הגנת הפרטיות – נעים להכיר

הרשות להגנת הפרטיות – מי אנחנו?

אנחנו הרשות להגנת הפרטיות, **והמשימה שלנו היא לדאוג להגנה על זכות היסוד לפרטיות** ועל מידע אישי במאגרי מידע בישראל.

אנו פועלים להגנה על מידע אישי בכלל המגזרים במדינת ישראל – המגזר הציבורי, הפרטי והמגזר השלישי, ולשם כך מוקנות לרשות סמכויות אכיפה מנהליות ופליליות שאנו מפעילים לאכיפת חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו. פעילות הרשות נועדה להבטיח שמידע אישי נאסף, נשמר ומעובד בצורה חוקית, אחראית ובטוחה, לצמצם סיכונים לפגיעה בפרטיות, ולהתמודד עם אתגרי הפרטיות בעידן הדיגיטלי, כמו איומי סייבר והיקפי השימוש ההולכים וגוברים במידע אישי.

באוגוסט 2024 אושר בכנסת תיקון מס' 13 לחוק, אשר מהווה את השינוי המקיף והמשמעותי ביותר בחוק מאז חקיקתו לפני כארבעה עשורים.

שימו לב! האם הארגון שלכם אוסף מידע אישי (Personal Data)?

עסק, חברה, עמותה או כל ארגון אחר אשר אוסף מידע אישי (על לקוחותיו, עובדיו וכד') מחויב לפעול בהתאם להוראות חוק הגנת הפרטיות והתקנות מכוחו לאורך כל מחזור החיים של המידע – החל מאיסוף המידע האישי, עיבודו ואחסונו, ועד לסיום השימוש בו ובתוך כך גם לדאוג לאבטחתו.

ריכזנו עבורכם את הדגשים המרכזיים:

1. מהו מידע אישי?

חוק הגנת הפרטיות, מגדיר **"מידע אישי"** כ**נתונים אודות אדם מזוהה או אדם הניתן לזיהוי באמצעים סבירים**, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי. כמו כן, החוק מתייחס גם ל"**מידע בעל רגישות מיוחדת**". בקטגוריה זו נכללים בין היתר – מידע אישי על צנעת חיי המשפחה של אדם ועל נטייתו המינית; מידע המתייחס למצב בריאותי; מידע גנטי; מזהה ביומטרי המיועד לשמש לזיהוי אדם או לאימות זהותו; מידע על מוצאו של אדם; על עברו הפלילי; דעותיו הפוליטיות; אמונותיו הדתיות או השקפת עולמו; נתוני מיקום של אדם המלמדים על כל אחד מסוגי המידע האמורים; מידע על הערכת אישיות שנערכה על ידי גורם מקצועי או באמצעי

שמיועד לביצוע הערכה זו; מידע על פעילות פיננסית ונתוני שכר; וכן מידע שחלה עליו חובת סודיות בדין.

זכרו! יש לעמוד בהוראות החוק ביחס לכל מאגרי המידע האישי שבידי הארגון – לקוחות, עובדים, ספקים חיצוניים וכל מאגר נוסף הכולל מידע אישי.

2. איסוף מידע אישי

הסכמה: איסוף מידע אישי מחייב קבלת הסכמה של האדם ("נושא המידע") או קיומה של הסמכה בדין. ההסכמה או אי ההסכמה של אדם לאיסוף מידע אודותיו מבטאת את האוטונומיה והשליטה של האדם במידע אישי הנוגע אליו. חוק הגנת הפרטיות קובע כי הסכמת האדם למסור מידע אישי על אודותיו צריכה להיות הסכמה מדעת. הכוונה היא שיש לתת לאדם את המידע הנדרש כדי להחליט אם הוא מסכים למסור את המידע האישי שלו, ולאיזו מטרה.

עיינו ב[גילוי הדעת] שלנו בנושא עיקרון ההסכמה.

חובת היידוע: החובה המעוגנת בסעיף 11 לחוק הגנת הפרטיות, **מחייבת כל גורם הפונה לאדם לצורך קבלת מידע אישי ליידע אותו האם חלה עליו חובה חוקית למסור את המידע או שהדבר תלוי ברצונו ובהסכמתו. כמו כן, על הפנייה לכלול התייחסות** לתוצאת אי ההסכמה ו**למטרות השימוש** במידע שמסר. בנוסף, יש לציין את שמו של בעל השליטה במאגר (בעל הארגון) ודרכי ההתקשרות עימו, ו**למי יועבר המידע**, וכן יש חובה ליידע את האדם על זכות לעיין במידע ולבקש את תיקונו אם המידע אינו נכון, שלם, ברור או מעודכן. **החובה חלה גם אם האדם פנה ביוזמתו אל הארגון כדי לקבל שירות מסוים.**

קראו את גילוי הדעת שלנו בנושא [חובת היידוע].

3. שימוש או עיבוד מידע אישי – עיקרון צמידות המטרה

"עיבוד" ו"שימוש" הם כל פעולה שמתבצעת על מידע אישי – לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו.

