

תיקון 13 לחוק הגנת הפרטיות כל מה שצריך לדעת

מדריך זה נועד לשירות לקוחותינו, אין לראות בו חוות דעת והוא אינו מהווה תחליף לייעוץ משפטי פרטני.

כל זכויות היוצרים במדריך שמורות למשרד נשיץ ברנדס אמיר ושות'

אין לעשות במדריך כל שימוש מסחרי ואסור להעתיק ו/או לשכפל ו/או לשנות את המדריך או לשלבו במסמכים אחרים.

ינואר 2025



חלק א' - הקדמה

תאריך 5.8.24 עבר בקריאה שלישית בכנסת תיקון 13 לחוק הגנת הפרטיות - תיקון גדול, משמעותי ומקיף, אשר יכנס לתוקף ב-14.8.25. משרדנו ליווה מקרוב את דיוני הצעת החוק לתיקון חוק הגנת הפרטיות בוועדת החוקה, חוק ומשפט של הכנסת.

חוק הגנת הפרטיות, אשר נחקק בשנת 1981, ולא תוקן מאז שנת 1996, הוא החוק המרכזי בישראל המסדיר את זכותו של אדם לפרטיות. החוק חל הן על המגזר הציבורי והן על המגזר הפרטי, והוא קובע כי פגיעה בפרטיות תהווה עוולה אזרחית, ובמקרים מסוימים אף עבירה פלילית, שלצידה חמש שנות מאסר. פרק א' לחוק קובע מהי פגיעה בפרטיות, מסדיר את עקרון ההסכמה לפיו אין פוגעים בפרטיותו של אדם אלא בהסכמתו, וכן מגדיר כמה מונחים מרכזיים, כגון "הסכמה", "מחזיק, לעניין הגדרת מאגר מידע", "שימוש" ועוד. פרק ב' לחוק קובע הסדרים לצורך הגנה על הזכות לפרטיות במאגרי מידע, המכילים "מידע" או "מידע רגיש" אודות אדם. החוק גם קובע הסדר מיוחד לעניין העברת מידע בין גופים ציבוריים (פרק ד') ושורה של עניינים נוספים. הרשות להגנת הפרטיות היא הגוף המסדיר, המפקח והאוכף (הרגולטור) על פי החוק.

מהו תיקון מס' 13?

מדובר בתיקון נרחב לחוק הגנת הפרטיות, שלא תוקן, כאמור, מזה כשלושים שנים. התיקון מביא עימו שורה של חידושים, לרבות:

- חיזוק יכולות הפיקוח והאכיפה המינהליים והפליליים של הרשות להגנת הפרטיות, לרבות האפשרות להטיל עיצום כספי בסכומים גבוהים על הפרות.
- הרחבת הגדרות המונחים שבחוק והתאמתן להתפתחויות הטכנולוגיות ולהסדרי הגנת מידע אישי במדינות מובילות בעולם, בראשם ה-GDPR (רגולציית הגנת המידע של האיחוד האירופי).
- עדכון ההוראות בנושא ניהול מאגר מידע ועיבוד חוקי של מידע.
- צמצום חובת רישום מאגרי מידע והטלת חובה חדשה להודיע לרשות על מאגרים מסוימים.
- עדכון החובה למנות ממונה על אבטחת מידע, הטלת חובת מינוי ממונה על הגנת הפרטיות (DPO) בארגונים מסוימים.
- ביטול תקופת ההתיישנות הקצרה בת שנתיים של תביעה אזרחית לפי חוק זה, ומעתה תקופת ההתיישנות תהיה 7 שנים, בהתאם לדיני ההתיישנות הכלליים.
- אפשרות הגשת בקשה לחוות דעת מקדמית בעניין עמידת מאגר מידע בדרישות החוק.
- קביעת הסדר פיקוח מיוחד בגופים ביטחוניים, לרבות חובת מינוי מפקח פרטיות פנימי בכלל גופי הביטחון אשר יונחה על ידי הרשות להגנת הפרטיות.
- קביעת הוראות מיוחדות לעניין הפעלת סמכויות הרשות להגנת הפרטיות בתקופת בחירות לכנסת ולרשויות המקומיות.
- עיגון החלטת הממשלה בדבר עצמאות הרשות להגנת הפרטיות ותפקידיה.

על מי חל התיקון לחוק?

כאמור, חוק הגנת הפרטיות חל על גופים ציבוריים ופרטיים כאחד. ביתר פירוט, פרק ב' לחוק חל על מי שבבעלותו מאגר מידע (בעל שליטה במאגר) וכן על מי שמחזיק במאגר מטעם בעל השליטה. מומלץ לכל ארגון לבדוק אם החובות החדשות שנקבעו במסגרת התיקון חלות על המאגרים בשליטתו או בהחזקתו. בין היתר, יש לבדוק את סוג המידע הנשמר במאגר, מספר האנשים שמידע אודותיהם קיים במאגר (נושאי המידע), ואת סוג פעולות עיבוד המידע שמבוצעות.

חלק ב' - עדכון מונחים

מהו "מידע" עליו חל החוק?

האם בתיקון לחוק השתנו הגדרות המונחים "מידע" ו-"מידע רגיש" עליהם חל החוק?

כן. שני המונחים יעודכנו ויוגדרו מעתה "מידע אישי" ו"מידע בעל רגישות מיוחדת". המונחים הותאמו להתפתחויות הטכנולוגיות ולהסדרים המודרניים של הגנת מידע אישי בעולם.

"מידע אישי" מוגדר בתיקון לחוק באופן רחב, כנתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי. "אדם הניתן לזיהוי" מוגדר כמי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר תעודת זהות, מזהה ביומטרי, נתוני מיקום או נתון אחד או יותר הנוגע למצבו הפיזי, בריאותי, כלכלי, חברתי ועוד.

הגדרת "מידע בעל רגישות מיוחדת" כוללת רשימה סגורה של סוגי מידע, הדומה ברובה (אך לא זהה) לסוגי המידע במאגרי מידע שחלה עליהם רמת האבטחה הבינונית בתוספת השנייה לתקנות אבטחת מידע (מידע אישי על צנעת חיי המשפחה של אדם ונטייתו המינית; מצב בריאותי; מידע גנטי ועוד), למעט מאגר מידע הכולל מידע בדבר הרגלי צריכה של אדם.

מידע בעל רגישות מיוחדת - שינויים מהותיים נוספים:

1. ההתייחסות למידע על נכסיו של אדם ומצבו הכלכלי: צומצמה ההגדרה של "מידע בעל רגישות מיוחדת" רק למידע על נתוני שכר ופעילות פיננסית של אדם.
2. התווספה התייחסות למידע אישי שהוא הערכת אישיות שנערכה מטעם גורם מקצועי שכדרך עיסוק מחווה דעתו על אישיותו של אדם, או שנערכה באמצעי שמיועד לביצוע הערכה שכזו (באשר לקווי אופי, יכולת שכלית, ויכולת תפקוד בעבודה ובלמודים). גורם כזה הוא, למשל, מכון מיון, מחלקות גיוס עובדים, עורכי מבחנים ממוחשבים ועוד.
3. מידע על חברות בארגון עובדים נחשב מידע בעל רגישות מיוחדת רק אם התקבל מהאיחוד האירופי לפי תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), התשפ"ג-2023, בהתאם להוראת התוספת להגדרה.
4. "מידע אישי שהוא נתוני מיקום ונתוני תעבורה": נתונים של ספק סלולר וכן נתונים על אודות מיקומו של אדם שיש בהם כדי ללמד על חלק מהפרטים המוגדרים כ"מידע בעל רגישות מיוחדת" (מידע אישי על צנעת חייו של אדם, מידע בריאותי, מידע שחלה עליו חובת סודיות שנקבע בדיון ועוד).

מהו "מאגר מידע" עליו חל החוק?

