משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة القانون التكنولوجيا والمعلومات

מדריך | תיקון מס' 13
לחוק הגנת הפרטיות

מאי 2025

תוכן עניינים

הקדמה

ביום 5.8.2024 אישרה הכנסת את חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, המהווה את העדכון המקיף והמהותי ביותר לדיני הגנת הפרטיות בישראל, מאז נחקק חוק הגנת הפרטיות בשנת 1981. תיקון מס' 13, אשר עתיד להיכנס לתוקפו ב-14 לאוגוסט 2025, כולל שורה של הסדרים חדשים ומתקדמים.

התיקון המקיף לחוק הגנת הפרטיות מהווה אבן דרך חשובה בהתאמת החוק הישראלי למציאות הטכנולוגית של ימינו, ולאתגרי עידן הבינה המלאכותית, בהגברת ההגנה על הזכות לפרטיות ועל המידע האישי של תושבי ישראל, ובחיזוק כלי האכיפה של הרשות להגנת הפרטיות בגין הפרות החוק ותקנותיו, ובגין אי-עמידה בדרישות הדין בתחום אבטחת המידע, והוא הכרחי לשם התמודדות עם איומי הסייבר הגוברים. כמו כן, התיקון לחוק מהווה צעד חשוב גם בראי ההתאמה של ישראל לדיני הגנת הפרטיות באיחוד האירופי וההכרה במדינת ישראל כמדינה בעלת מעמד תאימות (Adequacy), שאושררה לאחרונה על ידי האיחוד האירופי בינואר 2024.

במדריך זה נסקור את עיקרי ההסדרים הקבועים בתיקון מס' 13:

- עיגון בחוק של מעמד הרשות להגנת הפרטיות, ושל החלטת הממשלה בדבר עצמאות הרשות ותפקידיה.
- עדכון כלל ההגדרות המהותיות בחוק והתאמתן להתפתחויות הטכנולוגיות, החברתיות והמשקיות ולהסדרים הקיימים בחקיקה מודרנית של הגנת הפרטיות במדינות מובילות.
- קביעת חובת מינוי ממונה על הגנת הפרטיות (DPO) בכלל הגופים הציבוריים ובשורה ארוכה של חברות וארגונים במגזר הפרטי.
- צמצום משמעותי של חובת רישום מאגרי מידע דיגיטליים והחלפתה בחובת הודעה לרשות על מאגרים גדולים ורגישים.
- קביעת איסור גורף על עיבוד מידע אישי שנאסף באופן לא חוקי ואיסור על עיבוד מידע ללא הרשאה מאת בעל השליטה במאגר.
- קביעת סנקציות של עיצומים כספיים בסכומים משמעותיים (עד מיליוני ש"ח בגין כל הפרה) בשל הפרת הוראות החוק, התקנות בתחום אבטחת המידע והתקנות הנוגעות למאגרים בהם קיים מידע אישי שהועבר לישראל מהאיחוד האירופי.
- קביעת עבירות פליליות חדשות במאגרי מידע.
- עיגון סמכותה של הרשות להגנת הפרטיות לפנות לבית המשפט לקבלת צו להפסקת עיבוד מידע אישי במאגר, לרבות מחיקת מידע.
- עיגון בחוק של סמכויות האכיפה הפלילית של הרשות (ניתנו קודם לכן בהסמכה של השר לביטחון לאומי).
- הרחבת סמכות בתי המשפט לפסוק פיצויים ללא הוכחת נזק בגין הפרת החובות הקבועות בחוק.
- ביטול ההתיישנות המקוצרת בתביעות אזרחיות בגין פגיעה בפרטיות והפרות של החוק.
- הסדר בדבר מתן חוות דעת מקדמית מטעם הרשות בנוגע לעמידת מאגר המידע בדרישות החוק.
- קביעת הסדר פיקוח מיוחד בתחום הפרטיות בגופים ביטחוניים.

עיגון מעמדה של הרשות להגנת הפרטיות ותפקידיה בחוק

הרשות להגנת הפרטיות היא הרגולטור לפי חוק הגנת הפרטיות, ובעלת סמכויות הפיקוח והאכיפה של הוראות חוק זה.

החוק מעגן את מעמדה העצמאי של הרשות להגנת הפרטיות במשרד המשפטים, ואת תפקידיה כפי שנקבעו בהחלטת הממשלה מס' 1890 מיום 2.10.2022, אשר נוסחה המלא עוגן בתוספת הראשונה לחוק.

בסעיף 1(ב) בתוספת הראשונה לחוק נקבע כי "הרשות תהיה עצמאית בהפעלת הסמכויות המוקנות לראש הרשות לשם מילוי תפקידיה באמצעות עובדי הרשות ובהתאם להוראות כל דין, ותקציב הפעילות של הרשות ינוהל בנפרד בתוך תקציב משרד המשפטים. מתוך כיבוד עצמאותה של הרשות, תפעל הרשות באופן בלתי תלוי בעת הפעלת הסמכויות המוקנות לראש הרשות".

