא את חובת היידוע החלה על כל מי שפונה לאדם לשם קבלת מידע על אודותיו לשם עיבודו במאגר מידע. לאור מיקומו של הסעיף בפרק ב' לחוק, וכן מכיוון שהוראותיו חלות

¹⁹ עיקרון זה קבוע, בין היתר, בסעיף 12 לתקנות הגנה המידע האירופאיות (להלן: 'GDPR'), אשר כולל התייחסות ספציפית לצורך להגשת מידע עבור קטינים. לעניין כללי הנגשה של מסמכים עבור אנשים עם מוגבלות ראו לדוגמה תקנות שוויון זכויות לאנשים עם מוגבלות (התאמות נגישות לשירות), התשע"ג-2013.
²⁰ להרחבה ראו עמדת הרשות להגנת הפרטיות בעניין "חובת יידוע במסגרת איסוף ושימוש במידע אישי" (יולי, 2022).



גם בנסיבות של איסוף מידע מכח הסמכה בדין, עמדת הרשות היא כי סעיף זה לא בהכרח ממצה את כל הנדרש לשם עמידה בדרישת רכיב ההסכמה "מדעת". כלומר, הצגת כל פרטי המידע המנויים בסעיף זה בעת איסוף מידע מאדם היא מספקת לשם עמידה בחובת היידוע, אך לאו דווקא לשם עמידה ברכיב ההסכמה "מדעת".

25. לאור כך, לגישת הרשות אין בעמידה בתנאי סעיף 11 כדי להבטיח עמידה בדרישה לקבלת הסכמה מדעת. עמידה בתנאי הסעיף היא דרישת המינימום המתחייבת מהוראות החוק לביסוס חובת היידוע, אך במקרים מסוימים, עשוי מבקש ההסכמה להיות מחויב בפירוט נרחב יותר מהקבוע בסעיף זה לשם ביסוס רכיב ההסכמה מדעת לפגיעה בפרטיות ולעיבוד המידע במאגרי מידע.

ומהם אותם מקרים בהם נדרשת הרחבה זו? ככלל, עמדת הרשות היא כי בנסיבות בהן קיימים פערי כוח משמעותיים בין צדדים, או כאשר מדובר בפעולה בעלת פוטנציאל לפגיעה קשה בפרטיות או בנסיבות מורכבות אחרות (כגון שימוש בטכנולוגיה חדשה שהשלכות השימוש בה אינן ברורות דיין) – יש לראות בחובה זו כחובה מוגברת, ועל מבקש ההסכמה יהא להקפיד להציג באופן בולט ופשוט את הנתונים המהותיים הרלוונטיים להחלטת נושא המידע. העדר פירוט מספק במסגרת הליך קבלת ההסכמה עלול להביא לפגיעה בתוקפה של ההסכמה.²¹

26. עוד יובהר כי הדרישה שהסכמה תהיה מדעת, כפי שפורט לעיל בחלק זה, חלה הן ביחס להסכמה הניתנת באופן מפורש והן ביחס להסכמה מכללא, קרי הסכמה משתמעת הנלמדת מהתנהגותו של אדם.

הסכמה מרצון חופשי

27. על-פי מהותה, הסכמה לפגיעה בפרטיות חייבת להינתן מתוך רצון חופשי.²² כך לדוגמה, בעניין אליהו קבע בית המשפט המחוזי כי "סעיף 1 לחוק הפרטיות קובע, שאין לפגוע בפרטיותו של אדם 'ללא הסכמתו', כאשר ביסוד 'ההסכמה' צריכים להתמלא שני תנאים: עליה להיות הסכמה שניתנה מרצון חופשי, ועליה להיות הסכמה 'מדעת'..."²³ בעניין Muzyehuk קבע בית המשפט לעניינים מינהליים בת"א, ביחס להסכמה שניתנה לכאורה לחיפוש של רשות האוכלוסין וההגירה במכשירים ניידים של המבקשים להיכנס לישראל, כי "לא ניתן לראות בהסכמה, גם בהנחה שזו ניתנה לכאורה, כהסכמה חופשית ומרצון".²⁴ בעניין איסקוב, אשר עסק בסוגיית חדירת מעסיק לחשבונות דואר אלקטרוני של עובדת, קבע בית הדין הארצי

²¹ יובהר כי במקרים בהם מבקש ההסכמה עומד בתנאי סעיף 11 אך לא בדרישה לפירוט נרחב יותר בנסיבות בהן הוא נדרש לכך, הדבר אמנם לא ייחשב הפרה של הוראות סעיף 11 לחוק, אך יהווה איסוף מידע שלא מתוקף הסכמה מדעת בניגוד להוראות סעיף 1 ו-8(ד)(1) לחוק.

²² בירנהק, ה"ש 5, בעמ' 381.

²³ עניין אליהו, לעיל ה"ש 11, בפס' 26 לפסק דינה של השופטת אהד. לעניין זה ראו גם מיכאל בירנהק ועמרי רחום טוויג פרטיות מידעית, 181 (2026).

²⁴ עמ"נ (תל אביב-יפו) 12780-01-23 Ilona Muzyehuk נ' רשות האוכלוסין וההגירה, משרד הפנים (נבו, 11.7.2023), בפס' 53 לפסק דינה של השופטת אמנון-גונן.



לעבודה כי: "קיומו של רצון חופשי כתנאי להכרה בהסכמה הוא פועל יוצא מההגנה על הזכות החוקתית לפרטיות האוסרת חזירה למרחב הווירטואלי הפרטי "שלא בהסכמתו" של אדם...".²⁵ בעניין ה"אח הקטן", אשר עסק באפשרות של הורים להשתמש בשירותי חברות פרטיות לצילום וניתוח הנעשה במעונות יום לפעוטות ציין בית המשפט העליון כי "... לא ניתן להתעלם מכך שהסכמת מנהל המעון ועובדי המעון אינה בהכרח הסכמה חופשית ומרצון, לנוכח החשש האפשרי לפרנסתם ככל שיסרבו לכך".²⁶ בעניין הסניגוריה הציבורית, אשר דן בין היתר בסוגיית ההסכמה לחיפוש גורמי משטרה בחומרי מחשב של נחקרים, קבע בית המשפט העליון כי "... במישור היחסים שבין המדינה לבין הפרט, גם מקום שבו מדובר בהסכמה מדעת, אין מדובר בהכרח בהסכמה חופשית, מה שמשיע, מיניה וביה, על מעמדה הנורמטיבי של אותה הסכמה".²⁷ על חשיבות הרצון החופשי בהסכמה לפגיעה בפרטיות ניתן ללמוד גם מעמדת היועץ המשפטי לממשלה שהוגשה לבית המשפט המחוזי בעניין גרינברג, שם נאמר כי "יש להבטיח כי ללקוח קיימת אפשרות בחירה אמיתית (ההדגשה במקור), על מנת שניתן יהיה לומר כי הסכמתו ניתנה מרצון חופשי".²⁸

28. בהקשר הרפואי נפסק כי רצון חופשי מהווה אחד מיסודות ההסכמה מדעת, וכי יסוד זה נשען על זכותו של מטופל לאוטונומיה ולקבלת החלטות עצמאיות באשר לטיפול לו הוא זקוק.²⁹

29. רצון חופשי מהווה אחד מרכיבי ההסכמה גם בדיני הגנת המידע האירופיים. כך, סעיף 4(11) לרגולציית הגנת המידע של האיחוד האירופי (GDPR) מגדיר הסכמה ככזו אשר, בין היתר, ניתנת באופן חופשי ("freely given").