הגדרת המונח מאגר מידע, שהוא ייחודי לדין הישראלי, נותרה בעינה. החידוש בעניין זה הוא בצמצום החריג להגדרת "מאגר מידע" לעניין אוסף הכולל רק שם, מען ודרכי התקשרות: התיקון לחוק קובע כי החריג יחול רק כאשר מדובר באוסף הכולל מידע על עד 100,000 בני אדם, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם. כלומר, אם קיים פרט מידע אחד נוסף על אותם נושאי מידע, לא יחול החריג.

מהו "עיבוד" או "שימוש" במידע עליו חל החוק?

החוק בנוסחו הקודם הגדיר את המונח "שימוש" ככל פעולה במידע, "לרבות גילוי, העברה ומסירה". התיקון לחוק קובע הגדרה מפורטת יותר ל"שימוש" ומוסיף מונח חלופי תחת אותה הגדרה - "עיבוד" בהתאם מה למונח המקובל בדינים זרים: כל פעולה שמבוצעת על מידע אישי לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו או מתן גישה אליו. יובהר, כי בניגוד ל-GDPR האירופי, ההגדרה לא כוללת פעולות של מחיקה או השמדה של מידע.

חלק ג' - צמצום חובת הרישום

חובת הרישום וחובת הודעה לרשות

האם חובת רישום מאגרי המידע נותרה בעינה?

חובת הרישום של מאגרי מידע צומצמה משמעותית, אך לא בוטלה. אילו מאגרים יהיו חייבים ברישום לאחר כניסתו של התיקון לתוקף?

1. מאגר שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, שיש בו מידע על יותר מ-10,000 בני אדם. הכוונה למאגרים של סוחרי מידע.
2. בעל השליטה במאגר הוא גוף ציבורי (משרדי ממשלה ורשויות מקומיות), למעט אם מאגר המידע כולל מידע על עובדי הגוף הציבורי בלבד. החובה (להבדיל מהוראות אחרות של התיקון) אינה חלה על גופים ציבוריים נוספים המנויים בצו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו-1986.

מהי החובה החדשה למסירת הודעה לרשות להגנת הפרטיות?

מאגר שיש בו מידע בעל רגישות מיוחדת על יותר מ-100,000 בני אדם, שאינו חייב ברישום (כלומר לא של גוף ציבורי ולא של סוחר מידע), יהיה חייב במסירת הודעה לרשות על זהות בעל השליטה, מענו ודרכי ההתקשרות עימו, וזהות הממונה על הגנת הפרטיות בארגון ודרכי ההתקשרות עימו (אם נדרש מינוי). כמו כן, בעל השליטה במאגר כאמור נדרש למסור לרשות העתק ממסמך הגדרות המאגר שעריכתו נדרשת לפי תקנה 2 לתקנות אבטחת מידע.

מה לגבי מאגרי מידע שכבר רשומים במרשם ולא יהיו חייבים ברישום בעת כניסת התיקון לתוקף?

בעלי השליטה במאגרי מידע שאינם חייבים עוד בחובת רישום רשאים להודיע על כך לרשות להגנת הפרטיות, אשר תימחק את רישומו של מאגר המידע מהמרשם. אם לא תימסר הודעה, המאגר יישאר רשום ואז תחול על בעל השליטה במאגר החובה לעדכן את הרישום ככל שפרטים השתנו (החלפת מחזיקים, עיבוד סוגי מידע חדשים ועוד). אם חלה על המאגר חובת הודעה לרשות, ומבקשים למחוק את המאגר, חייבים למסור הודעה כאמור חלף הרישום או ניתן להשאיר את המאגר רשום כפי שהוא (ומעודכן בפרטיו).

האם צמצום חובת הרישום משמע שמאגרים שפטורים מרישום או הודעה לרשות פטורים מעמידה בחוק או בתקנות?

לא. כל מאגר חייב לעמוד בחובות המהותיות של החוק והתקנות. חשיבותו של מסמך הגדרת המאגר גברה עם התיקון לחוק, שכן הוא ממפה את המידע הנדרש לארגון כדי להבין איזה מידע הוא מעבד, מי המחזיקים, וכיצד בזה, כדי לקיים את החובות המהותיות הנגזרות מעיבוד המידע.

אם יש לי מאגר מידע שטרם נרשם, האם לרשום אותו או להמתין עד כניסת התיקון לתוקף?

ביחס למאגרים שממילא יהיו טעונים רישום לפי התיקון לחוק, יש לפעול לרישומם. לגבי מאגרים שיהיו כפופים לחובת הודעה לרשות עם כניסת התיקון לתוקף, הכריזה הרשות בדיוני הכנסת שלא יהיה שינוי ממדיניות האכיפה של הרשות עד היום, במסגרתה אכפה בעיקר את העמידה בחובות המהותיות ולא את אי הרישום כשלעצמו. עם זאת, ככל שמדובר במאגרים עם היקף מידע משמעותי או סוגי מידע מהרגישים יותר, כגון ביומטרי, מוצע בכל זאת לרשום את המאגר ולהמיר לאחר מכן בהודעה. ביחס למאגרים שלא יהיו כפופים לרישום או הודעה, כגון מרבית מאגרי העובדים, נראה כי לאור מדיניות האכיפה של הרשות ניתן להסתפק במסמך הגדרות מאגר עדכני וקיום שאר החובות המהותיות.



DATA

חלק ד' - עדכון הגדרות בעלי התפקידים, חובת מינוי DPO ושינויים בחובה למנות ממונה אבטחת מידע

מיהם ה"שחקנים" העיקריים של רגולציית הגנת המידע במאגרי מידע?

- עד היום החוק הגדיר את המונחים "מחזיק" ו"מנהל מאגר". החידוש המרכזי בעניין זה בתיקון 13 הוא הוספת הגדרת המונח "בעל שליטה". בדומה להגדרת "Controller" ב-GDPR (רגולציית הגנת המידע של האיחוד האירופי), בעל שליטה הוגדר בתיקון 13 כ-"מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או ארגון שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר מידע". יש לשים לב שבניגוד ל-GDPR, ההגדרה הישראלית לא כוללת את הרכיב של קביעת האמצעים לעיבוד המידע, מתוך הבנה שבמקרים רבים, דוגמת אחסון ענן, האמצעים לעיבוד המידע נקבעים דווקא על ידי המחזיק ומתוך רצון לשמר את אחריות בעל השליטה גם במקרים אלה.
- התיקון לחוק קובע הגדרה רחבה יותר למונח "מחזיק" מזו הקיימת כיום בחוק. ההגדרה החדשה פותרת אי בהירויות לגבי השאלה מי נחשב "מחזיק", ודומה כעת להגדרת "Processor" ב-GDPR. התיקון לחוק מגדיר "מחזיק" כ-"גורם חיצוני לבעל השליטה במאגר מידע המעבד מידע עבורו". שינוי ההגדרה של "מחזיק" מעלה שאלות לגבי המונח "גורם חיצוני" בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (אשר קובעת את החובה לערוך הסכם עיבוד מידע), שנותר בעינו ולא הובהר או נוסח במדויק במסגרת התיקון לחוק. לפיכך, הרשות להגנת הפרטיות תידרש להבהיר מה נותר תחת הגדרת "גורם חיצוני", אם נותר, לאחר שהגדרת "מחזיק" הורחבה כאמור.
- ומה בנוגע ל"מנהל המאגר"? עד היום הוגדר המונח בחוק כ"מנהל פעיל של ארגון שבבעלותו או בה חזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה". החוק הטיל על "מנהל מאגר" אחריות אישית ביחד ולחוד עם בעל המאגר. התיקון לחוק קובע כעת כי "מנהל המאגר" הוא "בעל שליטה במאגר מידע, ולעניין גוף ציבורי, כהגדרתו בסעיף 23 לחוק – המנהל הכללי של ארגון שבבעלותו או בהחזקתו מאגר מידע או מי שהמנהל הכללי הסמיכו לנהל את המאגר". כלומר, עם כניסתו לתוקף של החוק תבוטל חובת מינוי מנהל מאגר מידע בגופים פרטיים, והחובות שעדיין מוטלות על מנהל המאגר בחוק יחולו רק על בעל השליטה במאגר המידע. כלומר, גם בגוף ציבורי מנהל המאגר לא ישא בחבות אישית על הפרת הוראות החוק.