בין יתר תפקידיה של הרשות, אלו תפקידי הרשות המנויים בסעיף 2 בתוספת הראשונה:

- לפקח על מילוי הוראות חוק הגנת הפרטיות והתקנות שלפיו ביחס למאגרי מידע.
- לחקור חשדות לביצוע עבירות לפי חוק הגנת הפרטיות ביחס למאגרי מידע, בהתאם לסמכויותיה על פי דין.
- להעלות את המודעות בציבור לזכות לפרטיות במאגרי מידע, לערך ההגנה על הפרטיות ולחשיבותו בעידן המידע, באמצעות חינוך, הדרכה והסברה.
- לטפל בפניות ציבור שיש בהן ממש בעניין פגיעה בנושאי מידע לפי החוק.
- לפתח וליישם תוכניות מקצועיות והכשרות בתחומי פעילותה.
- לקדם ולקיים קשרים עם גופים מקבילים בעולם ובמסגרת פורומים בין-לאומיים שבהם משתתפים גופים מקבילים.
- לבצע את סמכויות רשם הגורמים המאשרים לפי חוק חתימה אלקטרונית, התשס"א-2001.

תחולה

חוק הגנת הפרטיות חל על כל מי שאוסף, משתמש או מעבד מידע אישי, ובכלל זה על גופים ציבוריים ופרטיים כאחד. הוראות החוק הנוגעות למאגרי מידע אינן חלות על אוסף פרטי מידע אישי שאינו למטרות עסק או למטרות ציבוריות.

עדכון כלל ההגדרות המהותיות של החוק

בתיקון מס' 13 עודכנו כלל ההגדרות המהותיות של החוק, והועברו רובן ככולן לסעיף 3 בחוק.
בכלל זה, עודכנה הגדרת "מידע אישי", "מידע בעל רגישות מיוחדת", "בעל שליטה במאגר מידע", "עיבוד ושימוש", "מחזיק", "מאגר מידע", "מנהל מאגר", "הרשות להגנת הפרטיות" ו"מזהה ביומטרי".

- ההגדרה של "**מידע**", שהופיעה עד כה בסעיף 7 לחוק, הוחלפה בהגדרה חדשה של "**מידע אישי**".
במקום ההגדרה הקודמת, שהתמקדה ב"נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו", ההגדרה החדשה מגדירה "**מידע אישי**" באופן רחב כ"**כל נתון 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 זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי". המשמעות היא שכל מידע הנוגע במישרין או בעקיפין לאדם מזוהה או אדם הניתן לזיהוי, אשר מוחזק או מעובד במאגר מידע, כפוף להוראות חוק הגנת הפרטיות, לתקנותיו ולחובות הקבועות בהן.

- הגדרת "**מידע בעל רגישות מיוחדת**" מחליפה את ההגדרה הקודמת "מידע רגיש", וכוללת רשימה של סוגי מידע אישי המפורטים בחוק:

  - ☐ מידע על צנעת חיי המשפחה של אדם, צנעת אישותו, ונטייתו המינית.
  - ☐ מידע המתייחס למצב בריאותו של אדם, כולל מידע רפואי לפי חוק זכויות החולה.
  - ☐ מידע גנטי כהגדרתו בחוק מידע גנטי.
  - ☐ מזהה ביומטרי המשמש או מיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב.
  - ☐ מידע על מוצאו של אדם.
  - ☐ מידע על עברו הפלילי של אדם.
  - ☐ מידע על דעותיו הפוליטיות של אדם, על אמונותיו הדתיות או השקפת עולמו.
  - ☐ הערכת אישיות שנערכה מטעם גורם מקצועי או באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים.
  - ☐ מידע על נתוני שכר של אדם ועל פעילותו הפיננסית.
  - ☐ נתוני מיקום ונתוני תעבורה, כהגדרתם בחוק נתוני תקשורת, שנוצרו על ידי ספק מורשה לפי חוק נתוני תקשורת.
  - ☐ נתונים על מיקומו של אדם המלמדים על כל אחת מהקטגוריות האחרות (למעט על הערכת אישיות, נתוני שכר ופעילות פיננסית).
  - ☐ מידע שחלה עליו חובת סודיות שנקבעה בדין.
  - ☐ מידע אישי אחר שקבע שר המשפטים, באישור ועדת החוקה, והוא נכלל בתוספת השנייה לחוק.

- הגדרת "**מאגר מידע**" השתנתה גם היא ומוגדרת כעת "**אוסף פרטי מידע אישי המעובד באמצעי דיגיטלי**", למעט אוסף לשימוש אישי שאינו למטרות עסק (או מטרות ציבוריות) ולמעט אוסף הכולל רק שם, מען ודרכי התקשרות, לגבי 100,000 בני אדם או פחות, שאינו מלמד כשלעצמו על מידע אישי נוסף לגבי מי שכלול בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף אחר הכולל פרטי מידע אחרים לגבי אותם בני אדם.

- תוספת משמעותית בפרק ההגדרות היא המונח "**בעל שליטה במאגר מידע**", שהוגדר לראשונה בחוק במקום המונח "בעל מאגר מידע" בחוק הקיים, וחל על "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 המידע". הכוונה היא לארגון עצמו, בין אם מדובר בגוף ציבורי או פרטי, ולא לבעל תפקיד ספציפי בגוף.