30. דוגמה לפגיעה ברכיב הרצון החופשי בדיני הגנת הפרטיות ניתן לראות בשימוש בכלים עיצוביים ו"טקטיקות אפלות" (dark patterns), שנועדו להקשות על נושא המידע להבין את משמעות הסכמתו ולהשפיע באופן פסול על החלטתו. שימוש שכזה עלול להצביע על כך שההסכמה שהתקבלה בנסיבות שכאלו אינה הסכמה מדעת, ואינה כזו המבטאת את רצונו החופשי של נושא המידע.³⁰

כך למשל, אפליקציה של משחק רשת המיועדת לילדים, ה"מקפצה" בזמן המשחק ובאופן קבוע בקשה לאיסוף נתוני מיקום, ש"מקפאה" את המשחק ומפריעה למהלכו התקין, שאינה מאפשרת גישה למידע על מטרת השימוש בנתוני המיקום אלא באמצעות "יציאה" מהמשחק,

²⁵ עניין איסקוב, לעיל ה"ש 15, בפס' 30 של השופטת ארד.
²⁶ בג"ץ 70206-12-24 האח הקטן בעמ' נ' הכנסת (נבו, 5.10.2025), בפס' 8 לפסק דינו של הנשיא עמית.
²⁷ בג"ץ 8298/22 הסניגוריה הציבורית נ' היועצת המשפטית לממשלה (נבו, 31.8.2025), בפס' 42 לפסק דינו של השופט סולברג.
²⁸ עמדת היועץ המשפטי לממשלה בת"צ (מרכז) 22141-03-15 פנחס יוסף גרינברג נ' חברת סלקום ישראל בע"מ (נבו, 5.3.2020), (להלן: 'עניין גרינברג'), בפס' 55. העמדה זמינה באתר נבו.
²⁹ ע"א 1303/09 מרגלית קדוש נ' בית החולים ביקור חולים, סה(3) 164 (נבו, 5.3.2012), בפס' 3 לפסק דינו של המשנה לנשיאה א' ריבלין.
³⁰ בירנהק, לעיל ה"ש 5, בעמ' 252. להרחבה ודוגמאות בנוגע לאופן השימוש בטקטיקות אפלות להשפעה על משתמשים ראו איגוד האינטרנט הישראלי "התמודדות עם מניפולציות של רשתות חברתיות כלפי משתמשים (dark patterns)" (28.4.22).



ואשר אינה מעניקה אפשרות פשוטה לביטול הקפיצה החוזרת של ההודעה – עשויה להיחשב כאפליקציה העושה שימוש בטקטיקה אפלה לקבלת הסכמה.

31. סוגיית הרצון החופשי בדיני הגנת הפרטיות מתעוררת בעיקר במצבים בהם קיימים פערי כוח בין מבקש ההסכמה לבין נושא המידע. במצבים שכאלו הסכמה לפגיעה בפרטיות עלולה להיחשב כ"חשודה"³¹, קרי כזו שקיים ספק האם ועד כמה ניתן לראותה כהסכמה שניתנה מתוך רצון חופשי, כן ואמיתי.

32. עמדה המבטאת את הקושי בהסתמכות על הסכמה הניתנת במצבים של פערי כוחות ניתן לראות בפסיקת בית המשפט העליון בעניין **דיין**:

"כאשר אדם מתבקש למסור מידע אודות חקירה פלילית במסגרת מכרז (או במצבים קרובים, כדוגמת ראיון עבודה) והוא מוסר מידע זה מרצונו, ניתן לכאורה לטעון כי הזכות לפרטיות אינה נפגעת, מאחר שאדם זכאי למסור מידע פרטי, כל עוד הדבר נעשה בהסכמה. אולם, לאמיתו של דבר, הסוגיה מורכבת יותר. **כאשר אדם נדרש למסור מידע לצורך השתתפות במכרז (או במצבים דומים) הוא מצוי במצב של תלות המצמצם את מרחב הבחירה העומד לרשותו.** אין להניח, שבעל מכרז (או מעביד) יוכל לדרוש גילוי של כל פרט הנוגע לחייו האישיים של המועמד, ולהצדיק את הדרישה בכך שהדבר נעשה 'מרצון'" (ההדגשות אינן במקור).³²

33. **דוגמאות מרכזיות למצבים של הסכמה "חשודה" הן הסכמה הניתנת ביחסי עבודה (בין מעסיקים לעובדים ולמועמדים לעבודה),³³ הסכמה הניתנת במערכת יחסים שבין צרכן למונופול עסקי והסכמה הניתנת לקבלת שירות חיוני (כגון שירותי תחבורה ציבורית, שירותי בריאות או שירות טכנולוגי חיוני).** להלן מוצגות דוגמאות ספציפיות להסכמות חשודות:

דוגמה #1: רשת לממכר מוצרי פארם, המפעילה חנות באזור גיאוגרפי מרוחק שבו אין לתושבי האזור חלופה סבירה אלא לערוך את קניותיהם בחנות זו, המתנה את אפשרות לקוחותיה לרכוש מוצרי פארם בהצטרפות למועדון לקוחות, הכרוכה באיסוף מידע אישי רב על אודותיהם.

³¹ בירנהק, לעיל ה"ש 5, בעמ' 381. עמדה זו נזכרה וקיבלה תוקף בפסיקתו של בית המשפט העליון בעניין **הסנגוריה הציבורית**, וזאת בנוגע למערכת היחסים של הפרט אל מול רשויות המדינה, ובאופן ספציפי בנוגע לסוגיית ההסכמה לחיפוש גורמי משטרה בחומרי מחשב של נחקרים. ראו עניין הסנגוריה הציבורית, לעיל ה"ש 27, בפס' 42 לפסק דינו של השופט סולברג.

³² ע"א 8189/11 **רפאל דיין נ' מפעל הפיס** (נבו, 21.2.2013), בפס' 34 לפסק דינה של השופטת ברק-ארז.

³³ להרחבה על הסכמה חשודה ביחסי עבודה ראו עניין איסקוב, לעיל ה"ש 15, פס' 30 לפסק דינה של השופטת ארד. כמו כן ראו עמדת הרשות להגנת הפרטיות בעניין "**היבטי פרטיות בוויטור על סודיות רפואית וחשיפת מידע רפואי בקבלה לעבודה**" (מרץ, 2023).



דוגמה #2: מעסיק המבקש לפקח על פעילות עובדיו בזמן עבודתם מהבית, ולשם כך מבקש את הסכמתם לשימוש במערכת המצלמת אותם בביתם באופן רציף, בכל שעות העבודה.³⁴

דוגמה #3: חברת טכנולוגיה המבקשת "לאמן" את מערכות זיהוי הפנים שלה ופונה לשם כך לאוכלוסיות מעוטות יכולת בהצעה למתן תשלום סמלי בעבור שימוש בתמונותיהם.

דוגמה #4: מלון המבקש את הסכמת האורחים לשימוש במערכת לזיהוי פנים, אך אינו מציין זאת מראש במסגרת הליך הזמנת החדרים המקוון.

דוגמה #5: רשות מקומית או חברה המעניקה שירות חיוני מחליטה כי פניות למוקד השירות שלה יתקבלו רק באמצעות פנייה בתוכנה להעברת מסרים מידיים (כגון וואטסאפ), באופן שיחייב למעשה את מי שמבקש לפנות אליהן להשתמש בתוכנה ומכאן גם להעניק לחברה שהיא בעלת השליטה של התוכנה (כגון מטא) "הסכמה" לאיסוף ולשימוש במידע על אודותיהם.³⁵

34. לגישת הרשות, במצבים מסוימים, בהם קיים חשש אינהרנטי כי ההסכמה שניתנה היא "חשודה", הנטל להראות כי הסכמה לפגיעה בפרטיות ניתנה מתוך רצון חופשי של אדם עשוי להיות מוטל על כתפיו של מבקש ההסכמה.