מינוי DPO היא חובה חדשה בדין הישראלי, אך היא קיימת מזה כמה שנים ברגולציית הגנת המידע האירופית (GDPR). באופן כללי, תפקידו של ה-DPO לשמש כתובת מקצועית להנהלת הגוף ולעובדיו בכל הקשור להיבטי הגנת הפרטיות בארגון וכן לוודא עמידה בהוראות החוק ותקנותיו.

מיהם הגופים הנדרשים למנות ממונה על הגנת פרטיות (DPO)?

- גופים ציבוריים (משרדי ממשלה, רשויות מקומיות) וכן גופים המנויים בצו הגנת הפרטיות (קביעת גופים ציבוריים), כגון אוניברסיטאות וקופות חולים.
- סוחרי מידע – בעל שליטה במאגר מידע הכולל מידע אישי על יותר מ-10,000 בני אדם, שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר, כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר. נזכיר כי מאגרים אלה חייבים בחובת רישום לפי התיקון לחוק.
- בעל שליטה או מחזיק במאגר מידע שעיסוקו העיקריים כוללים פעולות עיבוד מידע, אשר נוכח טיבו, היקפו או מטרתו מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר. הדוגמאות המוזכרות בתיקון בהקשר זה הן ספק מורשה לפי חוק התקשורת (בזק ושידורים), ספק סלולר, ספק אינטרנט, רשתות כבלים ולווין וספק שירות חיפוש מקוון. דוגמאות שניתנו על ידי ה-EDPB (המועצה להגנת מידע של האיחוד האירופי) לדרישה המקבילה ב-GDPR ועשויות להיות רלוונטיות גם בישראל כוללות, בין היתר, חברת אבטחה המפעילה מצלמות אבטחה בכמה קניונים או מרכזים מסחריים; אפיון אנשים על בסיס מידע אישי ("פרופילאות") למטרות הערכת סיכונים (לצרכי קביעת פרמיות ביטוח, מניעת הונאות וכדומה); מעקב אחר נתוני מיקום באמצעות אפליקציות סלולריות; מעקב אחר נתוני בריאות באמצעות טכנולוגיה לבישה; ואיסוף מידע מכלי רכב חכמים.
- בעל שליטה או מחזיק שעיסוקו העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר, לרבות בנק, חברת ביטוח, בית חולים כללי וקופת חולים. זוהי הקטגוריה הרלוונטית ביותר למרבית הגופים הפרטיים, אשר יצטרכו לבחון אם הם מעבדים מידע בעל רגישות מיוחדת ואם העיבוד הינו בהיקף ניכר.

מהו אותו עיבוד מידע ב"היקף ניכר" המוזכר בשתי הקטגוריות מעלה?

התיקון לחוק קובע שלשם כך יש לבחון את כמות בני האדם שמידע מעובד לגביהם, שיעורם באוכלוסייה מסוימת, היקף המידע, כמותו, טווח סוגי המידע המעובד, משך ותדירות פעולות העיבוד, משך השמירה, והתחום הגיאוגרפי של פעולות העיבוד.

מהם תפקידי ה-DPO (ממונה הגנת פרטיות)?

ה-DPO לא הוגדר בתיקון לחוק כגורם מבצע אלא כגורם מתכלל, מפקח ומייעץ. תפקידיו המנויים בתיקון לחוק כוללים:

- לשמש סמכות מקצועית ומוקד ידע בתחום הגנת הפרטיות; לייעץ להנהלת הארגון ולעובדיו; להכין תוכנית הדרכה ולפקח על ביצועה.
- להכין תכנית לבקרה שוטפת על העמידה בהוראות חוק הגנת הפרטיות לגבי מאגרי מידע, לוודא ביצועה, לדווח להנהלת הארגון על הממצאים ולהציע הצעות לתיקון הליקויים.
- לוודא קיומם של נוהל אבטחת מידע ומסמך הגדרות המאגר, שיובאו לאישור הנהלת הארגון, כנדרש לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.
- לוודא טיפול בפניות של נושאי מידע, ובכלל זה בקשות לעיון במידע או לתיקונו.

ה-DPO נדרש לדווח ישירות למנכ"ל הארגון או לעובד שכפוף ישירות למנכ"ל.
הוראה זו מדגישה את מעמדו הבכיר של ה-DPO בארגון ואת החשיבות שבמתן סמכויות מספקות לממונה, באופן שיאפשר לו לבצע את תפקידו באופן מיטבי.

יש לפרסם לציבור באופן נגיש ופשוט את דרכי ההתקשרות עם ה-DPO.

בדרך כלל מידע זה יכלול במסגרת מסמך מדיניות הפרטיות של הארגון.

מי יכול לשמש DPO?

- מי שהוא בעל ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע והיכרות עם תחומי פעילותו של הארגון. בוועדת החוקה, חוק ומשפט של הכנסת נערך דיון בשאלת היקף הידע הנדרש בנושא אבטחת מידע, שהרי DPO אינו חופף בתפקידיו או בסמכויותיו לפונקציה של ממונה אבטחת מידע. הובהר בדיונים כי במונח "הבנה הולמת", להבדיל מ"ידע מעמיק", הכוונה להבנה מספקת שתאפשר לוודא את הציות הארגוני לחובות הרגולטוריות בתחום אבטחת המידע. ואולם הנושא עשוי להגיע בעתיד לפתחם של הרשות להגנת הפרטיות ושל בית המשפט, שיידרשו לפרשנות המונח "הבנה הולמת".
- יובהר כי ניתן למנות DPO חיצוני, שאינו עובד הארגון.
- ה-DPO לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים עם מילוי תפקידיו לפי חוק הגנת הפרטיות. הוראה דומה קיימת ב-GDPR. ה-EDPB מנה כמה בעלי תפקידים שאינם יכולים לשמש, נוסף על תפקידם, גם כ-DPO, כמו המנכ"ל, מנהל משאבי אנוש או מנהל מערכות המידע. כמו כן, אין להכפיף את ה-DPO לנושא משרה בגוף עצמו או בגוף אחר אם הדבר עלול להעמידו בחשש לניגוד עניינים כאמור. הרשות להגנת הפרטיות הבהירה עוד במסמך המלצות למינוי ממונה הגנת פרטיות שפורסם בעבר כי בדרך כלל ה-DPO אינו יכול לשמש גם כממונה אבטחת המידע. זאת, משום שתפקידו של DPO רחב יותר, וכולל, בין היתר, הנחיה מקצועית של ממונה אבטחת המידע באשר לאופן בו יש ליישם את דרישות האבטחה כדי לשרת את תכליות דיני הגנת המידע האישי ולהבטיח שמירה מיטבית על הזכות לפרטיות בארגון.
- יצוין בהקשר זה כי בהחלטה משנת 2020 הטילה הרשות להגנת המידע הבלגית עיצום כספי בסך 50,000 אירו על חברת טלקום שמינתה את קצין הציות שלה כממונה הגנת מידע, באופן שהפר את הוראות ה-GDPR. החלטות דומות התקבלו לאחר מכן במדינות האיחוד האירופי והנושא אף הגיע להכרעת בית הדין האירופי לצדק, שאשרר את איסור ההחזקה בשני כובעים מנוגדים כאמור.



מינוי ממונה על אבטחת מידע

מדובר בחובה שהייתה קיימת עוד לפני התיקון לחוק, אך עברה כמה שינויים. בעקבות התיקון, יהיו ארגונים שיידרשו למנות כעת הן DPO והן ממונה על אבטחת המידע.

מיהם הגופים הנדרשים למנות ממונה על אבטחת מידע?