- הגדרת "**מחזיק**" הורחבה ביחס להגדרה הקודמת, וכעת כל "**גורם חיצוני לבעל השליטה במאגר מידע המעבר מידע עבורו**", הוא בגדר "**מחזיק**" במאגר.

- להגדרת המונח "שימוש" התווסף המונח "עיבוד", וההגדרה הורחבה ועודכנה לנוסח הבא: "עיבוד", "שימוש" - "כל פעולה שמבוצעת על מידע אישי, לרבות, קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו". הגדרה רחבה זו מבהירה כי כל פעולה אשר מבוצעת במידע אישי מהווה שימוש ועיבוד לעניין חוק הגנת הפרטיות וכלל המגבלות הרלוונטיות בחוק חלות ביחס אליה.

- שינוי הגדרות נוסף נעשה ביחס למונח "**מנהל מאגר**", אשר הוגדר בעבר כ"מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה". התיקון לחוק קובע כי מנהל המאגר הוא "בעל שליטה במאגר מידע, ולעניין גוף ציבורי, כהגדרתו בסעיף 23 – המנהל הכללי של ארגון שבבעלותו או בהחזקתו מאגר מידע או מי שהמנהל הכללי הסמיכו למנהל את המאגר". לפיכך, החובה למנות מנהל מאגר בגופים פרטיים **תתבטל** עם כניסתו לתוקף של תיקון 13, ובמקביל בוטלה גם האחריות האישית של מנהל מאגר ביחס לאבטחת המידע במאגר, לפי סעיף 17 לחוק. החובות שהיו מוטלות בחוק על מנהל המאגר יחולו על בעל השליטה במאגר המידע (כלומר, הארגון עצמו).

צמצום חובת רישום מאגרי מידע והוספת חובת הודעה לרשות

צמצום חובת רישום מאגרי מידע

במסגרת התיקון צומצמה משמעותית חובת הרישום שחלה עד היום כמעט על כל מאגרי המידע במשק. למעשה, חובת רישום מאגרי מידע ביחס לגופים במגזר הפרטי בוטלה כמעט לחלוטין, מתוך מטרה להקטין את הנטל הרגולטורי שהוטל על גופים במגזר זה.

חובת רישום מאגרי מידע תישאר על כנה ביחס למאגרי הגופים הבאים:

- מאגר מידע של גוף ציבורי, למעט מאגר הכולל מידע על עובדי הגוף הציבורי בלבד.
- מאגר שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, ויש במאגר מידע על 10,000 בני אדם ומעלה.

יצוין כי מאגר מידע שאינו חב ברישום בהתאם להסדר החקיקתי החדש, ימשיך להיות רשום במרשם מאגרי המידע, אלא אם בעל השליטה במאגר פנה לרשות להגנת הפרטיות בבקשה למחוק אותו מהמרשם.

שימו לב! העובדה שמאגר מידע לא יהיה חייב ברישום לאחר כניסתו לתוקף של תיקון 13, אינה פוטרת את המאגר או את בעל השליטה בו מקיום כל חובה אחרת לפי חוק הגנת הפרטיות, וכלל המגבלות והחובות הקבועות בחוק ובתקנותיו ימשיכו לחול על המאגר באופן מלא, אף אם אינו חייב ברישום.

חובת הודעה לרשות להגנת הפרטיות על מאגרי מידע גדולים בהם מידע בעל רגישות מיוחדת

ביחס למאגרי מידע שיש בהם **מידע בעל רגישות מיוחדת על יותר מ-100,000 איש** אולם אינם חייבים ברישום, נקבעה חובה חדשה בדין של מסירת הודעה לרשות בתוך 30 יום על מאגר המידע.

מה צריכה לכלול הודעה לרשות על מאגר מידע לפי סעיף 8א(ב) לחוק?

- פרטי בעל השליטה במאגר ודרכי ההתקשרות עימו.
- פרטי הממונה על הגנת הפרטיות ודרכי ההתקשרות עימו (אם קיימת חובה למנותו).
- העתק של מסמך הגדרות מאגר הנדרש לפי תקנה 2 לתקנות אבטחת מידע, התשע"ז-2017 (להלן: "תקנות אבטחת מידע").

מינוי ממונה על הגנת הפרטיות

חובת מינוי ממונה על הגנת הפרטיות

התיקון קובע חובת מינוי ממונה על הגנת הפרטיות (Data Protection Officer- DPO), בכל גוף ציבורי ובשורה ארוכה של ארגונים במשק, שפעולתם כרוכה בסיכון גבוה לפרטיות. תפקידו של הממונה הוא לפעול להבטחת קיום הוראות החוק ותקנותיו, ולקידום השמירה על הפרטיות ואבטחת המידע במאגרי מידע.

נציין כי הרשות פרסמה גילוי דעת ייעודי ומפורט בנושא מינוי ממונה על הגנת הפרטיות, המתייחס בהרחבה לסוגי הגופים המחויבים במינוי ממונה, מהות תפקידו ותחומי האחריות של הממונה, הידע והכישורים הנדרשים ממנו, ולהוראות נוספות בחוק המסדירות את מעמדו של הממונה בתוך הארגון ומתכונת העסקתו. להלן נתייחס בקצרה להוראות החוק עצמו בנוגע לממונה. להסבר נרחב יותר, יש לעיין בגילוי הדעת.