במקרים שכאלו יכול מבקש ההסכמה לנקוט אמצעים שונים - כגון העמדת חלופה סבירה או אי-התניית קבלת השירות במתן הסכמה לאיסוף מידע שאינו נדרש באופן סביר לשם מתן השירות - על מנת להראות כי ההסכמה מבטאת את רצונו החופשי ואת בחירתו האמיתית של נושא המידע. גם קיומה של חלופה אחרת העומדת לנושא המידע על-ידי גורמים אחרים המעניקים שירות דומה יכולה להיחשב כמענה הולם לטענה בדבר היותה של הסכמת נושא המידע הסכמה שאינה חופשית.

בנוסף, וכפי שיצוין גם בהמשך, יישום מהלכים שונים לחיזוק הליך קבלת ההסכמה, כגון העדפת קבלת הסכמה מפורשת ולא מכללא; שימוש במנגנון של הסכמה אקטיבית (בניגוד לפסיבית); ושימוש בכלים טכנולוגיים ועיצוביים לפישוט והנגשת דרישת ההסכמה והמידע הנלווה לה – במקרים שמהלכים שאלו אינם מחויבים על-פי הוראות הדין – יאפשר לבעל שליטה להראות כי ההסכמה שקיבל ניתנה כדין.

כל האמור נכון במיוחד במקרים של מתן שירות חיוני או ביחס למקומות בהם ניתנים שירותים שכאלו.

כך למשל, חברה המפעילה שירותי תחבורה ציבורית אשר מבקשת לעבור לשימוש באמצעי תשלום מתקדמים, האוספים מידע רציף על נתוני המיקום של ציבור הנוסעים, תוכל להמשיך

³⁴ להרחבה על סוגיית הגנה על פרטיות במתכונת של עבודה מרוחק ראו עמדת הרשות להגנת הפרטיות בעניין "היבטי פרטיות במעקב אחר עובדים בעבודה מרוחק" (מאי, 2023).

³⁵ יצוין כי על-פי תנאי השימוש של אפליקציית וואטסאפ, תוכן ההתכתבות עם חשבון וואטסאפ 'עסקי', גם כאשר המשתמש הנוסף הוא חשבון פרטי והתכתובת כוללת מידע אישי, עשוי להיות מועבר לחברת פייסבוק (מטא) לצורך שימוש בו למטרות שונות, כולל הצגת פרסומות ומטרות מסחריות אחרות.



ולעמיד לציבור את האפשרות לשלם באמצעים אחרים, שאינם אוספים נתונים אלו, או באמצעים שעושים זאת תוך שמירה על האנונימיות של המשתמש.³⁶

35. **וידגש שבמצב בו אדם כלל אינו יכול לסרב לפעולה הפוגעת בפרטיותו, יהיה קשה לראות בהסכמתו ככזו שניתנה מתוך רצון חופשי, והדבר עשוי להשליך על תוקפה של הסכמה זו.**³⁷

תפיסה זו באה לידי ביטוי בפסיקת בית המשפט העליון בעניין **גוטסמן**, שם ציין בית המשפט כי "על-אף שהסכמה לצורך פגיעה בפרטיות ניתן להסיק משורה של מקרים ודרכי התנהגות, מוטב להפעיל משנה זהירות בקביעה כי נתקבלה הסכמה לפרסום".³⁸ בית המשפט המשיך וציטט בהקשר זה את דבריה של פרופ' רות גביזון, לפיהם "יש להיזהר ולא להפעיל את הכוח המצדיק של ההסכמה על מקרים בהם ברור כי אין הסכמה ממש והשימוש בהסכמה הוא לכן קונסטרוקטיבי ופיקטיבי".³⁹

36. תפיסה זו באה לידי ביטוי בעניין **בנק לאומי**, שם קבע בית המשפט המחוזי בירושלים, כי התנייה של בנק את פתיחת החשבון בו בויתור מראש על חובת הסודיות כלפי החברות הקשורות לתאגיד הבנקאי, אינה הוגנת ומקפחת את הלקוחות.⁴⁰

37. **יובהר שבנסיבות בהן הסכמה ניתנת במסגרת יחסי עבודה,**⁴¹ או כאשר על מבקש ההסכמה חלים כללי המשפט הציבורי (כגון משרד ממשלתי, רשות מקומית) – הפגיעה בפרטיות כפופה גם לעמידה בדרישת המידתיות.⁴²

הסכמה במפורש או מכללא

38. על-פי סעיף 3 לחוק הגנת הפרטיות, הסכמה לפגיעה בפרטיות יכולה להינתן במפורש (כלומר בצורה מפורשת) או להילמד מכללא, כלומר שלא במפורש ובאופן משתמע.

39. הסכמה מפורשת יכולה להינתן בכתב או בעל-פה, ומשמעותה היא שאדם הסכים באופן מפורש, ולפיכך מובהק וחד-משמעי, לפגיעה בפרטיותו בהקשר שבו התבקשה ההסכמה. **על-פי רוב,**

³⁶ להרחבה ראו מסמך המדיניות של הרשות להגנת הפרטיות בנושא "היבטי פרטיות ביישומונים (אפליקציות) לתשלום ותיקוף שימוש בשירותי תחבורה ציבורית" (יולי, 2020).

³⁷ עם זאת, ככלל, הסכמה עשויה להיחשב כתקפה גם בנסיבות בהן לא עומדת לנושא המידע חלופה מעשית אחרת למתן הסכמתו לשימוש במידע מסוים על אודותיו, וזאת כל עוד המידע נחוץ לשם מתן השירות אותו מבקש נושא המידע לקבל.

³⁸ ע"א 1697/11 א. גוטסמן אדריכלות בע"מ נ' אריה ורדי (נבו, 23.1.2013) (להלן: "עניין גוטסמן"), בפס' 30 לפסק דינו של השופט פוגלמן.

³⁹ רות גביזון "איסור פרסום הפוגע בפרטיות", בתוך זכויות אזרח בישראל – קובץ מאמרים לכבוד חיים ה. כהן, 177, 199 (1982).

⁴⁰ ע"ש (י-ם) 195/97 היועץ המשפטי לממשלה נ' בנק לאומי לישראל פ"מ תשס"ג(1) 481 (2004), בפס' 282. בית המשפט דחה בעניין זה את טענת הבנק כי הלקוחות הנם אנשים "בוגרים ועצמאים ומבינים היטב על מה הם חותמים", כך שהתנייה אינה מקפחת אותם. בית המשפט ציין כי אם הלקוח יזקק לאשראי או לכל שירות אחר מחברות הקשורות לתאגיד הבנקאי, כי אז יוכלו נותני אותם שירותים להתנות את מתן השירותים בויתור על הסודיות הבנקאית, ומכאן שאין צורך בויתור גורף ומראש על הסודיות הבנקאית, הנובעת בין היתר מחוק הגנת הפרטיות, כתנאי לפתיחת חשבון.

⁴¹ ראו עניין איסקוב, לעיל ה"ש 15.

⁴² עניין הסנגוריה הציבורית, לעיל ה"ש 27.



חתימה על חוזה, לחיצה אקטיבית על רובריקת אישור מסמך תנאי שימוש, ואמרה בעל פה מהווים הסכמה מפורשת. גם מחווה גופנית כגון הנהון בתגובה לשאלה מפורשת עשויה להיחשב כהסכמה מפורשת, אם כי בנסיבות מסוימות, וכפי שיפורט בהמשך, עלול להתקיים קושי להסתמך על סוג הסכמה שכזו.

לדוגמה, לחיצה על כפתור "אני מסכים" בתחתית מסמך תנאי שימוש בעת הורדת אפליקציה, מהווה הסכמה מפורשת לתנאי השימוש, לרבות בנוגע לתנאים המתייחסים לאיסוף ואופן השימוש במידע אישי.

40. הסכמה מכללא היא הסכמה משתמעת, קרי כזו הניתנת ללמידה מתוך הנסיבות, הסיטואציה, ודרכי ההתנהגות של האדם נושא המידע, וזאת על יסוד הפרשנות הסבירה והמקובלת של אותה התנהגות.