- בעל שליטה או מחזיק בחמישה מאגרי מידע החייבים ברישום או בהודעה לרשות להגנת הפרטיות. זהו תיקון לעומת הנוסח הקיים, שחייב רק מחזיק בחמישה מאגרי מידע במינוי.
- גוף ציבורי – משרדי ממשלה, רשויות מקומיות וגופים המנויים בצו הגנת הפרטיות (קביעת גופים ציבוריים), כגון קופות חולים ואוניברסיטאות.
- בנק, חברת ביטוח וחברה העוסקת בדירוג או בהערכה של אשראי.

נזכיר כי תקנה 3 לתקנות אבטחת מידע קובעת שבין אם חלה חובה למנות ממונה אבטחת מידע ובין אם מונה ממונה מבלי שחלה חובה כזו, עליו להכין נוהל אבטחת מידע ולהביאו לאישור בעל המאגר. כן עליו להכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אבטחת מידע, לבצע אותה ולהודיע לבעל המאגר על ממצאיו.

בנוסף, תקנה 3 לתקנות אבטחת מידע קובעת כי ממונה אבטחת מידע יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר. בנוסף, ממונה אבטחת המידע לא יכול לשמש כמנהל מאגר המידע וכן לא ישמש בתפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים. עמדת הרשות להגנת הפרטיות היא אפוא שממונה אבטחת המידע לא יכול לשמש גם כמנהל מערכות המידע של הארגון.

בניגוד ל-DPO, התיקון לא מציין במפורש כי ממונה אבטחת מידע יכול אף הוא להיות חיצוני לארגון, אולם הרשות להגנת הפרטיות הבהירה כי לדעתה הדבר אפשרי.

חשוב לשים לב לכך שהממונה על אבטחת המידע חב באחריות אישית לאבטחת המידע (ס' 17ב(ב) לחוק). בניגוד ל-DPO, שאינו חב באחריות אישית.

חלק ה' - ועיצומים כספיים סמכויות האכיפה של הרשות להגנת הפרטיות

סמכויות האכיפה של הרשות להגנת הפרטיות - מה נשתנה בתיקון 13?

תיקון 13 מרחיב בצורה ניכרת את סמכויות הפיקוח והאכיפה של הרשות להגנת הפרטיות:

1. לראשונה עוגנה סמכות להטיל עיצום כספי בגין הפרה של הוראות החוק, תקנות אבטחת מידע ותקנות העברת מידע מהאזור הכלכלי האירופי. עד התיקון, לרשות הייתה סמכות להטיל קנס מינהלי בסכומים נמוכים מאוד בגין מספר מועט של הפרות, ולא ניתן היה להטיל בכלל קנס על הפרה של תקנות אבטחת מידע. ראו הרחבה בנושא מטה.
2. הוסדרו סמכויות פיקוח שוטפות על הוראות החוק לרבות אלה שהרשות מוסמכת להורות על הפסקת הפרתן וכן סמכויות בירור מינהלי שחלות מקום בו מתעורר יסוד סביר להניח כי בוצעה הפרה של הוראות החוק.
3. עוגנה סמכות להורות על הפסקת הפרה ביחס להפרות מסוימות, כמו למשל אם נמצא כי נעשה שימוש בידיעה על ענייניו הפרטיים של אדם במאגר מידע שלא למטרה לשמה נמסרה (הפרה של סעיף 2(9)); אם נמצא כי מידע אישי עובד למטרה שמהווה פגיעה בפרטיות לפי סעיף 2 לחוק; אם הופרו הוראות מסוימות הנוגעות למינוי DPO ועוד. המשמעות היא שבגין הפרות אלה לא ניתן להטיל עיצום כספי באופן ישיר ומיידי על המפר, אלא הרשות תצטרך קודם להודיע לבעל השליטה או למחזיק כי מעשיו מהווים הפרה לכאורה, לתת לו זכות טיעון, ואם לא תשתכנע אחרת, להורות לו להפסיק אותה באופן ובתקופה שתורה. רק אם לא תופסק ההפרה יוטל עיצום כספי. ביחס לחובת מינוי DPO במגזר הפרטי, הטלת עיצום כספי תתאפשר רק לאחר שיתפרסם צו של שר המשפטים, באישור ועדת החוקה, חוק ומשפט של הכנסת. לעומת זאת, ניתן יהיה להטיל עיצום כספי ישיר על אי-מינוי DPO במגזר הציבורי או אצל סוחר מידע.
4. נקבעה הסמכות במקרים חמורים וקיצוניים לפנות לבית המשפט בבקשה לקבל צו שיפוטי שיורה על הפסקת עיבוד מידע אישי ואף למחיקת המידע שבמאגר במלואו, אם יש יסוד סביר להניח כי מתבצעת או עומדת להתבצע הפרה של הוראות מסוימות וכאשר הדבר נדרש לשם הפסקת ההפרה. למשל, במצבים של הפרת צמידות המטרה, עיבוד ללא הרשאה, עיבוד לא חוקי, והפרת חובת אבטחת המידע, לרבות תקנות אבטחת מידע ומסירת מידע מגוף ציבורי בניגוד להוראות החוק. צו כאמור יכול להינתן במעמד שני הצדדים, לאחר שניתנה זכות טיעון לפני בית המשפט, או במעמד צד אחד, ל-48 שעות בלבד, במהלכן לא יינתן צו מחיקה.
5. עוגנה הסמכות לקיים הליך פיקוח רחב (אודיט). מדובר בהליך שהרשות מקיימת בשנים האחרונות, אך כעת הוסדר לראשונה בחוק. במסגרת זו מתקיימים פיקוחי רחב מגזריים או נושאים לבחינת עמידה בהוראות החוק והתקנות.

מהם עקרונות העיצום הכספי?

העיצום הכספי הוא כלי אכיפה מנהלי (ולא פלילי), המאפשר לרשות מינהלית להטיל סנקציה כספית במקרים של הפרת הוראות חוק ותקנות רגולטוריות. בעניינו, חוק הגנת הפרטיות יאפשר להטיל עיצום כספי על בעל השליטה או על מחזיק המאגר בהתאם להוראות התיקון.

מנגנון העיצום הכספי בתיקון 13 חל על כמה קטגוריות של הפרות, בהן: הפרות הנוגעות לחובת הרישום של המאגר או הודעה לרשות; הפרה של זכויות פרטניות של נושאי מידע; הפרות הקשורות בגודל המאגר. הפרה של קטגוריות מסוימות של הוראות החוק תוביל להטלת סכום כספי קבוע והפרה של קטגוריות מסוימות אחרות תוביל להטלת סכום שיוכפל במספר נושאי המידע במאגר.

ניתן להטיל כמה עיצומים אם בוצעו כמה הפרות שונות, אולם יוטל רק עיצום כספי אחד בגין אותו מעשה המהווה הפרה של כמה הוראות. כל הסכומים צמודים למדד ומתעדכנים אחת לשנה.

עיצומים על הפרת הוראות החוק

ההפרה	סכום העיצום (צמוד למדד אחת לשנה)	הערות
חובת רישום מאגר (גוף ציבורי וסוחר מידע) או הודעה לרשות על מאגר עם מידע בעל רגישות מיוחדת על 100,000 אנשים ומעלה או אי מסירת הודעה על שינוי בפרטי המאגר	מאגר רגיל - 150,000 ש"ח	מעל מיליון אנשים - 300,000 ש"ח
זכויות פרטניות של נושאי מידע כמו סירוב לבקשת זכות עיון או סירוב לבקשת תיקון או סירוב למחוק ממאגר לדיוור ישיר	15,000 ש"ח לכל הפרה	
פנייה לקבלת מידע מבלי שנמסרה הודעה כנדרש (סעיף 11, סעיף 17א)	מידע רגיל - 50 ש"ח עבור כל פנייה שנעשתה	מידע בעל רגישות מיוחדת - 100 ש"ח עבור כל פנייה שנעשתה
הפרות הקשורות בגודל המאגר (למשל: פנייה לקבוצה בלתי מסוימת ללא הודעה לפי סעיף 11; אי מינוי ממונה אבטחת מידע; אי מינוי DPO בגוף ציבורי או סוחר מידע; אי ציות להוראת הפסקת הפרה)	מידע רגיל - 2 ש"ח לכל אדם במאגר	מידע בעל רגישות מיוחדת - 4 ש"ח לכל אדם במאגר
		סכום העיצום לא יפחת מ- 30,000 ש"ח
		סכום העיצום לא יפחת מ- 20,000 ש"ח (מידע רגיל) ומ- 40,000 ש"ח (מידע בעל רגישות מיוחדת)

