

הסכמה בפרטיות – עמדת הרשות להגנת הפרטיות והמלצות מעשיות לארגונים

עדכוני לקוחות

ביום 25 בפברואר 2026 פרסמה הרשות להגנת הפרטיות ("הרשות") [גילוי דעת](#) מקיף בנושא יישום עיקרון ההסכמה בדיני הגנת הפרטיות ("גילוי הדעת"). במסמך זה מבקשת הרשות לפרט ולהבהיר את עמדתה באשר לאופן שבו יש לקבל הסכמה תקפה בעידן הדיגיטלי לפי חוק הגנת הפרטיות, התשמ"א-1981 ("החוק"), וכן להתוות את התנאים והקריטריונים שעל פיהם תיבחן תקפותה של הסכמה כאמור.

גילוי הדעת מבטא את הפרשנות המשפטית המנחה את הרשות במימוש סמכויות הפיקוח והאכיפה שלה, ובכלל זה סמכויות להטלת עיצומים כספיים. להלן תמצית עיקרי הדברים והשלכותיהם המעשיות עבור ארגונים.

רכיבי ההסכמה: מדעת ורצון חופשי

החוק דורש כי הסכמה תהיה מדעת, קרי הסכמה הניתנת כשהפרט מודע למטרות איסוף המידע, לאופן השימוש בו ולהשלכות החלטתו. לעמדת הרשות, עמידה בחובת היידוע הפורמלית הקבועה בסעיף 11 לחוק מהווה דרישת מינימום בלבד, ותוקף ההסכמה תלוי במידע שנמסר בפועל ובאופן הצגתו. לפיכך, ניסוחים כלליים או עמומים - כגון שימוש בביטויים כמו "בין היתר" ביחס לסוגי המידע או למטרות השימוש - עלולים שלא לעמוד בדרישה. בדומה, כאשר מידע עשוי לעבור לגורמים נוספים, יש להבהיר את טיב השימוש במידע, למשל באמצעות ציון סוג הגורמים שאליהם יועבר (כגון "חברות פרסום").

בנוסף, על ההסכמה להינתן מתוך רצון חופשי. בהתאם, הסכמה עשויה להיחשב "חשודה" כשניתנת בנסיבות של תלות או היעדר חלופה אמיתית - למשל ביחסי עבודה, במתן שירות חיוני או כאשר השירות מותנה בהסכמה לאיסוף מידע שאינו נחוץ למתן השירות. בנסיבות כאלה, עשוי הנטל לעבור למבקש ההסכמה להראות כי ניתנה מתוך בחירה אמיתית. הרשות מציעה לצמצם סיכון זה באמצעות העמדת חלופה סבירה, הימנעות מהתניית השירות בהסכמה לאיסוף מידע שאינו חיוני והעדפת מנגנוני הסכמה מפורשים ואקטיביים.

שימושים חורגים במידע וחובת גילוי מוגברת

כאשר נעשה שימוש במידע למטרות החורגות מתכלית השירות שלשמה נאסף - או כאשר מדובר בנסיבות המגבירות את הסיכון לפגיעה בפרטיות, כגון פערי כוח בין הצדדים, מתן שירות חיוני (כמו שירותי בריאות או תחבורה) או שימוש בטכנולוגיות חדשות - הארגון עשוי להידרש לרמת גילוי והנגשה גבוהה יותר. במקרים כאלה אין להסתפק באזכור כללי במסגרת תנאי שימוש או מדיניות פרטיות, אלא יש להציג את המידע המהותי הרלוונטי להחלטת נושא המידע באופן ברור ובולט, ולעיתים אף לשקול קבלת הסכמה נפרדת, למשל באמצעות הודעה ייעודית בעת ההרשמה לשירות.

אופן קבלת ההסכמה - אקטיבית ופסיבית

על-פי החוק, הסכמה לפגיעה בפרטיות יכולה להינתן בצורה מפורשת (לדוגמה, חתימה על חוזה או לחיצה אקטיבית על רובריקת אישור מסמך תנאי שימוש) או להילמד באופן משתמע. כך לדוגמה, לעמדת הרשות, המשך גלישת משתמש באתר אינטרנט, לאחר שהוצג בפניו המידע הנדרש לשם קבלת הסכמתו מדעת לאיסוף מידע עליו עם כניסתו לאתר תיחשב על-פי רוב הסכמה מכללא לאיסוף המידע ולשימוש בו. יחד עם זאת, הסכמה כזו תהיה תקפה רק אם קיים קשר סביר בין מטרת איסוף המידע ואופן השימוש בו למאפייני השירות. ואילו במקרים של שימוש במידע אישי שאינו נדרש למתן השירות, או לשימוש בו למטרות השונות מהותית ממטרת ההתקשרות - יש להעדיף **הסכמה מפורשת ואקטיבית (Opt-in)** על פני הסכמה משתמעת או פסיבית (Opt-out).