41. בתי המשפט קבעו לא פעם כי התנהגותו של אדם יכולה להיחשב כהסכמה מכללא לפגיעה בפרטיותו. כך לדוגמה, פעילותו הפומבית של אדם במפלגה פוליטית נחשבת על-פניו כמבטאת הסכמה מכללא לחשיפת דעתו הפוליטית. גם אדם שמשותף בצילומים לצרכי פרסום ושיווק פעילות בה הוא לוקח חלק, ובמסגרת זו גם משתף פעולה עם צוות הצילום, יתקשה לטעון בשלב מאוחר יותר כי לא נתן הסכמתו לצילומים.⁴³ באופן דומה, אדם הלוקח חלק בתהלוכה המתקיימת באופן פומבי במרחב הציבורי נחשב ככזה שהעניק הסכמה מכללא לפרסום תמונתו לעניין הדיווח התקשורתי בדבר קיום התהלוכה.⁴⁴

בעניין **ונטורה** ציין בית המשפט העליון כי מספר חשבון הבנק של אדם נמנה עם ענייניו הפרטיים ופרסומו ללא הסכמה יהיה פגיעה בפרטיות. עם זאת, כאשר אדם מושך שיק לטובת פלוני, ועליו מודפסים שמו, כתובתו, וחשבון הבנק, הרי שיש לראות בכך הסכמה בהתנהגות להעברת אותו מידע לידיעתו של כל אדם שאותו שיק יוסב לו בדרך הרגילה, ואין בפעולות הללו, ככלל, משום פגיעה אסורה בפרטיותו.⁴⁵

42. בהקשר הדיגיטלי, עמדת הרשות היא כי שימוש בשירותים דיגיטליים מסוימים עשוי לעיתים ללמד על הסכמה מכללא של משתמשים לאיסוף ועיבוד מידע על אודותיהם במסגרת שימושים אלו.

כך לדוגמה, המשך "גלישת" משתמש באתר אינטרנט, לאחר שהוצג בפניו המידע הנדרש לשם קבלת הסכמתו מדעת לאיסוף מידע על אודותיו עם כניסתו לאתר (גם אם הופנה לפירוט נוסף במקום אחר באתר), תיחשב על-פי רוב הסכמה מכללא לאיסוף המידע ושימוש בו.

⁴³ ת"א (חיפה) 24285-09-14 **יוחאי פורטל נ' ירון זוננשין** (נבו, 1.8.2016). לפסיקה דומה בעניין צילום מתעמלת בחדר-כושר ופרסום תמונתה בעיתון לצרכי שיווק ראו ת"א (פתח-תקווה) 1591/07 **יעקובסון נ' אביגד** (נבו, 16.9.2008). לביקורת על החלטה זו ראו בירנהק, לעיל ה"ש 2, בעמ' 102.

⁴⁴ ת"א (ירושלים) 6023/07 **שגב ישראל אפריאט נ' ידיעות אחרונות בע"מ** (נבו, 5.1.2008), (להלן: "עניין אפריאט").

⁴⁵ ע"א 439/88 **רשם מאגרי מידע נ' משה ונטורה** (נבו, 27.7.1994), בעמ' 822.



עם זאת, הסכמה מכללא בנסיבות שכאלו תיחשב תקפה רק בנסיבות בהן קיים קשר סביר בין מטרות איסוף המידע ואופן השימוש בו למאפייני אותו השירות. כמו כן, עמדת הרשות היא כי בהקשר הדיגיטלי הסכמה מכללא עשויה להיות ניתנת להוכחה בין היתר באמצעות הדגמת הנסיבות התומכות בקיומה של הסכמה שכזו, לדוגמה באמצעות הצגת המסכים (screens) שהמשתמשים בשירות דיגיטלי מסוים נחשפו אליהם לצורך קבלת השירות, ושכוחם להעיד על הסכמתם לאיסוף המידע ועיבודו.

43. עם זאת, חשוב לציין כי פסיקת בתי המשפט צמצמה במקרים שונים את האפשרות להסתמך על התנהגותו של אדם כהסכמה משתמעת לפגיעה בפרטיותו.

כך, במספר פסקי דין נקבע כי אין בעצם יחסי נישואין כדי להוות הסכמה משתמעת לפגיעה בפרטיות בין בני זוג, וכי שאלת ההסכמה המשתמעת לפגיעה בפרטיות בהקשר זה צריכה להיבחן ביחס לנסיבותיו של כל מקרה ומקרה.⁴⁶ בעניין **גוטסמן** קבע בית המשפט העליון, בין היתר, כי אין בעובדה שאדם הסכים לגלות פרטים מסוימים לגורמים מסוימים, כדי להוות הסכמה משתמעת לגילוי אותם פרטים לגורמים אחרים.⁴⁷ כמו כן, בעניין **זינגר** קבע בית המשפט העליון כי העובדה שאדם השאיר את תיבת הדואר האלקטרוני שלו פתוחה על גבי מחשבו, אינה מהווה הסכמה שאחר יעיין בהודעותיו.⁴⁸ בעניין **פלונית** נקבע כי הימצאותה של אישה בחוף ים כשחלק גופה העליון חשוף, אינו מהווה הסכמה מכללא לפרסום תמונתה.⁴⁹ ביחסי עבודה קבע בית הדין הארצי לעבודה, בעניין **פרידמן** ובעניין **גולדברג** כי בין עוצמת הפגיעה בפרטיות לבין טיבה של ההסכמה הנדרשת קיימת זיקת גומלין, דהיינו ככל שהפגיעה בפרטיותו של עובד קשה יותר, כך על מעסיק לקבל את הסכמתו המפורשת של העובד לפגיעה, ולא להסתפק בהסכמה הנלמדת מהתנהגותו.⁵⁰

כפי שנקבע בהתאם לנסיבות המקרה בעניין **כהן**, שפת גוף כגון הנהון ראש או הבעת פנים אינה מהווה בהכרח מסד ראייתי עובדתי מספק לרמה הנדרשת להוכחה ברורה ומודעת של הסכמה לצילום או לשימוש בתמונות לצרכים מסחריים.⁵¹ בהקשר זה ממליצה הרשות לנקוט זהירות

⁴⁶ עניין **פלונית נ' בית הדין הרבני האזורי בנתניה**, לעיל ה"ש 6. ראו גם: תמ"ש (ראשון לציון) 10-01-17772 **פלוני נ' אלמוני** (נבו, 11.11.2013); תמ"ש (פתח תקוה) 11-07-19229 **פלונית נ' פלוני** (נבו, 14.12.2015); תלה"מ (ירושלים) 1118-09-17 **ד.מ.נ' ת.מ.** (נבו, 21.5.2019); תלה"מ (תל אביב-יפו) 21-07-47127 **פלונית נ' פלוני** (נבו, 27.12.2023).
⁴⁷ עניין **גוטסמן**, לעיל ה"ש 38.

⁴⁸ רע"א 2552/16 **זינגר נ' חברת יהב חמיאס טכנולוגיות (1990) בע"מ** (נבו, 10.5.2016).

⁴⁹ ת"א (נתניה) 5680/02 **פלונית נ' שניידר אליעד** (נבו, 6.2.2006). לפסיקה דומה בה נדחתה טענה להסכמה לפרסום על יסוד העדר הסתייגות ראו: ת"א (תל אביב-יפו) 05/50267 **פלונית נ' חדשות ערוץ 10** (נבו, 29.10.2008). לדיון בדבר פגיעה בפרטיות במצב של התנגדות לצילום ולפרסום הצילום ברבים ראו רע"א 06/6902 **מנשה זרור צדיק נ' הוצאת עיתון הארץ בע"מ** (נבו, 13.8.2008).