הפרה	סכום העיצום (צמוד למדד אחת לשנה)	הערות
הפרת חמורות (למשל: הפרת הוראה של ראש הרשות להפסיק שימוש בניגוד למטרה או לגבי מידע שנאסף בניגוד להוראות כל דין; עיבוד מידע אישי למטרה שאינה כדן; עיבוד מידע ללא הרשאה)	מידע רגיל - 4 ש"ח לכל אדם במאגר	סכום העיצום לא יפחת מ-200,000 ש"ח
אי מסירת מסמך או עותק מחומר מחשב למפקח (כחלק מסמכות הפיקוח והבירור המנהלי)	300,000 ש"ח	
עיבוד בניגוד למטרה כאשר ניתן היה לקבוע כדן מטרה כאמור (הפרת סעיף 8(ב))	מאגר המנוהל בידי יחיד - 2,000 ש"ח רמת אבטחה בסיסית - 2,000 ש"ח רמת אבטחה בינונית - 40,000 ש"ח רמת אבטחה גבוהה - 160,000 ש"ח	

תקנות אבטחת מידע - עיצומים כספיים

לגבי תקנות אבטחת מידע, עיצומים כספיים מוטלים רק על הפרות של הוראות ספציפיות. כלומר, לא כל הפרה של התקנות תגרור הטלת עיצום כספי ובמקרים מסוימים העיצום אף אינו חל על כל היבט של הפרת התקנה. לדוגמה, לא ניתן להטיל עיצום כספי על הפרת תקנה 3, העוסקת בתפקידו של הממונה על אבטחת המידע. לגבי החובה לשמור תיעוד של הגישה למידע (לוגים), החובה בתקנות הינה לשמור תיעוד ל-24 חודשים, אולם העיצום הכספי יוטל על מי שלא שמר לפחות 12 חודשים, דהיינו די בשמירת התיעוד 12 חודשים על מנת שלא יוטל עיצום. כמו כן, ביחס לחלק מהתקנות, הטלת עיצום כספי תתאפשר רק לאחר קבלת התראה מהרשות. העיצומים הכספיים יוטלו בסכומים קבועים, לפי סוג ההפרה; סכום העיצום בגין אותה הפרה גבוה יותר ככל שרמת האבטחה של מאגר המידע גבוהה יותר. נזכיר, כי תקנות אבטחת מידע עצמן קובעות הוראות שונות, בהתאם לרמת האבטחה של המאגר.



עיצומים על הפרת הוראות תקנות אבטחת המידע

ההפרה	סכום העיצום (צמוד למדד אחת לשנה)	הפרת הוראות תקנות אבטחת מידע (תוספת שלישית)
הפרת הוראות לגביהן נקבע כפל סכום העיצום:	קטגוריה מחמירה יותר: הפרת הוראות תקנות מסוימות (כמו מסמך הגדרות מאגר, בדיקת מידע עודף, נוהל אבטחה, תיעוד אירוע אבטחת מידע ועוד):	הפרת הוראות תקנות מסוימות (למשל: אי הכנת מסמך מבנה מערכות המאגר; אי קיום הדרכת כוח אדם ועוד):
(1) אי עריכת סקר סיכונים, אי עריכת מבדקי חדירות:	מאגר המנוהל בידי יחיד - 2,000 ש"ח	מאגר המנוהל בידי יחיד - 1,000 ש"ח
רמת אבטחה גבוהה - 320,000 ש"ח (ואם במאגר יש מידע על יותר ממיליון אנשים - 640,000 ש"ח).	רמת אבטחה בסיסית - 2,000 ש"ח	רמת אבטחה בסיסית - 1,000 ש"ח
(2) אי דיווח לרשות על אירוע אבטחה חמור:	רמת אבטחה בינונית - 40,000 ש"ח	רמת אבטחה בינונית - 20,000 ש"ח
רמת אבטחה בינונית - 80,000 ש"ח	רמת אבטחה גבוהה - 160,000 ש"ח (ואם במאגר יש מידע על יותר ממיליון אנשים - 320,000 ש"ח).	רמת אבטחה גבוהה - 80,000 ש"ח (ואם במאגר יש מידע על יותר ממיליון אנשים - 160,000 ש"ח).
(3) הפרה של תקנה 15 לעניין עיבוד מידע במיקור חוץ (בקרה ופיקוח, חתימת הסכם עיבוד מידע):	רמת אבטחה בסיסית - 4,000 ש"ח	רמת אבטחה בסיסית - 4,000 ש"ח
רמת אבטחה בסיסית - 4,000 ש"ח	רמת אבטחה בינונית - 80,000 ש"ח	רמת אבטחה בינונית - 80,000 ש"ח
רמת אבטחה גבוהה - 320,000 ש"ח (ואם במאגר יש מידע על יותר ממיליון אנשים - 640,000 ש"ח).	רמת אבטחה גבוהה - 320,000 ש"ח (ואם במאגר יש מידע על יותר ממיליון אנשים - 640,000 ש"ח).	רמת אבטחה גבוהה - 320,000 ש"ח (ואם במאגר יש מידע על יותר ממיליון אנשים - 640,000 ש"ח).

תקנות העברת מידע מהאזור הכלכלי האירופי - עיצומים כספיים



לגבי תקנות העברת מידע מהאזור הכלכלי האירופי - חלק מהוראות התקנות אינן מאפשרות הטלת עיצום ישיר, וניתן יהיה להטיל עיצום כספי רק לאחר אי ציות להוראת הפסקת הפרה שנתקבלה מהרשות. חלק מההפרות הן בסכום קבוע בגין כל הפרה, וחלקן יוטל במכפלה של מספר נושאי המידע (כדוגמת מודל העיצומים הכספיים בגין הפרת הוראות החוק עצמו).

עיצומים על הפרת הוראות תקנות העברת מידע מהאזור הכלכלי האירופי

הפרה	סכום העיצום (צמוד למדד אחת לשנה)
הפרת הוראות תקנות העברת מידע מהאזור הכלכלי האירופי (תוספת רביעית)	<p>15,000 ש"ח על אי הודעה בכתב על הח" לטה בבקשה למחיקת מידע לבקשת נושא מידע</p>
	<p>2 ש"ח לכל אדם במאגר (מידע רגיל) או 4 ש"ח לכל אדם במאגר (מידע בעל רגישות מיוחדת) על הפרות פרטניות (לא פחות מ-20,000 ש"ח למידע רגיל ו-40,000 ש"ח למידע בעל רגישות מיוחדת): אי הפעלת מנגנון לצמצום מידע עודף או לבדיקה כי המידע שלם, נכון, ברור ומעודכן; אי תיקון מידע או מחיקתו.</p>
	<p>4 ש"ח לכל אדם שפנה (מידע רגיל) או 8 ש"ח לכל אדם שפנה (מידע בעל רגישות מיוחדת) (לא פחות מ-200,000 ש"ח): אי ציות להוראה להפסקת הפרה של ראש הרשות לגבי כל ההפרות שלהלן: בקשה למחיקה שלא בוצעה, אי מחיקת מידע עודף, אי מתן הודעה על קבלת מידע, אי מתן הודעה על העברת מידע לצד שלישי.</p>

האם קיימת אפשרות להפחית את סכום העיצום?

לפי התוספת החמישית לחוק, בסמכותה של הרשות להפחית את סכום העיצום הכספי בנסיבות הבאות וב־שיעורים המפורטים בטבלה מטה. אם התקיימו כמה נסיבות, ניתן להפחית את הסכום בשיעורים המנויים לצד אותן נסיבות במצטבר, ובלבד ששיעור ההפחתה לא יעלה על 70% מסכום העיצום.