על מי מוטלת החובה למנות ממונה על הגנת הפרטיות?

- **בעל שליטה** שהוא גוף ציבורי או **מחזיק** במאגר של **גוף ציבורי**, לרבות משרדי ממשלה, רשויות מקומיות, גופים אחרים הממלאים תפקיד ציבורי לפי דין וכן גופים אחרים הכלולים בצו הגנת הפרטיות (קביעת גופים ציבוריים), תשמ"ו-1986, לרבות קופות חולים, בתי חולים, מוסדות להשכלה גבוהה, ארגוני עובדים ועוד, למעט גוף המוגדר כ"גוף בטחוני" לפי סעיף 23ב לחוק, לגביו קיים הסדר נפרד המחייב מינוי של מפקח פרטיות פנימי.
- בעל שליטה שמטרתו העיקרית היא **איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה**, לרבות שירותי דיוור ישיר, ויש במאגר מידע על יותר מ-10,000 איש. הכוונה היא לארגונים העוסקים בסחר במידע במובן הרחב של המונח, המגלמים סיכון גבוה יותר לפגיעה בפרטיות.
- בעל שליטה או מחזיק שעיסוקיו העיקריים כוללים או כרוכים בפעולות **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**, או מי שעיסוקו העיקרי כרוך בפעולות אלה, ובין היתר חברת סלולר ומנוע חיפוש מקוון.
- בעל שליטה או מחזיק במאגר מידע שעיסוקו העיקרי כולל **עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר**. החוק קובע במפורש כי בנקים, חברות ביטוח, בתי חולים וקופות חולים מחויבים במינוי ממונה לפי סעיף זה.

תפקידי הממונה על הגנת הפרטיות בארגון:

- ישמש סמכות מקצועית ומוקד ידע, וייעץ להנהלת הגוף בתחום הגנת הפרטיות.
- יכין תכנית הדרכה בתחום הגנת הפרטיות ויפקח על ביצועה.
- יכין תכנית לבקרה שוטפת על עמידה בהוראות החוק והתקנות, יוודא ביצועה, ידווח להנהלת הגוף על ממצאיו, ויציע הצעות לתיקון הליקויים.

- יוודא קיומם של נוהל אבטחת מידע ומסמך הגדרות מאגר כהגדרתם בתקנות אבטחת מידע, שיובאו לאישור הנהלת הגוף.
- יוודא טיפול בפניות של נושאי מידע לגבי עיבוד מידע אישי או מימוש זכויות לפי החוק ותקנותיו, ובכלל זה בקשות לעיון במידע ולתיקון מידע.
- ישמש איש קשר עם הרשות להגנת הפרטיות, ודרכי ההתקשרות עמו יפורסמו לציבור.

מי יכול לכהן כממונה על הגנת הפרטיות?

סעיף 17ב3(א) לחוק קובע כי הממונה על הגנת הפרטיות "**יהיה בעל הידע והכישורים הנדרשים למילוי תפקידו בצורה נאותה**". זו הדרישה המהותית והכללית שאת תוכנה והיקפה יש לקבוע בכל מקרה לגופו "בשים לב לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו". בלי לגרוע מהדרישה הכללית, בחוק מפרט תחומי ידע ספציפיים בהם חייב כל ממונה לשלוט -

- **ידע מעמיק בדיני הגנת הפרטיות** – על הממונה להיות בעל שליטה מלאה ומקיפה במכלול החקיקה והרגולציה הישראלית בתחום הגנת הפרטיות, הרלוונטית לעיבוד מידע אישי ולהגנה על הפרטיות בישראל.
- **הבנה הולמת בטכנולוגיה ואבטחת מידע** - הממונה על הגנת הפרטיות נדרש להפגין הבנה טכנולוגית ברמה שתאפשר לו לבצע באופן יעיל את תפקידו, לאור המאפיינים הספציפיים של הארגון בו הוא מכהן, תחום עיסוקו, פעולות עיבוד המידע שהארגון מבצע והטכנולוגיות המשמשות אותן.
- **היכרות עם תחומי פעילותו של הארגון ומטרותיו** - בשים לב לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו.

הוראות נוספות הנוגעות לממונה על הגנת הפרטיות

- החוק מתיר להעסיק את הממונה גם במתכונת של **נותן שירותים חיצוני (מיקור חוץ)**, אולם רצוי שהממונה יהיה עובד הארגון וחלק אינטגרלי מן הארגון.
- מתכונת ההעסקה והיקף המשרה של הממונה (פנימי או חיצוני) צריכים להיבחן לגופו של כל ארגון בהתאם למאפייניו הספציפיים, ובהתחשב באופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו.

☐ הממונה ידווח ישירות למנכ"ל, או לגורם הכפוף במישרין למנכ"ל.

☐ בעל השליטה או המחזיק יספקו לממונה את **התנאים והמשאבים הדרושים** למילוי נאות של תפקידו, ויוודאו שהוא **מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות**.