⁵⁰ ע"ע (ארצי) 24-01-41179 **ד"ר מרק פרידמן בע"מ - רויטל אלקנר** (נבו, 26.3.2025), בפסקה 97 לפסק דינה של הנשיאה ורדה וירט לבנה; בר"ע (ארצי) 24-06-29583 **המוסד לביטוח לאומי - שני שילה גולדברג** (נבו, 28.12.2025), בפסי' 129 לפסק דינה של השופטת חני אופק-גנדלר. יצוין כי בעניין **גולדברג** נקבע שהעברת מידע רפואי מהמוסד לביטוח לאומי אל מעסיק או משלם פנסיה, מחייבת הסכמה מפורשת של עובד, ולא ניתן להסתפק בהסכמה מכללא.

⁵¹ תא"מ (עפולה) 13-07-50830 **אופיר כהן נ' שארבל קמוע** (נבו, 8.9.2019). פסיקת בית המשפט עסקה בהקשר זה בהעברת תמונות שצולמו במסגרת קמפיין פרסומי לאתר הפייסבוק העסקי של אשת הצלם בהיעדר הסכמת המצולמת או אימה לכך.



בהסתמכות על הסכמה הניתנת בדרך של מחווה פיזית או תנועת גוף ולקחת בחשבון את הצורך לתעד כי ניתנה הסכמה.

44. ככלל, שתיקתו של אדם, או העדר מחאה מצדו לאיסוף או שימוש במידע הנוגע אליו, כשלעצמם, לא יכולים ללמד על הסכמה תקפה לפי דיני הגנת הפרטיות. כלומר, לגישת הרשות, שתיקה או העדר מחאה יכולים ללמד על הסכמה לפגיעה בפרטיות רק כאשר קיימות נסיבות מהן ניתן ללמוד כי נושא המידע אכן התכוון להעניק את הסכמתו. לצד זאת, בהתאם לדרישה להסכמה מדעת, יש להוכיח כי לנושא המידע עמדה המודעות הנדרשת למתן ההסכמה.

45. גם במקרים בהם הסתמכות על הסכמה מכללא היא אפשרית, רצוי שלא להסתפק בהסכמה שכזו, אלא לפנות לאדם לקבלת הסכמתו המפורשת. זאת בעיקר במקרים של איסוף ושימוש מידע רגיש או נקיטת פעולה העלולה להביא לפגיעה קשה בפרטיות.

בהקשר זה יפים דברי בית המשפט המחוזי בעניין שטנגר, בו נדחתה עתירה לגילוי מידע על שכרם של פרקליטים המועסקים בוועדת האתיקה המחוזית, תוך שנקבע כי "יש לזכור, כי הזכות לפרטיות הינה זכות חוקתית, כך שנראה כי מן הראוי הוא לצמצם את השימוש בדוקטרינת ההסכמה מכללא אשר באה להגבילה".⁵²

46. כמו כן יש לזכור, כי הסכמה מכללא לשימוש במידע למטרה אחת, אין בה בכדי להתיר שימוש במידע למטרה אחרת. על כן, מי שאסף מידע על אודות אדם למטרה מסוימת על יסוד הסכמה מכללא, אינו רשאי להשתמש במידע למטרות אחרות, אלא לאחר קבלת הסכמה חדשה לכך מנושא המידע.

כך לדוגמה, סטודנטים צולמו במהלך שיעור בקמפוס של מוסד להשכלה גבוהה. הצילום נעשה בידיעתם ובהסכמה מכללא לעצם הצילום, אך מבלי שנאמר להם אילו שימושים ייעשו בו בהמשך. לאחר מספר שנים, מצלם התמונה מבקש להשתמש בה לצרכים מסחריים ולפרסמה כחלק מקמפיין שיווקי לחברה לשיפור ציוני בגרויות. במצב עניינים זה, אין להסתמך על ההסכמה מכללא לצילום, ועל מצלם התמונה לפנות לסטודנטים במטרה לקבל את הסכמתם המפורשת לפרסום התמונה למטרה האמורה, תוך פירוט מטרת הפרסום.⁵³

⁵² עת"מ (תל אביב-יפו) 36541-12-12 חיים שטנגר נ' ועד מחוז תל-אביב והמרכז של לשכת עורכי הדין בישראל (נבו), 25.2.2014, בפרק 3 לפסק הדין. בית המשפט קבע בעניין זה כי: "אף אם זכותם לפרטיות של הפרקליטים המועסקים על ידי ועדת האתיקה המחוזית הינה מסויגת ויש לראותם כמי שהסכימו למסירת פרטים אישיים מסוימים לציבור אותו הם משרתים, הרי שהמידע המבוקש בגדר עתירה זו נוגע לענייניו הפרטיים ביותר של אדם, אשר חשיפתו מדורגת במקום גבוה במדרג הפגיעות בפרטיות ואיני סבורה כי יש לראות את המשיבים 4-7 כמי שהסכימו מכללא לחשיפתו בעצם מינויים לתפקיד זה".

⁵³ לעניין דומה ראו: ת"א (תל אביב-יפו) 43369-03-18 שרית יחיא נ' המכללה האקדמית ספיר (נבו), 12.3.2020. בעניין זה נקבע כי הסכמת המצולמים ניתנה לעצם הצילום שלהם, ואולם לא לשימוש בתצלומים למטרות שונות, לרבות מטרות פרסום.



הסכמה אקטיבית (Opt-in) או פסיבית (Opt-out)

47. ככלל, הסכם בין צדדים במסגרתו ניתנת הסכמה אקטיבית ומפורשת לפגיעה בפרטיות, יכול לכלול הוראות ספציפיות במתכונת המלמדת על רמת מודעות גבוהה יותר לפגיעה בפרטיות, ביחס לחלק מהתנאים המפורטים בו. הסכמות אלו יכולות להינתן בשתי צורות:

האחת, על יסוד פעולה אקטיבית של אדם מתוכה ניתן ללמוד על הסכמתו (Opt-in), כגון סימון ברובריקה המתירה שימוש במידע למטרה ספציפית אחרת מהמטרה לה ניתנה ההסכמה הכללית.

השנייה, על יסוד התנהגות פסיבית (Opt-out), כגון הימנעות מסימון ברובריקה שאוסרת על שימוש במידע אישי שאינו הכרחי למתן השירות, וזאת כאשר ההסכם מבהיר כי העדר הסימון מבטא קבלה של כלל תנאי ברירת המחדל הקבועים בו.⁵⁴

עם זאת, כפי שיפורט להלן, איסוף המידע ושימוש בו מכוח הסכמה אקטיבית דווקא, קרי במתכונת של Opt-in, יכול ללמד על מודעות גבוהה יותר לרכיבי ההסכמה. בנסיבות מסוימות, מתכונת זו היא שתגשים את הדרישה להסכמה מדעת.

48. כך, בעמדת היועץ המשפטי לממשלה בעניין **גרינברג**,⁵⁵ נאמר כי שימוש במידע אישי (כגון נתוני מיקום) למטרות "פרופיילינג" שאינו קשור ישירות בתכלית העסקה, מחייב קבלת הסכמה אקטיבית לכך מצד האדם נושא המידע, ולא ניתן להסתפק בעניין זה בהסכמה פסיבית, במיוחד במצבים של פערי כוח בין הצדדים, ובשים לב לקושי ליידע אותם באופן אקטיבי בדבר משמעות הסכמתם לאיסוף ועיבוד מידע על אודותיהם.

49. חובת קבלת הסכמה אקטיבית מסוג Opt-in חלה, לעמדת הרשות להגנת הפרטיות, גם בהקשר של **שירותי דיוור ישיר**.⁵⁶ בהקשר זה עמדת הרשות להגנת הפרטיות היא שבחווה אחיד, הסכמת לקוח לשימוש במידע על אודותיו למטרת שירותי דיוור ישיר, שאיננה קשורה בתכלית העסקה, צריכה להיות במתכונת של Opt-in, באמצעותה מביע הלקוח באופן אקטיבי אינדיקציה מפורשת להסכמתו לשימוש המבוקש.