הפחתת העיצומים

שיעור הפחחה	הנסיבות להפחחה
10%	לא הוטל עיצום כספי, התראה מנהלית או התחייבות להימנע מהפרה בשלוש השנים הקודמות
20%	לא הוטל עיצום כספי, התראה מנהלית או התחייבות להימנע מהפרה בחמש השנים הקודמות
30%	ההפרה הופסקה ביוזמת המפר, אשר דיווח עליה לרשות
20%	נקיטת פעולות למניעת הישנות ההפרה ולהקטנת הנזק
10%	מינוי DPO עד למסירת ההודעה על כוונת החיוב (הודעה בדבר הכוונה להטיל עיצום), אם המפר חב בחובת מינוי (ההפחחה לא חלה על גופים ציבוריים וסוחרי מידע)
30%	הפחחה בשל תשלום או פיצוי ששולם (במסגרת הליך אזרחי למשל)
20%	הפחחה בשל נסיבות אישיות
עד 70%	שיעור הפחחה מצטבר

הפחחה לעסק זעיר או קטן

עסק זעיר הוא עסק שמחזור העסקאות שלו בשנה שקדמה למועד ההפרה לא עלה על 4 מיליון ש"ח. עסק קטן הוא עסק שמחזור העסקאות שלו הוא בין 4 מיליון ש"ח ל-10 מיליון ש"ח. עסק זעיר או קטן זכאי להפחחת העיצום הכספי כך שלא יעלה על סכומים מסוימים.

עסק קטן	עסק זעיר	
<p>40,000 ש"ח</p> <p>לדוגמה: עסק קטן שלא הודיע על מאגר מידע החייב בהודעה לרשות להגנת הפרטיות (סעיף 8א(ב)) והוטל עליו עיצום בסכום של 150,000 ש"ח יוכל לבקש להפחית את הסכום ל- 40,000 ש"ח</p>	<p>20,000 ש"ח</p> <p>לדוגמה: עסק זעיר שסירב לתת לשני פונים זכות עיון במידע האישי (סעיף 13) והוטל עליו עיצום בסכום של 30,000 ש"ח יוכל לבקש להפחית את הסכום ל- 20,000 ש"ח</p>	<p>קטגוריה ראשונה של הפרות שמנויות בסעיף 6(1) לתוספת החמישית (הוראות החוק, תקנות אבטחת מידע ותקנות העברת מידע מהאזור הכלכלי האירופי)</p>

עסק קטן	עסק זעיר	
<p>100,000 ש"ח</p> <p>לדוגמה: עסק קטן שחלה עליו רמת האבטחה הבינונית והפר כמה הוראות לפי תקנות אבטחת מידע (כגון הכנת מסמך הגדרות מאגר, בדיקת מידע עודף, והכנת נוהל אבטחה), והוטל עליו עיצום בסכום של 120,000 ש"ח, יוכל לבקש להפחית את הסכום ל- 100,000 ש"ח</p>	<p>50,000 ש"ח</p> <p>לדוגמה: עסק זעיר שפנה לקבוצת אנשים לקבלת מידע אישי ולא מילא אחר דרישות סעיף 11, והוטל עליו עיצום בסכום של 100,000 ש"ח, יוכל לבקש להפחית את הסכום ל- 50,000 ש"ח</p>	<p>קטגוריה שנייה של הפרות שמנויות בסעיף 6(2) לתוספת החמישית (הוראות החוק, תקנות אבטחת מידע ותקנות העברת מידע מהאזור הכלכלי האירופי)</p>
<p>140,000 ש"ח</p>	<p>70,000 ש"ח</p>	<p>אי מסירת מסמך או עותק מחומר מחשב למפקח (כחלק מסמכות הפיקוח והבירור המינהלי)</p>

* אם מדובר בכמה הפרות, לא יעלו העיצומים על הגבוה מבין הסכומים בטבלה.

הפחתה לכל העוסקים בשל התחשבות במחזור עסקאות

אם סכום העיצום הכספי הסופי (בין אם הופחת הסכום בשל הנסיבות מעלה ובין אם לאו) עולה על 5% ממחזור העסקאות של המפר, הרשות תפחית את סכום העיצום ל-5% ממחזור העסקאות.

מפר המבקש הפחתה מכל סוג נדרש להגיש לרשות אישור לעניין גובה מחזור העסקאות שלו בתוך 30 ימים ממועד מסירת ההודעה על כוונת החיוב בעיצום כספי.

ערעור על החלטת הרשות בעניין עיצום כספי

ניתן לערער בזכות לבית משפט השלום, בתוך 45 ימים, על החלטות הרשות בעניין הטלת עיצום כספי, התראה מינהלית והתחייבות להימנע מהפרה. ואולם אין בהגשת הערעור כדי לעכב את ביצוע ההחלטה (אלא אם הרשות הסכימה לכך או שבית המשפט הורה על כך).

התראה מינהלית והתחייבות להימנע מהפרה

חשוב לציין כי הרשות יכולה, חלף הטלת עיצומים: (1) למסור התראה מינהלית שבה תודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהיה צפוי לעיצום כספי; או (2) להורות למפר להגיש לרשות כתב התחייבות לפיו המפר יתחייב להפסיק את ההפרה, להימנע מהפרה נוספת, ולהפקיד עירבון בגובה העיצום הכספי שהיה ניתן להטיל, אשר ניתן יהיה לחלט אם לא יעמוד בתנאים.

אם המפר המשיך לבצע את ההפרה לאחר שנמסרה התראה מינהלית או שהוגש כתב התחייבות, המשך ההפרה ייחשב "הפרה נמשכת". במצב זה יתווסף על סכום העיצום הכספי החלק המאה שלו לכל יום שבו נמשכה ההפרה. התיקון לחוק מגדיר גם מהי הפרה חוזרת. זוהי הפרה שבוצעה בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על המפר עיצום. במקרה זה יתווסף על העיצום הכספי סכום השווה לעיצום הכספי שהוטל.

בהמשך צפויים להתפרסם נהלים ותקנות בעניין הסמכות להטיל עיצום כספי. כך, למשל, יפורסמו תקנות הקובעות מהן הוראות החוק שהפרתן תוביל למסירת התראה מינהלית חלף הטלת עיצום כספי.

חלק ו' - סמכויות אכיפה (חקירות פליליות)

התיקון מביא עימו חידוש גם בתחום סמכויות האכיפה הפליליות של הרשות. עד עתה, סמכות החקירות הפליליות של הרשות ניתנו בהסמכה פרטנית של השר לביטחון לאומי. במסגרת התיקון, עוגנו סמכויות האכיפה הפליליות של הרשות בחוק: סמכות חקירה כאשר מתעורר יסוד סביר לחשד שנעברה עבירה לגבי ידיעה על ענייניו הפרטיים של אדם במאגר מידע או עבירה לפי פרק ב' לחוק (מאגרי מידע). כמו כן, עוגנה סמכות תפיסת חפץ הקשור לעבירה כאמור או סמכות לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב בהתאם לפקודת סדר הדין הפלילי (מעצר וחיפוש).

בנוסף, נקבעו מספר עבירות חדשות תוך החלפת פרק העבירות הקיים בחוק: הפרעה לחוקר או מפקח במילוי תפקידו; הטעיית מפקח; עיבוד מידע ממאגר מידע בלא הרשאה; מסירת פרטים לא נכונים בפנייה לקבלת מידע בכוונה להטעות (בניגוד להוראות סעיף 11) ומסירת מידע מגוף ציבורי שלא כדין.