חזרה מהסכמה

הרשות מכירה בכך כי במקרים מסוימים הסכמה לפגיעה בפרטיות עשויה לכלול גם אפשרות לחזור ממנה ולבקש את הפסקת השימוש במידע אישי, אף שאין לכך עיגון מפורש בחוק. בהתאם, כאשר אדם מבקש לחזור בו מהסכמתו - או כאשר התנהגותו מעידה על כך, הרשות ממליצה לבחון האם ההסכמה עומדת בעינה ולשקול בחיוב את קבלת הבקשה להפסקת השימוש במידע. זאת, במיוחד אם ההסכמה ניתנה למטרה נקודתית או לתקופה מוגבלת.

המלצות מעשיות – כיצד נכון לקבל הסכמה לאיסוף מידע לשימוש בו?

על סמך גילוי הדעת, ריכזנו להלן המלצות עיקריות לאיסוף הסכמה:

- **הצגה בולטת וברורה של הבקשה להסכמה:** יש להדגיש את ההיבטים המרכזיים של איסוף המידע והשימוש בו, במיוחד כאשר השימוש עלול לחרוג מהציפייה הסבירה של המשתמש.
- **הנגשה ופשטות בהליך ההסכמה:** מומלץ להשתמש באמצעים ברורים וידידותיים למשתמש כדי להנגיש את המידע הנחוץ לקבלת הסכמה מדעת, למשל על-ידי הודעות קופצות, באגרים וכלים אינטראקטיביים, ולהימנע משימוש בעיצוב מטעה "וטקטיקות אפלות" (Dark Patterns) המקשות על הפרט להבין את משמעות הסכמתו.
- **יידוע מוגבר בנסיבות מורכבות:** כאשר נעשה שימוש בטכנולוגיות חדשות העלולות לפגוע בפרטיות או במצב של פערי כוח בין הצדדים, יש להציג את המידע בצורה ברורה ובולטת.
- **קבלת הסכמה מחודשת במקרה של שינוי במטרות השימוש במידע:** שינוי במטרות השימוש במידע מחייב קבלת הסכמה נוספת מהמשתמשים, במפורש או בדרך אחרת המלמדת על מודעותם לשינוי.
- **הצעת חלופות:** במצבים של חשש להסכמה "חשודה" יש להציע חלופות סבירות, להימנע מהתניית השירות באיסוף מידע שאינו נחוץ, ולאפשר למשתמשים לבחור אילו סוגי מידע ייאספו ולאילו מטרות.
- **תיעוד הסכמה:** הסכמה היא עניין טעון הוכחה, ולכן חשוב לשמור תיעוד שלה, בפרט כאשר ההסכמה מתקבלת טלפונית או בעל-פה (למשל באמצעות הקלטה), ובמיוחד במקרים של איסוף מידע רגיש או של פערי כוחות בין הצדדים.
- **העדפת מנגנון Opt-in:** כאשר השימוש במידע אינו נחוץ למתן השירות (אלא למשל לפרסום המבוסס על פרופילינג), מומלץ לקבל הסכמה אקטיבית נפרדת.
- **אפשרות לחזרה מהסכמה:** מומלץ לבחון את המקרים המתאימים שבהם נכון לאפשר למשתמשים לחזור בהם מהסכמתם ולהפסיק שימוש במידע, ולבחון בקשות כאלה באופן ענייני.

גילוי הדעת מפרט כאמור את עמדת הרשות בקשר לאופן איסוף ההסכמה לשימוש במידע אישי וצפוי להנחות את עמדתה אף במסגרת הליכי אכיפה. כמו כן, עמדה זו עשויה גם לשמש בתי משפט בבואם להכריע בתביעות הנוגעות לפגיעה בפרטיות. על רקע זה, חשוב שכל ארגון יבחן את האופן שבו הוא אוסף הסכמה לאור עמדת הרשות, וינקוט צעדים לצמצום הסיכונים לתביעות ולצעדי אכיפה בהקשר זה.

אנו מזמינים אתכם לפנות אלינו לכל שאלה ו/או התייעצות בנושא.

*עדכון זה הוכן בסיועה של רונה טל.

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.

אנשי קשר



אסף הראל
שותף