50. מעבר לכל האמור, כאשר הסכם כולל סעיפים למתן הסכמה לאיסוף מידע אישי שאינו נדרש למתן השירות, או לשימוש בו למטרות השונות מהותית ממטרת ההסכם (שלגביה ניתנה

⁵⁴ מיכאל בירנהק הסביר את הבדל בין המושגים באופן הבא: "שתי האפשרויות הן opt out לעומת opt in. במצב הראשון בררת-המחל היא שהמידע ייאסף וייעשו בו שימושים ככל שאוסף המידע מפרט, ואדם שמתנגד לכך צריך לבצע פעולה יזומה של שינוי בררת-המחל. במצב השני בררת-המחל היא שהמידע לא ייאסף, אלא אם כן האדם מסכים שהוא ייאסף... במצב של opt out האפשרות לשינוי בררת-המחל כלולה בחווה מפורש, ואז ההסכמה היא מפורשת...". ראו: מיכאל בירנהק "שליטה והסכמה: הבסיס העיוני של הזכות לפרטיות" **משפט וממשל** יא 9, 53-54 (התשס"ח).

⁵⁵ לעיל הי"ש 28.

⁵⁶ ראו הנחיית הרשות להגנת הפרטיות מס' 2/2017 "**פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר**" ושירותי דיוור ישיר".



הסכמה כללית ומפורשת), רצוי שההסכמה הנפרדת לסעיפים אלו תיעשה במתכונת של הסכמה אקטיבית (Opt-in) ולא באופן פסיבי (Opt-out).

51. גם במקרים אחרים שאינם נוגעים להסכמה המאפשרת פגיעה בפרטיות לפי סעיף 2 לחוק הגנת הפרטיות, ואשר בהם ניתן לעיתים להסתפק בהעדר התנגדות - לא תמיד ניתן להסתפק בהעדר ההתנגדות של אדם, ועל מבקש המידע לפנות בבקשה לקבלת הסכמה אקטיבית.

כך, בפסיקת בית המשפט העליון נקבע כי ככלל, במצבים של פנייה לרשות ציבורית על יסוד הוראות חוק חופש המידע, התשנ"ח-1998, למסירת מידע אישי על אדם, החוסה תחת חוק הגנת הפרטיות, **נדרשת הסכמתו האקטיבית של נושא המידע** לצורך מסירת המידע.⁵⁷

חזרה מהסכמה

52. הסכמה לפגיעה בפרטיות עשויה, במקרים מסוימים, לכלול גם את זכותו של אדם לחזור בו מהסכמתו, כלומר, לבקש את הפסקת השימוש במידע על אודותיו.

53. כך לדוגמה, בעניין **אפריאט**, נקבע כי אדם אשר העניק הסכמה לפרסום תמונתו אשר צולמה במסגרת השתתפותו במצעד הגאווה, רשאי לחזור בו מהסכמתו, בין שזו ניתנה במפורש ובין שמכללא, ומרגע שעשה כן, אין לעשות עוד שימוש בתמונה זו.

54. עמדה עקרונית המכירה בזכות לחזרה מהסכמה, במיוחד במקרים של פגיעה קשה בפרטיות, מצאה מקומה בפסיקת בית המשפט העליון בעניין **פלוני**,⁵⁸ שם ציין השופט סולברג כי:

"דומני, כי הסכמתו של אדם לפגיעה בפרטיותו, איננה סוף פסוק. מעמדה החוקתי של הזכות, אופייה האישי הקשה של הפגיעה בפרטיות, עשויים להציב את התרופות בגין חזרה מהסכמה, במקום שונה מזה שעל-פי דיני החוזים. יתכן שאכיפה לא תהא מוצדקת, בנסיבות של פגיעה קשה בפרטיות, לעומת פיצויים כספיים שיכול ותהיה הצדקה לפסוק בגין החזרה מן ההסכמה, אם זו גרמה לנזק. על-פי "מקבילית כוחות" בין עוצמת הפגיעה בפרטיות לבין תוקפה של ההסכמה, ככל שהפגיעה קטנה יותר כך יגברו הסיכויים לקבלת סעד אכיפתי; ככל שהפגיעה קשה יותר, תיטה הכף להימנע מאכיפה, תוך מתן אפשרות לסעד של פיצויים".⁵⁹

55. לעמדת הרשות, במקרים בהם נעשה שימוש במידע על אדם מתוקף הסכמה שהתקבלה כדון, והאדם נושא המידע מבקש לחזור בו מהסכמתו ולהפסיק את השימוש במידע על אודותיו,

⁵⁷ ראו ע"מ 2820/13 רוזנברג נ' רשות האכיפה והגבייה (נבו, 11.6.2014), פסקה 20 לפסק דינו של השופט שהם. להבדיל, קבע בית המשפט כי בכל הנוגע למידע העלול לגרום נזק לצד שלישי, אך אינו מוגן לפי חוק הגנת הפרטיות, ניתן להסתפק בהעדר התנגדות של הצד השלישי, ולא נדרשת הסכמה אקטיבית. לעניין זה ראו גם ע"מ 1386/07 **עיריית חדרה נ' שנירם בע"מ** (נבו, 16.7.2012).

⁵⁸ ע"מ 8954/11 **פלוני נ' פלונית** (נבו, 20.4.2014). בהליך זה דחה בית המשפט העליון ערעור על החלטת בית המשפט המחוזי, שקיבל תביעה למתן צו מניעה לפיו יאסר על המערער לפרסם ולהפיץ ספר שכתב, המגולל את מערכת היחסים האינטימית שהתקיימה בינו לבין המשיבה.

⁵⁹ שם, בפס' 160 לפסק דינו של השופט סולברג.



מומלץ כי בעלי שליטה יבחנו בחיוב קבלת בקשה זו גם במקרים בהם ההסכמה איננה הדירה מלכתחילה כמפורט בסעיפים 53-54 לעיל, וזאת במיוחד במצבים בהם המשך השימוש במידע יפגע באופן קשה בפרטיות המבקש, ובמצבים בהם בעל השליטה לא יכול להצביע על אינטרסים לגיטימיים ומשמעותיים להמשך עיבוד המידע, אשר חלקם מפורטים בהמשך.

56. יובהר כי אין בחזרה מהסכמה בכדי לפגוע בחוקיות איסוף המידע והשימוש בו שקדמו לה, ככל שההסכמה לאיסוף ולשימוש במידע ניתנה כדין. כמו כן, קבלת בקשה לחזרה מהסכמה תחייב את הפסקת פעילות עיבוד המידע שנאסף על יסוד ההסכמה, אך לא בהכרח את מחיקתו של המידע שכבר נאסף כדין בעת שההסכמה עמדה בתוקף.

57. ככלל, המשך עיבוד המידע הכרחי לקיום חובות רגולטוריות, לצורך קיום דרישות אבטחת מידע, או לשם צרכים לגיטימיים אחרים של בעל השליטה הנובעים מההתקשרות בין הצדדים, כגון לצרכי התגוננות משפטית – ייחשבו שיקולים המצדיקים אי-מתן אפשרות לחזרה מהסכמה, אלא במקרים שהוראות הדין יחייבו זאת.

58. כמו כן, שיקולים נוספים לאי-מתן אפשרות לחזרה מהסכמה עשויים להיות, אלא אם נקבע אחרת בהוראות הדין, מקרים בהם פעולת עיבוד המידע כבר הסתיימה ולא מדובר בשירות מתמשך, כגון במקרים של מידע אישי שנמסר לצורך הליכי מיון לעבודה שכבר בוצעו, או במקרים של מסירת מידע רפואי לצורך השתתפות במחקר רפואי, לאחר שכבר נעשה שימוש במידע לצרכי המחקר. כך גם במקרים בהם ימצא כי קבלת הבקשה אינה אפשרית מבחינה טכנולוגית או במקרים בהם בעל השליטה יוכיח כי קבלת הבקשה תחייבו בהשקעת משאבים בלתי סבירה.