- **הממונה לא ימלא תפקיד נוסף שיעמידו בחשש לניגוד עניינים**, ולא יהיה כפוף למי שיכול להעמידו בחשש ניגוד עניינים. איסור זה חל גם לגבי כפיפות לגורם בגוף אחר שיכול להעמידו בחשש ניגוד עניינים, אם מדובר בממונה המשמש במיקור חוץ במספר גופים. בחינת קיומו של פוטנציאל לניגוד עניינים צריכה להיבחן לגופו של כל תפקיד בכל ארגון, אולם ככלל אצבע ניתן לומר שהוא מתקיים בתפקידים בכירים כגון מנהל שיווק, מנהל לקוחות, מנהל כספים, מנהל מערכות מידע או CTO.

האם הממונה על הגנת הפרטיות יכול למלא גם תפקיד של ממונה אבטחת מידע או CISO בארגון?

ממונה הגנת פרטיות וממונה אבטחת המידע הם שני תפקידים שונים במהותם - אשר לכל אחד מהם דרישות ידע, מיומנות ויכולות אחרות. לא בכדי החליט המחוקק שתפקידים אלו ידורו יחדיו בארגון, בעת ובעונה אחת.

חוק הגנת הפרטיות אינו אוסר במפורש על כך שממונה הגנת הפרטיות הארגוני ישמש גם כממונה אבטחת המידע או ה-CISO בארגון. עם זאת, דרישות החוק בעניין הידע והכישורים של הממונה על הגנת הפרטיות ובעניין אופן מילוי תפקידו, ברוב המקרים לא מתאימות למאפיינים של תפקיד ממונה האבטחה, או לעיתים אף יוצרות מורכבות משפטית להטלת כפל התפקידים על אותו אדם כאמור. נסביר:

- בחינת הרקע המקצועי והידע הנדרש עבור ביצוע התפקיד, מצביעה על כך שממונה אבטחת המידע הארגוני אינו בהכרח מקיים את דרישות הידע והכישורים עבור ממונה על הגנת הפרטיות כפי שנקבעו בחוק, בדגש על "ידע מעמיק בדיני הגנת הפרטיות". זאת במיוחד בכל הנוגע להיבטים המשפטיים והרגולטוריים של דיני הגנת הפרטיות, שהם בעלי חשיבות גם לנוכח תפקידו של ממונה הגנת הפרטיות כאיש הקשר של הארגון עם הרשות להגנת הפרטיות, בכל מגוון היבטי רגולציית הפרטיות והגנת המידע האישי.

- החוק קובע כי הממונה לא ימלא תפקיד נוסף שיעמידו בחשש לניגוד עניינים, ולא יהיה כפוף למי שיכול להעמידו בחשש ניגוד עניינים. לצד החפיפה הרחבה בתכליות ובתוכן של שני האינטרסים בשני התפקידים, קיים ביניהם גם שוני העשוי להביא להתנגשות. ממונה אבטחת המידע לא יוכל למלא במקביל גם את תפקיד הממונה על הגנת הפרטיות, אלא אם יש באפשרותו לאזן בצורה נאותה בין שני התפקידים, מבלי שתיפגע יכולתו למלא כל אחד מהם. בארגונים החייבים במינוי ממונה אבטחת מידע לפי סעיף 17ב(א) לחוק, יקשה לכאורה על ממונה האבטחה לאזן בצורה נאותה בין התפקידים, מפני שסעיף 17ב(ב) מטיל עליו אחריות אישית לאבטחת המידע בארגון. אחריות דומה אינה מוטלת במישרין על מי שנושא בתפקיד הממונה על הגנת הפרטיות, ועובדה זו כשלעצמה יכולה להשליך מערך השיקולים במקרים של התנגשות בין שני תחומי האחריות.

- ממונה אבטחת המידע לא בהכרח יעמוד בדרישת החוק לפיה על הממונה על הגנת הפרטיות לדווח ישירות למנכ"ל הארגון או למי שכפוף במישרין למנכ"ל.

- לבסוף, בארגונים גדולים או ארגונים בעלי היקף גדול של פעילות עיבוד מידע אישי, תפקיד הממונה על אבטחת המידע נושא באחריות כבדה ומצריך את תשומת ליבו המלאה של בעל התפקיד, באופן שלא יאפשר לו ככלל למלא בצורה נאותה גם את תפקיד הממונה על הגנת הפרטיות. נזכיר לעניין זה כי החוק קובע במפורש שעל הארגון לספק לממונה על הגנת הפרטיות את "התנאים והמשאבים הדרושים למילוי נאות של תפקידו ויוודא כי הוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות". הוראה דומה במהותה קיימת גם ביחס לממונה אבטחת המידע הארגוני, בתקנה 3(6) לתקנות אבטחת מידע.

מינוי ממונה על אבטחת המידע בארגון

חובת מינוי ממונה על אבטחת מידע, הקבועה בסעיף 17ב לחוק, הורחבה והוחלה לראשונה גם ביחס לבעלי שליטה במאגרים מרובים.

הגופים הנדרשים למנות ממונה על אבטחת מידע לאחר תיקון 13

- בעל שליטה או מחזיק בחמישה מאגרי מידע החייבים ברישום או בחובת הודעה לרשות להגנת הפרטיות בהתאם להסדר החדש בעניין חובת ההודעה.
- 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.