נדגיש כי השימוש במידע אישי צריך להיעשות רק למטרה שלשמה המידע נאסף מלכתחילה (למשל: מסירת מספר טלפון למטרת קבלת חשבונית על הרכישה באמצעות שליחת הודעת SMS).

נוסף על כן, גם פעולות שגרתיות, כדוגמת שמירת מידע במערכת ממוחשבת (אחסון), נחשבות ל"עיבוד מידע" וחייבות להיעשות בהתאם להוראות החוק. שימוש במידע אישי למטרה אחרת מהמטרה (או המטרות) שלשמן ניתנה הסכמת האדם – **אסור** לפי הוראות החוק.

זכרו! פגיעה בפרטיות עלולה להביא להטלת עיצומים כספיים בהיקפים משמעותיים על הארגון, ואף לשמש בסיס לתביעה אזרחית שתאפשר תביעת פיצוי כספי ובמקרים חמורים להוות עבירה פלילית, שעונשה עד 5 שנות מאסר.

עם סיום השימוש במידע, וכאשר אין בו עוד צורך להשגת המטרה שלשמה נאסף – רצוי להביא למחיקתו או להתממתו (תהליך שמטרתו הפיכת מידע אישי לבלתי ניתן לקישור לאדם מזוהה). מעבר לכך, הדין **מחייב** את בעל השליטה במאגר המידע לבחון פעם בשנה האם כל המידע האישי שקיים במאגרי המידע שברשותו דרוש לו, כדי לוודא שהוא לא מחזיק מידע אישי עודף. להרחבה, ראו כאן.

פן נוסף להגנה על הפרטיות כולל היבטי אבטחת מידע. **למה חשוב לשים לב?**

4. אבטחת מידע

אבטחת מידע היא נדבך מרכזי בהגנה על פרטיות. כל גורם האוסף, שומר או משתמש במידע אישי מחויב להקפיד לשמור את המידע האישי שנאסף באופן מוגן ומאובטח היטב בהתאם לחוק ולתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. זאת, בהתאם לרמת האבטחה שמאגר המידע מחויב בה, ואשר נקבעת, בין היתר, לפי סוגי המידע והיקפו. למידע נוסף בנושא זה ראו את המדריך המלא ליישום תקנות הגנת הפרטיות (אבטחת מידע) ושאלות ותשובות בנושא.

זכרו - איסוף ממוקד מצמצם את הסיכון לאירועי אבטחת מידע!

5. האם חלה על הארגון חובה לרשום את מאגר המידע או למסור הודעה לרשות?

חובת הרישום: במסגרת התיקון לחוק הגנת הפרטיות, צומצם היקף חובת הרישום החלה על מאגרי מידע, מתוך מטרה להקטין את הנטל הרגולטורי שהוטל על עסקים קטנים ובינוניים והתמקדות במאגרים המציבים איומים משמעותיים לפרטיות. חובת הרישום חלה ביחס למאגרי מידע שמטרתם העיקרית היא **איסוף מידע אישי לצורך מסירתו לאחר**, בתמורה או שלא בתמורה, במסגרת פעילות עסקית שוטפת – לרבות שירותי דיוור ישיר, וזאת אם המאגר כולל מידע אישי **על 10,000 איש ומעלה** ("סוחרי מידע"), וכן על גופים ציבוריים.

למידע נוסף, חפשו "רישום מאגר מידע" באתר הרשות להגנת הפרטיות.

לקריאה נוספת בנושא דיוור ישיר – ראו את הנחיית הרשות בעניין פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר.

חובת הודעה: במקרים שבהם יש במאגר המידע, **מידע בעל רגישות מיוחדת** (למשל, מידע על נתוני מיקום של אדם, או מידע על נטייתו המינית) **על 100 אלף איש ומעלה**, על בעל השליטה למסור הודעה לרשות שבה ייכללו זהות בעל השליטה במאגר המידע, מענו ודרכי ההתקשרות עמו, פרטי הממונה על הגנת הפרטיות אם קיימת חובה למנותו ודרכי ההתקשרות עימו. להודעה יש לצרף העתק ממסמך הגדרות המאגר, שהכנתו נדרשת מכוח תקנות הגנת הפרטיות (אבטחת מידע).

6. נתקלת באירוע אבטחה או דליפת מידע? יש לדווח לנו באופן מיידי!

לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, בעל מאגר מידע **מחויב**, במקרים המנויים בתקנות, לדווח באופן **מיידי** לרשות להגנת הפרטיות על התרחשותו של אירוע אבטחה חמור ועל הצעדים שנקט הארגון בעקבות האירוע.

ניתן לדווח על אירוע אבטחה חמור באמצעות טופס דיגיטלי.

כמו כן, ניתן להדפיס את הטופס הדיגיטלי ולשלוח לכתובת: ppa_SecurityEvents@justice.gov.il

7. מינוי ממונה על הגנת הפרטיות

בעלי שליטה במאגרי מידע מחויבים, בתנאים מסוימים, למנות ממונה על הגנת הפרטיות (DPO):

- בעל שליטה במאגר מידע שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, ויש במאגר מידע אישי על 10,000 בני אדם ומעלה. הכוונה היא לארגונים שעוסקים בסחר במידע (Data Brokers), וזאת מאחר שסחר במידע כרוך בסיכון גבוה יותר לפגיעה בפרטיות;
- בעל שליטה במאגר מידע או מחזיק במאגר מידע שעיסוקו המרכזי כולל פעולות עיבוד מידע אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר.