59. במקרים בהם התנהגותו של נושא מידע עשויה ללמד כי הוא מבקש לחזור בו מהסכמתו, או ללמד על כך שההסכמה מלכתחילה ניתנה באופן נקודתי או לזמן מוגבל, מומלץ כי בעל מאגר יפנה לנושא המידע על מנת לבחון האם הסכמתו עומדת בעינה.⁶⁰

כך למשל, במקרה בו אדם הוריד אפליקציית ניווט בעת שהותו בחו"ל, ואינו עושה שימוש באפליקציה למשך פרק זמן ממושך (למשל במשך שנה), מומלץ לפנות לאותו אדם לשם יידועו כי השימוש במידע על אודותיו נמשך מתוקף ההסכמה שהעניק עם הורדת האפליקציה, ולבחון האם הסכמתו עומדת בעינה.

⁶⁰ להסדרה בדין של מנגנון ווידוא תוקף הסכמה שניתנה לתקופה קצובה בהקשר של מידע אישי פיננסי ראו סעיף 26(ב) לחוק שירות מידע פיננסי, התשפ"ב-2021, אשר קובע חובה אחת לשישה חודשים, לנקוט "פעולות הדרושות כדי לוודא כי הלקוח מודע לכך שאפשרות הגישה עומדת בעינה בהתאם להסכמתו כאמור".



סיכום: עיקרי הדגשים של הרשות להגנת הפרטיות בנושא הסכמה

60. כל פעולה המהווה פגיעה בפרטיותו של אדם לפי סעיף 2 לחוק הגנת הפרטיות חייבת להיעשות בהסכמה או מכוח הסמכה בדיון. ככלל, פגיעה בפרטיות בהיעדר הסמכה חוקית או הסכמה מהווה הפרה של הוראות החוק.

61. הסכמה לפגיעה בפרטיות, המתקבלת באופן מפורש או מכללא (קרי באופן משתמע), חייבת להיות מדעת. על כן, **על מבקש ההסכמה לפעול באופן המבטיח כי האדם נושא המידע מודע לתוכן הבקשה, למטרותיה, ולהשלכות הסכמתו או סירובו לבקשה.**

62. על מבקש ההסכמה להקפיד להעמיד בפני אדם את הנתונים הרלוונטיים הדרושים לו, באורח סביר ובצורה מובנת, בקבלת החלטתו. בקשת הסכמה שאינה כוללת את נתוני המידע הנדרשים לגיבוש רכיב ה"מדעת" עלולה להביא לכך שההסכמה שניתנה על בסיסה לא תיחשב הסכמה תקפה. סוג הנתונים והיקפם עשויים להשתנות בהתאם לנסיבות ובהן בין היתר: סוג המידע ורגישותו והשימושים המבוקשים במידע.

63. רכיב ההסכמה "מדעת" וסבירותו נבחנים לא רק ביחס לזהות, סוג והיקף פירוט הנתונים המוצגים לנושא המידע לשם קבלת הסכמתו, אלא גם ביחס לאופן הצגתם. **יש להקפיד כי תוכן ההסכמה יוצג באופן ברור, נגיש ומובן.** התייחסות מיוחדת יש לתת בהקשר זה לאוכלוסיות מיוחדות, כגון בני-נוער או אנשים עם מוגבלות.

64. במקרים של שירות המבקש לאסוף מידע למטרות השונות באופן מהותי מתכלית העסקה העיקרית יש לתת לכך ביטוי ובולטות במסגרת הצגת מטרות השימוש, ככל הניתן בנפרד משאר רכיבי ההתקשרות, בטרם מתן ההסכמה. הסכמה מכללא בנסיבות שכאלו תיחשב תקפה רק בנסיבות בהן קיים קשר סביר בין מטרות איסוף המידע ואופן השימוש בו למאפייני אותו השירות.

65. לעמדת הרשות, עמידה בתנאי סעיף 11 לחוק היא דרישת המינימום המתחייבת לשם קיום חובת היידוע, ואולם אין בה כדי להבטיח את העמידה בדרישת ההסכמה מדעת. ככלל, **בנסיבות בהן קיימים פערי כוח משמעותיים בין צדדים, או כאשר מדובר בפעולה בעלת פוטנציאל לפגיעה קשה בפרטיות או בנסיבות מורכבות אחרות (כגון שימוש בטכנולוגיה חדשה שהשלכות השימוש בה אינן ברורות דיון) – יש לראות בחובה זו כחובה מוגברת, ועל מבקש ההסכמה יהא להקפיד להציג באופן בולט ופשוט את כלל הנתונים הרלוונטיים להחלטה.** העדר פירוט מספק במסגרת הליך קבלת ההסכמה עלול להביא לפגיעה בתוקפה של ההסכמה.

66. במצבים מסוימים, בהם קיים חשש אינהרנטי כי ההסכמה שניתנה היא "חשודה", הנטל לשכנע כי הסכמה לפגיעה בפרטיות ניתנה מתוך רצון חופשי של אדם עשוי להיות מוטל על כתפיו של מבקש ההסכמה.



67. לשם בחינת השאלה האם הסכמה ניתנה מתוך בחירה ורצון חופשי אמיתי ייבחנו, בין היתר, נסיבות מתן ההסכמה, מועד קבלתה, אופן הצגת הבקשה (לרבות שימוש מבקש המידע ב"טקטיקות אפלות" ובכלים עיצוביים שנועדו להקשות על נושא המידע), אופן קבלת ההסכמה (במפורש או מכללא; באופן אקטיבי או פסיבי), וזהות הצדדים ויחסי הכוחות ביניהם.

במקרים של הסכמה חשודה יכול מבקש ההסכמה לנקוט אמצעים שונים - כגון העמדת חלופה סבירה או אי-התניית קבלת השירות במתן הסכמה לאיסוף מידע שאינו נדרש - על מנת להראות כי ההסכמה מבטאת את רצונו החופשי ואת בחירתו האמיתית של נושא המידע. גם קיומה של חלופה אחרת העומדת לנושא המידע על-ידי גורמים אחרים המעניקים שירות דומה יכולה להיחשב כמענה הולם לטענה בדבר היותה של הסכמת נושא המידע הסכמה שאינה חופשית.

68. במצב בו אדם כלל אינו יכול, הלכה למעשה, לסרב לפעולה הפוגעת בפרטיותו, יהיה קשה לראות בהסכמתו ככזו שניתנה מתוך רצון חופשי, והדבר עשוי להשליך על תוקפה של הסכמה זו. וזאת ללא קשר לשאלה האם ההסכמה ניתנה במפורש או מכללא. עם זאת, הסכמה עשויה להיחשב כתקפה גם בנסיבות בהן לא עומדת לנושא המידע חלופה מעשית אחרת אלא לתת הסכמתו לשימוש במידע על אודותיו, וזאת כל עוד המידע נחוץ לשם מתן השירות אותו מבקש נושא המידע לקבל.

69. שינוי מהותי של תנאי שימוש במידע ללא קבלת הסכמה נוספת, אם באופן מפורש ואם מכללא, יחשב כשימוש במידע שלא על יסוד הסכמה שהתקבלה מדעת ומתוך רצון חופשי.

70. אופן קבלת ההסכמה עשוי להשפיע על תוקפה. גם במקרים בהם הסתמכות על הסכמה מכללא היא אפשרית, רצוי ככל הניתן לפנות לאדם לקבלת הסכמתו המפורשת, וזאת בעיקר במקרים של איסוף מידע רגיש או נקיטת פעולה העולה להביא לפגיעה קשה בפרטיות.

71. ככלל, שתיקתו של אדם, או העדר מחאה מצדו לאיסוף מידע הנוגע אליו, כשלעצמם, לא מהווים הסכמה תקפה לפי דיני הגנת הפרטיות.