הוראות מהותיות הנוגעות לניהול מאגר מידע ועיבוד המידע בו

איסורים נורמטיביים חדשים בדבר עיבוד מידע שלא כדין

תיקון 13 כולל מספר איסורים נורמטיביים מהותיים חדשים ביחס לעיבוד מידע במאגר מידע, המפורטים בסעיף 8 העוסק בניהול מאגר מידע ועיבוד חוקי של מידע אישי.

להלן תמצית הסדרים אלו:

- **עיבוד בניגוד למטרה שנקבעה כדין** (סעיף 8(ב))- לא יעבד אדם מידע אישי במאגר מידע אלא למטרת המאגר שנקבעה לו כדין.
- **עיבוד ללא הרשאה** (סעיף 8(ג)) - לא יעבד אדם מידע אישי ממאגר מידע ללא הרשאה מאת בעל השליטה במאגר המידע, או בחריגה מהרשאה כאמור.
- **איסור גורף על עיבוד מידע במאגר בלתי חוקי** (סעיף 8(ד)) - בעל שליטה לא יעבד מידע במאגר ולא ירשה לאחר לעבד עבורו, אם המידע הכלול במאגר נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק הגנת הפרטיות, או להוראות כל דין אחר המסדיר עיבוד מידע.

סייגים – החוק קובע מספר סייגים ביחס לאיסור זה:

- ☐ ביחס לסעיף זה, "עיבוד" מוגדר למעט אחסון באקראי ובתום לב.
- ☐ החוק קובע כי כאשר מידע אישי נמסר לבעל שליטה מגורם אחר, ובעל השליטה **לא ידע ולא היה** עליו לדעת כי אותו גורם פעל שלא כדין, הוא לא יישא באחריות לעיבוד שלא כדין לפי סעיף זה, אשר בוצע לפני שידע או שהיה עליו לדעת על כך.
- ☐ האיסור לא יחול על הפרת דין קלת ערך בנסיבות העניין.

הסדרים מהותיים נוספים

חובת היידוע הקבועה בסעיף 11 מחייבת כל גורם המבקש לאסוף מידע אישי מאדם עבור מאגר מידע, לפרט בפניו נתונים הנוגעים לאיסוף ולשימוש שייעשה במידע על אודותיו.

במסגרת תיקון 13 **הורחבה חובת היידוע**, כך שהיא כוללת גם יידוע ביחס לתוצאות אי ההסכמה למסור את המידע המבוקש, וכן ביחס לקיומן של זכות עיון במידע אישי ושל זכות לבקש תיקון של מידע אישי. לפיכך, החל ממועד כניסתו לתוקף של החוק, פנייה לאדם לקבלת מידע אישי לשם עיבודו במאגר מידע צריכה לכלול את כל הפרטים הבאים:

- אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו ומהי תוצאת אי-ההסכמה.
- המטרה אשר לשמה מבוקש המידע.
- למי יימסר המידע ומטרות המסירה.
- קיומה של זכות עיון במידע האישי לפי סעיף 13.
- קיומה של זכות לבקש תיקון של המידע האישי לפי סעיף 14.

פיצויים ללא הוכחת נזק וביטול ההתיישנות המקוצרת

הרחבת סמכות בתי המשפט לפסוק פיצויים ללא הוכחת נזק וביטול ההתיישנות המקוצרת

החוק מרחיב את האפשרות לתבוע פיצוי ללא הוכחת נזק גם ביחס להפרות של הוראות חוק הגנת הפרטיות הקבועות בפרקים ב' ו-ד' לחוק, בסכום של עד 10,000 ש"ח, בעילות הבאות:

- ניהול מאגר החייב ברישום, מבלי שנרשם לפי סעיף 8א.
- פניה לאדם לקבלת מידע אישי אודותיו, ללא הודעה כנדרש בסעיף 11 או בסעיף 23ד(א)
- אי-מתן זכות עיון במידע אישי לפי סעיף 13.
- אי-תיקון או מחיקת מידע שבעל השליטה או המחזיק הסכים לבצע, או אי-הודעה על השינוי למי שקיבל את המידע לפי סעיף 14(ב).
- אי-מסירת הודעה על סירוב לתקן מידע או למוחקו לפי סעיף 14(ג).
- גוף ציבורי שלא הודיע לרשות על קבלה דרך קבע של מידע אישי מגוף ציבורי אחר, לפי סעיף 23ד(ג).

שינוי משמעותי נוסף ביחס לתביעות אזרחיות בגין פגיעה בפרטיות, הוא **ביטול תקופת ההתיישנות המקוצרת שעמדה עד כה על שנתיים** ביחס לתביעה אזרחית לפי חוק הגנת הפרטיות. המשמעות היא שתקופת ההתיישנות בגין תביעות אזרחיות לפי חוק הגנת הפרטיות **תהא מעתה זהה לתקופת ההתיישנות הכללית העומדת על שבע שנים (או יותר), בהתאם לדיני ההתיישנות הכלליים**. הוראה זו תחול רק ביחס לעילת תביעה שנוצרה לאחר כניסתו לתוקף של תיקון 13.