חלק ז' - הוראות מהותיות הנוגעות לניהול מאגר מידע ועיבוד חוקי של מידע

בתיקון נכללו מספר הוראות מהותיות חדשות:



- **תיקון סעיף צמידות המטרה.** סעיף 8(ב) הקובע את עיקרון צמידות המטרה תוקן לאור צמצום חובת רישום המאגרים: "לא יעבד אדם מידע אישי במאגר מידע אלא למטרת מאגר שנקבעה לו כדין". המשמעות היא שלאחר התיקון, לא יהיה קשר לשאלה אם המאגר נרשם או איזו מטרה נקבעה כאשר נרשם ויש לבחון מהי המטרה שנקבעה כדין לעיבוד מידע במאגר.
לכן, מומלץ להקפיד לדייק במטרות השימוש בכל מסמך רלבנטי, כדוגמת מדיניות פרטיות, מסמכי הגדרות מאגר וכיוצ"ב.
- **קביעת הוראה נורמטיבית בדבר איסור עיבוד מידע אישי ממאגר מידע ללא הרשאה של בעל השליטה במאגר המידע או בחריגה מהרשאה.**
תיקון זה חשוב במיוחד למחזיקים במאגרי מידע שכן עליהם לוודא שמטרות העיבוד שמתיר להם בעל השליטה במאגר מוגדרות היטב, כוללות את הנדרש להם לטובת ביצוע השירותים וכי אין שימושים נוספים שלא הותרו להם.
- **קביעת הוראה נורמטיבית בדבר איסור עיבוד מידע אישי ואיסור מתן הרשאה לאחר לעבד את המידע אם המידע נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק הגנת הפרטיות או להוראות כל דין אחר המסדיר עיבוד מידע.** חריג להוראה זו הוא במצב שבעל השליטה קיבל מידע מגורם אחר ובעל השליטה לא ידע או לא היה עליו לדעת שהגורם שמסר לו את המידע פעל שלא כדין. נציין, כי הסעיף לא יחול על הפרת דין קלת ערך בנסיבות העניין, גם אם בעל השליטה ידע או שהיה עליו לדעת כאמור.

הוראות מהותיות נוספות צפויות להכלל בתיקון הבא של החוק.



חלק ח' - הרחבת חובת היידוע

הרחבת חובת היידוע של מבקש מידע - סעיף 11

סעיף 11 לחוק קובע את היקף חובת היידוע בעת איסוף מידע אישי מנושאי מידע. הסעיף תוקן במסגרת תיקון החוק והתווספו נושאים שיש לפרט במסגרת חובת היידוע. התיקון מחייב בראש ובראשונה את עדכון מסמכי מדיניות הפרטיות של הארגון ביחס לאיסוף מידע מלקוחות, עובדים וכו'. עם כניסתו של תיקון 13 לתוקף, פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע צריכה להכיל את כל הפרטים הבאים:

1. האם חלה על האדם חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו ובה־סכמתו. מעתה, יש לפרט גם את תוצאת אי-ההסכמה של אדם למסור מידע;
 2. המטרה אשר לשמה מבוקש המידע;
 3. מעתה, יש לפרט גם את שמו של בעל השליטה במאגר המידע ודרכי התקשרות עימו;
 4. למי יימסר המידע ומטרות המסירה;
 5. מעתה, יש לפרט את קיומן של זכות העיון במידע האישי ושל הזכות לבקש תיקון של המידע האישי (סעיפים 13 ו-14 לחוק);
 6. בנוסף, ככל שעל הארגון חלה חובה למנות ממונה הגנת פרטיות, מאחר והתיקון קובע שיש לפרסם את פרטי הקשר עימו, מומלץ לכלול תוספת זו גם במסגרת מדיניות הפרטיות המעודכנת.
- נציין כי יש לבחון מסמכי מדיניות פרטיות קיימים ובמידת הצורך לעדכן אותם גם בשים לב לשאר הוראות התיקון, לדוגמה, הרחבת ההגדרה של מידע אישי והוספת הגדרה רחבה של המונח עיבוד.

חלק ט' - פיצויים לדוגמה

פיצויים לדוגמה

התיקון לחוק מרחיב את האפשרות לתבוע פיצוי ללא הוכחת נזק. סעיף 29א לחוק בנוסחו הקיים מאפשר (גם לאחר כניסתו לתוקף של תיקון 13) לבית המשפט לחייב אדם שהורשע בעבירה של פגיעה בפרטיות במזיד לפי פרק א' לחוק או נתבע במשפט אזרחי בגין פגיעה בפרטיות, לשלם לנפגע פיצוי ללא הוכחת נזק בסכום שלא יעלה על 50,000 ש"ח.

סעיף 15א החדש לחוק מרחיב את האפשרות לתבוע פיצוי ללא הוכחת נזק גם להפרות של הוראות הנוגעות לזכות לפרטיות במאגרי מידע (פרקים ב' ו-ד' לחוק). הסעיף קובע כי אם בעל שליטה או מחזיק הפרו הוראות מסוימות, בית המשפט רשאי לפסוק פיצויים שאינם תלויים בנזק (פיצויים לדוגמה), בסכום שלא יעלה על 10,000 ש"ח.

לדוגמה: בעל שליטה שעובד מידע אישי במאגר החייב ברישום, ולא רשם אותו (סעיף 8א). הדבר מותנה בפנייה מוקדמת לבעל השליטה בדרישה לרשום את המאגר, ורק בחלוף 90 ימים מיום פנייתו; פנייה לקבלת מידע לשם עיבודו במאגר מידע בלי שנמסרה הודעה כדרישת סעיף 11. גם כאן, הדבר מותנה בפנייה מוקדמת לבעל השליטה ובחלוף 30 ימים מהפנייה; בעל שליטה שלא אפשר לאדם לעיין במידע שעליו, בניגוד להוראות סעיפים 13 או 13א.

הסעיף מפרט את השיקולים שעל בית המשפט לשקול בבואו לפסוק את סכום הפיצוי, כמו היקף ההפרה וחומרתה והתנהגות המפר. עוד נקבע, כי אדם לא יוכל לקבל פיצוי לדוגמה יותר מפעם אחת, בשל אותו מעשה או מחדל.

חלק י' - חוות דעת מקדמית

חוות דעת מקדמית

התווסף לחוק במסגרת התיקון מנגנון מתן חוות דעת מקדמית על ידי הרשות. גם כיום ניתן להגיש לרשות בקשה לחוות דעת מקדמית, בהתאם לנוהל המפורסם באתר הרשות, אך הרשות לא חייבת לספק חוות דעת כאמור. החידוש בתיקון 13 הוא קביעת חובה לרשות לתת את חוות הדעת, אלא אם כן התקיימו חריגים מסוימים.

בעל שליטה או מחזיק, או מי שעומד להיות אחד מאלה, יוכלו לבקש מהרשות חוות דעת מקדמית בעניין עמידת מאגר המידע בדרישות הוראות החוק, לעניין עיבוד מידע במאגר מידע. חוות הדעת תינתן תוך 60 ימים ממועד קבלת הבקשה או ממועד המצאת המסמכים הנוגעים בדבר, לפי המאוחר. אם הרשות החליטה שלא לתת חוות דעת מקדמית, עליה להודיע על כך למבקש בתוך 45 ימים. הרשות תפרסם נוהל באתר האינטרנט שלה לגבי נסיבות שבהן לא תינתן חוות דעת לגבי בקשות מסוגים מסוימים כמו בקשה שעניינה תיאורטי או אקדמי, בקשה הנגועה בחוסר ניקיון כפיים וכו'. הרשות רשאית לפרסם את חוות הדעת בהסכמת המבקש. אם לא הסכים לכך, באפשרותה לפרסמה ללא פרטים מזהים.

חשיבות מנגנון חוות הדעת המקדמית הינה במיוחד כשמדובר בתיקון חדש לחוק, שאין לגביו עדיין הנחיות או תקדימים ליישום, והמנגנון נועד לתת לבעלי שליטה ומחזיקים וודאות ביחס לאופן שבו הם מיישמים את החוק.