72. מתן הסכמה בעל-פה היא עניין טעון הוכחה, ועל כן מומלץ כי מבקש ההסכמה יתעד אותה באמצעים הניתנים להצגתה, וזאת בעיקר במקרים של איסוף מידע רגיש או בנסיבות בהן קיימים פערי כוח בין הצדדים.

73. הסכמה מפורשת או מכללא לשימוש במידע למטרה אחת, אין בה בכדי להתיר שימוש במידע למטרה אחרת. על כן, גם מי שאסף מידע למטרה מסוימת על יסוד הסכמה מכללא, אינו רשאי להשתמש במידע למטרות אחרות, אלא לאחר קבלת הסכמה חדשה לכך מנושא המידע.



74. כאשר הסכם כולל סעיפים למתן הסכמה לאיסוף מידע אישי שאינו נדרש למתן השירות, או לשימוש בו למטרות השונות מהותית ממטרת ההסכם (שלגביה ניתנה הסכמה כללית ומפורשת), רצוי שההסכמה במסגרת סעיפים אלו תיעשה במתכונת של הסכמה אקטיבית נפרדת (Opt-in) ולא באופן פסיבי (Opt-out).

ואולם, במקרים בהם ההסכם כולל סעיפים למתן הסכמה לשימוש במידע אישי לצרכי "פרופיילינג" שאינו נדרש או קשור ישירות למטרת שירות בין צדדים שביניהם יש פערי כוח, וכן לעמדת הרשות להגנת הפרטיות גם בהקשר של שירותי דיוור ישיר – לא ניתן להסתפק בהסכמה פסיבית, ועל ההסכמה להתקבל במתכונת של הסכמה אקטיבית נפרדת (Opt-in).

75. במקרים בהם נעשה שימוש במידע על אודותיו של אדם מתוקף הסכמה שהתקבלה כדין, והאדם נושא המידע מבקש לחזור בו מהסכמתו ולהפסיק את השימוש במידע על אודותיו, מומלץ לבחון בחיוב קבלת בקשה זו ככל האפשר, גם במקרים בהם ההסכמה איננה הדירה מלכתחילה כמפורט בסעיפים 53-54 לעיל במיוחד במצבים בהם המשך השימוש במידע יפגע באופן קשה בפרטיות המבקש ובמצבים בהם בעל השליטה לא יכול להצביע על אינטרסים לגיטימיים ומשמעותיים להמשך עיבוד המידע.

76. יישום מהלכים שונים לחיזוק הליך קבלת ההסכמה, כגון העדפת קבלת הסכמה מפורשת ולא מכללא; שימוש במנגנון של הסכמה אקטיבית (בניגוד לפסיבית); ושימוש בכלים טכנולוגיים ועיצוביים לפישוט והנגשת דרישת ההסכמה והמידע הנלווה לה – במקרים שמהלכים אלו אינם מחויבים על-פי הוראות הדין – יאפשר לבעל שליטה להראות כי ההסכמה שקיבל ניתנה כדין.

77. נזכיר, כי כל הפוגע בפרטיותו של אדם ללא הסכמתו ומבקש להסתמך לשם כך על הוראות סעיף 18(2) לחוק, צריך לעמוד בדרישת המידתיות (ראו סעיף 20(ב) לחוק). בכלל זה, עליו להיות מסוגל להצביע על הסיבות והאינטרסים הלגיטימיים המצדיקים, לגישתו, את פגיעתו בפרטיות נושא המידע, ואם לא כן הוא עלול להיות מוחזק כמי ש"פגע ביודעין במידה גדולה משהיתה נחוצה באופן סביר" לצורך האינטרסים להם ניתנה ההגנה בסעיף 18 וכמי שפעל שלא בתום לב.⁶¹

78. איסוף מידע אישי ושימוש בו הפוגעים בפרטיות, שאינם מלווים בהסכמה תקפה בהתאם לאמור במסמך זה או בהסמכה בדין, מהווים עוולה אזרחית ועשויים להוות עבירה פלילית. מעבר לכך, במקרים אלו עשויה הרשות להפעיל את סמכויות האכיפה המוקנות לה בדין וכן לסרב לאשר רישום של מאגר מידע החייב ברישום, כמו גם להשהות או לבטל רישום של מאגר קיים, שמשמעותם איסור על ניהול והחזקת מאגר המידע.⁶² בעניין זה יובהר כי על-פי סעיף

⁶¹ להרחבה וליישום הוראות סעיף 18 באירועי חירום ראו: [הרשות להגנת הפרטיות "עקרונות הגנת פרטיות בהתמודדות עם אירועי חירום" \(ספטמבר, 2024\)](#).
⁶² ראו סעיף 10(ב2) לחוק הגנת הפרטיות.



8(ד1) לחוק הגנת הפרטיות, חל איסור על עיבוד מידע אישי במאגר אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע". הוראה זו חלה על מידע שנאסף שלא מתוקף הסכמה תקפה לפי החוק, אלא אם קיימת הסמכה בדין לאיסופו.

המלצות לחיזוק הליך קבלת הסכמה מקוונת⁶³

- בעת פנייה לקבלת הסכמה מקוונת ובניסוח מסמכי מדיניות פרטיות ותנאי שימוש, הדגישו והבליטו את ההיבטים המרכזיים והמשמעותיים ביותר הנוגעים לפרטיות, לאופן השימוש במידע הנאסף במסגרת השירות ולתכליות השימוש בו.
- השתמשו בדרכים יצירתיות וחדשניות לפישוט הליך קבלת ההסכמה, ובכלל זה:
 - השתמשו בסרטוני הסברה, תמונות ואימוג'ים;
 - השתמשו ב"באנרים קופצים" להבלטת הדגשים המרכזיים הנוגעים לפרטיות;
 - השתמשו בכלים אינטראקטיביים להגברת המעורבות של משתמשים בהליך קבלת ההסכמה.
- התאימו את טפסי קבלת ההסכמה והיידוע לסוגי המכשירים השונים (כגון מחשב נייד, טלפון חכם), בהם עשוי להיעשות שימוש למתן הסכמה.
- הציגו למשתמשים רמות שונות של פירוט בדבר איסוף המידע ואופן השימוש בו (מרמת הפירוט הבסיסית הנדרשת על-פי דין ועד רמת פירוט גבוהה ומפורטת), ואפשרו להם לשלוט על רמת הפירוט לה הם מבקשים להיחשף.
- הימנעו מקבלת הסכמה גורפת למתן שירות, ואפשרו למשתמשים להחליט איזה סוגי מידע הם מוכנים כי יאספו, ולאילו מטרות.
- ככל שבכוונתכם לאסוף מידע ולהשתמש בו באופן העלול להיות חורג מהמקובל בהקשר של אותו סוג השירות – הבהירו והדגישו זאת בטרם קבלת ההסכמה, וקבלו הסכמה מפורשת לכך. כאמור, הסכמה מכללא בנסיבות שכאלו תיחשב תקפה רק בנסיבות בהן קיים קשר סביר בין מטרות איסוף המידע ואופן השימוש בו למאפייני אותו השירות.

הורים המעניקים הסכמה לאיסוף נתוני מיקום של ילדיהם לאפליקציה שנועדה לספק הגנה על ילדים במרחב הפיזי אינם מצפים שהאפליקציה תשתמש במידע לשיווק ופרסום מוצרים. על חברה המבקשת להשתמש בנתוני המיקום לצרכים אלו, לפעול להבהרת הדברים בצורה מפורשת, במסגרת קבלת הסכמה נפרדת מההורים לשימושים נוספים אלו.

⁶³ חלק זה מבוסס בחלקו על הנחיות נציב הפרטיות הקנדי. להרחבה ראו: Office of the Privacy Commissioner of Canada [Guidelines for obtaining meaningful consent](#) (13, Aug. 2021).