יצוין, כי החובה חלה גם על גופים ציבוריים.

תפקידיו של הממונה על הגנת הפרטיות: לפעול להבטחת קיום הוראות חוק הגנת הפרטיות בגוף, ולקדם הגנה על הפרטיות ואבטחת המידע במאגרי המידע של הגוף. לשם כך על הממונה להיות בעל ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע והיכרות עם תחומי פעילותו של הגוף שבו הוא ממלא את תפקידו ומטרותיו. הממונה על הגנת הפרטיות אינו חייב להיות עובד הגוף שבו ימלא את תפקידו, וניתן להיעזר בשירותיו של ממונה הגנת פרטיות שיינתנו באופן חיצוני לגוף.
לקריאה נוספת, ראו את פרסום הרשות באשר למינוי ממונה על הגנת הפרטיות.

8. עיצוב לפרטיות

עקרון ה"עיצוב לפרטיות" (המוכר כ- Privacy by Design) דוגל בעיצוב מערכות המידע והתהליכים כך שיגנו על הפרטיות, ויצמצמו למינימום ההכרחי את המידע האישי שנאסף, מעובד ונשמר. יישום העיקרון מתחיל כבר בשלב התכנון וממשיך לאורך כל מחזור החיים של איסוף המידע והשימוש בו.

אחד הכליים המרכזיים ביישום עקרון זה הוא ביצוע תסקיר השפעה על פרטיות (Privacy Impact Assessment).

מהו תסקיר השפעה על פרטיות?

תהליך אשר נועד לסייע לארגון באיתור, הערכה וניהול של סיכונים לפרטיות בפרויקטים או פעילויות עסקיות וארגוניות אחרות הכוללות עיבוד של מידע אישי. התסקיר מזהה את מכלול הסיכונים לפרטיות, בוחן חלופות ומציע את הדרך לצמצם את הסיכונים למינימום.

לפרטים נוספים, קראו את המדריך שפורסם על ידי הרשות בנושא.

לקריאה בנושא "טכנולוגיות מגבירות פרטיות"

לכלי הדיגיטלי שפרסמה הרשות להערכת סיכוני פרטיות בארגון

9. מעבירים מידע אישי לחו"ל?

אם הארגון מעביר מידע אישי לחו"ל, יש לפעול בהתאם להוראות חוק הגנת הפרטיות ולתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.

10. מקבלים מידע מהאזור הכלכלי האירופי?

אם הארגון שלכם מקבל מידע אישי מהאזור הכלכלי האירופי, עליכם לפעול בהתאם להוראות תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023. לתשומת ליבכם, החובות חלות **גם על מידע אישי אחר המצוי באותו מאגר יחד עם המידע שהתקבל מהאזור הכלכלי האירופי** – כלומר, גם על מידע אישי על תושבי ישראל שקיים במאגר שיש בו מידע אישי שהתקבל מהאזור הכלכלי האירופי.

למידע נוסף בנושא ראו את פרסום הרשות הגנת הפרטיות וכן את השאלות והתשובות בנושא.

אנחנו כאן בשבילכם!

בכל שאלה, פנייה או תלונה בנושאי פרטיות ומידע אישי – מוזמנים לפנות אלינו:

- טופס מקוון: טופס פנייה או תלונה לרשות להגנת הפרטיות
- דוא"ל לפניות כלליות: ppa@justice.gov.il
- מוקד טלפוני: 3103*

הגנת הפרטיות בארגון: מדריך חובה לעסקים

מדריך זה, מטעם הרשות להגנת הפרטיות ומשרד המשפטים, מפרט את הדגשים המרכזיים לארגונים האוספים ומעבדים מידע אישי, ומסביר את **חובות הארגון לאורך כל מחזור החיים** של המידע, החל מאיסופו ועד למחיקתו, במטרה להבטיח עמידה בהוראות החוק.

חובות מרכזיות על הארגון

אבטחת מידע היא חובה

יש להגן על המידע בהתאם לרמת האבטחה הנדרשת לפי סוג והיקף המידע.

דווחו מיידית על דליפת מידע

במקרה של אירוע אבטחה חמור, חובה לדווח לרשות להגנת הפרטיות.

מינוי ממונה הגנת פרטיות (DPO)

חובה בתנאים מסוימים, כמו סחר במידע או ניטור שיטתי של אנשים.

עקרונות יסוד בטיפול במידע אישי

איסוף מידע מחייב הסכמה מדעת

יש ליידע את האדם מדוע המידע נאסף ומהן זכויותיו בנוגע אליו.

מהו "מידע אישי"?

כל נתון על אדם מזוהה או הניתן לזיהוי, לרבות מידע רגיש.

עיקרון "צמידות המטרה"

יש להשתמש במידע אישי אך ורק למטרה שלשמה הוא נאסף במקור.