חלק יא' - תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)

בחודש ספטמבר 2024, פורסמה הנחיית הרשות להגנת הפרטיות, לאחר הליך של שימוע ציבור, בעניין תפקיד הדירקטוריון בפיקוח על מילוי חובות התאגיד בהתאם לתקנות הגנת הפרטיות (אבטחת מידע). ההנחיה חלה על כל החברות אשר עיבוד מידע אישי הוא בליבת הפעילות שלהן (להבדיל מעיבוד מידע שרק נלווה לפעילות הליבה), או שקיימת סבירות שפעילותן תיצור סיכון מוגבר לפרטיות. הקביעה אם ההנחיה חלה על החברה תעשה לאור מאפייני הארגון (כדוגמת חברות העוסקות בסחר במידע), סוגי המידע המעובד ורגישותו (ראו הגדרת "מידע בעל רגישות מיוחדת", שהורחבה בצורה ניכרת בתיקון מס' 13 לחוק), מידע על אוכלוסיות ייחודיות, דוגמת קטינים, או היקף נושאי המידע ומורשי הגישה.

לפי ההנחיה, על דירקטוריון החברה מוטלת חובה לפקח על ציות החברה לחוק הגנת הפרטיות ולתקנות הגנת הפרטיות (אבטחת מידע). בנוסף לחובת הפיקוח והבקרה הכללית, דירקטוריון החברה (בין אם היא בעלת המאגר או המחזיקה בו), נדרש לקיים את כל אלה:

- יש לוודא כי קיימת מדיניות פרטיות פנימית בארגון בדבר אופן הציות לחוק הגנת הפרטיות והתקנות, לרבות חובת הדיווח המיידית לרשות להגנת הפרטיות על קרות אירוע אבטחת מידע וקביעת בעלי התפקידים האחראים על מימוש המדיניות. המדיניות צריכה להתייחס לאופן השימוש במידע אישי בחברה וניהולו בנושאים מהותיים, וכן להגדיר תהליכי פיקוח, בקרה, וציות אפקטיביים.
- בהתייחס לחובות המוטלות על בעלי מאגרים ומחזיקים מכוח תקנות אבטחת מידע, הדירקטוריון נדרש לקיים דיון במסמך הגדרות המאגר שהחברה מחויבת לערוך לפי התקנות, טרם אישורו הסופי; לקיים דיון בעקרונות המרכזיים של נוהל אבטחת המידע הארגוני שעל החברה לערוך לפי התקנות, בטרם אישורו; לקיים דיון בתוצאות סקר הסיכונים, מבדקי החדירות והביקורת התקופתית שהחברה מחויבת לערוך בהתאם לרמת האבטחה של מאגריה, ובעקבות בחינת אירועי האבטחה שאירעו בחברה.
- הדירקטוריון נדרש לקבל דיווחים שוטפים על הציות לתקנות אבטחת המידע מהגורמים האחראים בחברה, כגון ממונה אבטחת המידע וממונה הגנת הפרטיות.

האם ניתן לאצול את חובות וסמכויות הדירקטוריון בהקשר זה לגורם אחר? על פי ההנחיה, במקרים המתאימים, ובשים לב למידת הסיכון לפרטיות הכרוך בפעילותה של החברה, לגודלה ולהרכב הדירקטוריון, ניתן לקבוע בהחלטת דירקטוריון גורם אחר בחברה שיהיה אחראי על ביצוע פעולות אלה, תוך פיקוח על קיומן בפועל על ידי הדירקטוריון. החלטה כאמור יש לתעד ולנמק בנסיבות הקשורות לארגון הספציפי שבו מדובר.

אלו צעדי אכיפה עשויים להיות רלוונטיים בקשר עם חובות הדירקטוריון הנ"ל? הרשות מציינת כי חברה שהדירקטוריון בה אינו מקיים את חובת הפיקוח המתוארת, או שאינו מעורב במידה נאותה בביצוע הפעולות הקונקרטיות המפורטות בהנחיה, מפרה לכאורה את הוראות חוק הגנת הפרטיות ותקנות אבטחת המידע, ועלולה להיות חשופה לסנקציות הקבועות בחוק. לרבות אלו שנקבעו בתיקון 13 לחוק הגנת הפרטיות, לאחר כניסתו לתוקף. נדגיש כי הדירקטוריון עצמו לא חשוף לאחריות ישירה ולהטלת עיצום כספי (עם כניסתו לתוקף של תיקון 13) מכוח ההנחיה, אך חברי הדירקטוריון עשויים לחוב באופן אישי בהתבסס על דיני התאגידים ודיני ניירות ערך הכלליים. הרשות להגנת הפרטיות הודיעה כי תפעל לאכוף את ההנחיה בחודשים הקרובים ועוד בטרם כניסתו של תיקון 13 לחוק לתוקף באוגוסט 2025.

מה כדאי לעשות בפועל? אנו ממליצים לקבוע מדיניות הגנת פרטיות ארגונית, אשר תכלול את עקרונות העל של הציות לדיני הגנת הפרטיות בארגון, ותקבע בעלי תפקידים וגורמים אחראים ליישום וביצוע, בהתאם לכללי הממשל התאגידי המקובלים. אם הדירקטוריון מעדיף להאציל סמכויות, ומתקיימות נסיבות המצדיקות זאת, מומלץ למנות בעל(י) תפקיד(ים) בארגון שתינתן להם הסמכות לקיים את הוראות ההנחיה. בעל התפקיד יציג לדירקטוריון, לכל הפחות פעם בשנה (ולגבי אירועי אבטחת מידע בתדירות גבוהה יותר), בצורה מרוכזת, את אופן עמידת החברה בהוראות החוק ותקנות אבטחת מידע, והדירקטוריון יקיים על כך דיון, בכובעו הפיקוחי. יש לקבוע גם גורמים מפקחים בדרג נמוך מהדירקטוריון, כדוגמת ועדת היגוי או תת ועדה של ההנהלה, ולשמר לדירקטוריון סמכות פיקוחית על אותה ועדה, והכל בהתאם לגודל ומורכבות הארגון.



מידע עלינו:

מחלקת IT, הגנת הפרטיות וסייבר של משרד נשיץ ברנדס אמיר

מתמחה בייעוץ שוטף ללקוחות רבים במשק הישראלי, בנושאי סייבר, פרטיות, ניהול מאגרי מידע, ענן ואבטחת מידע. המחלקה מספקת גם שירותי DPO.

המחלקה מייעצת ללקוחות ביחס לדין הישראלי וגם ביחס ל-GDPR, החוק החדש בקליפורניה (CCPA) ודינים במדינות נוספות, ובכלל זה אימוץ ויישום תוכניות אכיפה רב-לאומיות של אבטחת מידע והגנת פרטיות.

צוות המחלקה מלווה לקוחות בטיפול באירועי סייבר, משתתף כיועץ בהפקת לקחים וניתוח ממצאים לאחר אירועי סייבר, ומלווה חברות בהליכי פיקוח וביקורת של רשות הגנת הפרטיות, וכן ייצג בהליכים משפטיים וליטיגציה.

ראש המחלקה, עו"ד דלית בן-ישראל, לקחה חלק פעיל בדיונים בועדת חוקה בכנסת בנושא תיקון 13 לחוק הגנת הפרטיות, התשמ"א-1981, ומייעצת לארגונים ביישום והיערכות לכניסתו לתוקף של התיקון לחוק ומרצה במרבית קורסי הכשרת ה-DPO בחסות הרשות להגנת הפרטיות.

עו"ד נעמה גורני לר שימשה טרם הצטרפותה לפירמה, עד לפני כחצי שנה, כעורכת דין ברשות להגנת הפרטיות, ובכובעה זה ליוותה מצד הרשות את הליכי החקיקה של תיקון 13.

מוזמנים לפנות אלינו בכל שאלה!

מייל: dbenisrael@nblaw.com; טלפון: 03-6236010

צוות המחלקה



עו"ד דלית בן-ישראל, שותפה
ראש מחלקת IT הגנת פרטיות וסייבר



אליס פיטוסקי, משפטנית



עו"ד רוני כלפון



עו"ד דניאל דהב



עו"ד נעמה גורני לר



עו"ד שריי אסולין