סמכויות אכיפה מנהלית ועיצומים כספיים

סמכויות האכיפה של הרשות להגנת הפרטיות

תיקון 13 מעדכן את כלל סמכויות האכיפה של הרשות להגנת הפרטיות, בתחום האכיפה המנהלית ובתחום האכיפה הפלילית.
סמכויות הפיקוח והבירור המנהלי המוקנות למפקחים ברשות, שהופעלו קודם לכן מכוח סעיף 10 לחוק הגנת הפרטיות עודכנו במסגרת החוק והורחבו לכל הפרה של סעיף 2 לחוק, ביחס למאגר מידע. החוק מבחין בין הליך פיקוח אשר ניתן לפתוח בו גם כאשר אין כל חשד להפרה של הוראות החוק או התקנות (כגון פיקוח שגרתי), לבין הליך בירור מנהלי בו ניתן לפתוח כאשר ישנו יסוד סביר להניח כי בוצעה הפרה של אותן הוראות מהחוק והתקנות, אשר ניתן להטיל בגינן עיצום כספי או להורות על הפסקת הפרתן לפי החוק.

בהליך בירור מנהלי נתונות למפקח כלל הסמכויות של הליך הפיקוח, לצד הסמכות לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב ולבצעם בעצמו או באמצעות מפקח אחר.
סמכויות האכיפה הפלילית המוקנות לחוקרים ברשות להגנת הפרטיות, שניתנו עד כה בהסמכה מטעם השר לביטחון לאומי, הוסדרו בגוף החוק.

עיצומים כספיים

החוק מרחיב באופן משמעותי את סל כלי האכיפה והסנקציות המנהליות שהרשות להגנת הפרטיות רשאית לנקוט בהן, ומעגן לראשונה את סמכותה של הרשות להטיל עיצום כספי, **בסכומים משמעותיים ביותר**, בגין הפרה של הוראות החוק, תקנות אבטחת מידע ותקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), תשפ"ג-2023 (להלן: "תקנות לעניין מידע שהועבר מהאזור הכלכלי האירופי"). בתוך כך, בוטל מנגנון הקנסות המנהליים שהיה קבוע עד כה בגין הפרות של חוק הגנת הפרטיות.

שימו לב - החוק קובע כי במקרה שבו הוטל עיצום כספי על מחזיק במאגר מידע, תישלח הודעה על כך גם לבעל השליטה במאגר, לצד הוראה כי עליו לפעול להפסקת ההפרה בידי המחזיק. אם לא הופסקה ההפרה ובעל השליטה לא פעל על פי הוראות הרשות - ניתן יהיה להטיל עליו את העיצום הכספי שהוטל על המחזיק במאגר, כאילו הוא היה המפר.

מנגנון העיצומים הכספיים וסכומי העיצום חולקו למספר קבוצות, על פי ההפרות השונות:

הפרות הנוגעות לרישום מאגרי מידע והודעה לרשות על מאגרי מידע

◀ סכום העיצום: 150,000 ₪

◀ במאגר שבו מעל מיליון נושאי מידע **סכום העיצום יוכפל**

- ☐ אי-רישום מאגר מידע החייב ברישום לפי סעיף 8א(א).
- ☐ אי-מסירת הודעה לרשות על מאגר מידע החייב בהודעה לפי סעיף 8א(ב)(1).
- ☐ מסירת פרטים שאינם נכונים בבקשה לרישום מאגר לפי סעיף 9.
- ☐ אי-מסירת הודעה לרשות על שינוי בפרטי רישום המאגר לפי סעיף 9(ד), למעט שינוי במען של בעל השליטה, או אי-מסירת הודעה על שינוי בפרטים שנמסרו במסגרת הודעה על מאגר מידע לפי סעיף 8א(ב)(2).
- ☐ עיבוד מידע במאגר המשמש לשירותי דיוור ישיר מבלי שהמאגר נרשם, או מבלי שאחת ממטרותיו הרשומות במרשם היא שירותי דיוור ישיר, לפי סעיף 17ד.
- ☐ גוף ציבורי שלא הודיע לרשות על כך שהוא מקבל מידע דרך קבע מגוף ציבורי אחר, לפי סעיף 23ד(ג).

הפרות בעניין מסירת הודעה לאדם לשם איסוף מידע אודותיו

◀ סכום העיצום:

- ☐ 50 ש"ח כפול מספר בני האדם שהפניה נעשתה אליהם.
- ☐ 100 ש"ח כפול מספר בני האדם שהפניה נעשתה אליהם, אם נעשתה לגבי מידע בעל רגישות מיוחדת. סכום העיצום בגין כל הפרה **לא יפחת מ-30,000 ש"ח.**

- ■ פניה לאדם לקבלת מידע אודותיו לשם עיבודו במאגר מידע, ללא מסירת הודעה כנדרש בסעיף 11 (כאשר הפניה היא לאדם מסוים).
- ■ פניה לאדם בדיוור ישיר, מבלי שהתקיימו תנאי סעיף 17ו(א).
- ■ גוף ציבורי שלא פירט בדרישת מידע שהוא מוסר מידע דרך קבע, לפי סעיף 23ד(א).

דוגמה: אם נעשתה פניה ל-5,000 איש לשם איסוף מידע אישי אודותיהם, ללא מסירת הודעה כנדרש בסעיף 11, והפניה נוגעת למידע בעל רגישות מיוחדת - סכום העיצום הכספי בגין ההפרה יעמוד על 500,000 ש"ח.

הפרות הנוגעות לעיבוד מידע שלא כדין

◀ סכום העיצום:

- ☐ 4 ש"ח בגין כל נושא מידע במאגר.
- ☐ 8 ש"ח בגין כל נושא מידע במאגר, אם קיים בו מידע בעל רגישות מיוחדת.
- ☐ סכום העיצום בגין כל הפרה **לא יפחת מ-200,000 ש"ח**.
- ☐ שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה לפי סעיף 2(9),

  או עיבוד מידע אישי במאגר למטרה המהווה פגיעה בפרטיות לפי סעיף 2, לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה.
- ☐ עיבוד מידע אישי במאגר מידע למטרה שאינה כדין, בניגוד להוראות סעיף 8(ב), אלא אם

  כן העיבוד נעשה רק בניגוד להוראות סעיף 2.
- ☐ עיבוד מידע אישי במאגר שהמידע בו נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק

  זה, או להוראות כל דין אחר המסדיר עיבוד מידע, לפי סעיף 8(ד), לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה.
- ☐ עיבוד מידע אישי ללא הרשאה של בעל השליטה במאגר או בחריגה מהרשאה, לפי סעיף 8(ג).
- ☐ בעל שליטה שמסר מידע מגוף ציבורי בניגוד להוראת סעיף 23ב(א), מבלי שהתקיימו

  תנאי סעיף 23ג.

דוגמה: אם נעשה עיבוד מידע אישי בחריגה מהרשאה של בעל השליטה, במאגר שבו מידע על 200,000 איש וקיים בו מידע בעל רגישות מיוחדת – סכום העיצום הכספי בגין ההפרה יעמוד על 1,600,000 ש"ח.

הפרות הנוגעות לזכות העיון ובקשות לתיקון ומחיקת מידע

◀ סכום העיצום: 15,000 ₪

- ☐ אי-מתן זכות עיון לאדם המבקש לעיין במידע אישי אודותיו במאגר מידע, לפי סעיף 13.
- ☐ ביצוע שינוי במידע אישי ללא מסירת הודעה לכל מי שקיבל את המידע, לפי סעיף 14(ב).
- ☐ אי-מסירת הודעה בדבר סירוב לתקן או למחוק מידע לבקשת נושא המידע, לפי סעיף 14(ג).
- ☐ אי-תיקון מידע על ידי מחזיק, שבעל השליטה הסכים לתקן או שבית המשפט הורה

  לתקן, לפי סעיף 14(ד).
- ☐ סירוב למחיקת מידע ממאגר המשמש לדיוור ישיר לבקשת נושא המידע, לפי סעיף 17(ב).
- ☐ סירוב לבקשת נושא מידע להימנע ממסירת מידע המתייחס אליו ממאגר לדיוור ישיר, לפי סעיף 17(ג).

הפרות הנוגעות לממונה הגנת הפרטיות, ממונה אבטחת מידע ודיווור ישיר

◀ סכום העיצום:

- ☐ 2 ש"ח בגין כל אדם שקיים לגביו מידע במאגר.
- ☐ 4 ש"ח בגין כל אדם שקיים לגביו מידע במאגר, אם קיים בו מידע בעל רגישות מיוחדת.
- ☐ סכום העיצום בגין כל הפרה **לא יפחת מ-20,000 ש"ח**, ואם קיים במאגר מידע בעל רגישות מיוחדת – **לא יפחת מ-40,000 ש"ח**.
- ☐ פניה לאדם לקבלת מידע אודותיו לשם עיבודו במאגר מידע, ללא מסירת הודעה כנדרש בסעיף 11, כאשר הפניה נעשתה לקבוצה בלתי מסוימת.
- ☐ אי-מינוי ממונה על אבטחת מידע, לפי סעיף 17ב(א).
- ☐ אי-מינוי ממונה על הגנת הפרטיות (DPO) בגופים ציבוריים או בגופים העוסקים בסחר במידע, לפי סעיפים 17ב1(א)(1)-(2).
- ☐ אי-קיום אחת ההוראות הבאות הנוגעות לממונה על הגנת הפרטיות, לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה, לפי סעיף 23כה(ד) –לא סופקו לממונה התנאים והמשאבים הדרושים למילוי נאות של תפקידו או שהוא לא היה מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות. הממונה אינו מדווח ישירות למנכ"ל או למי שכפוף אליו במישרין. הממונה אינו בעל הידע והכישורים הנדרשים לפי החוק. הממונה ממלא תפקיד נוסף או כפוף לנושא משרה באופן שעלול להעמידו בחשש לניגוד עניינים.
- ☐ ניהול מאגר מידע המשמש לשירותי דיוור ישיר, ללא רישום בדבר המקור שממנו התקבל כל אוסף נתונים, מועד קבלתו, ולמי נמסר, לפי סעיף 17ה.
- ☐ גוף ציבורי שלא קיים רישום של המידע האישי שמסר לגוף ציבורי אחר לפי פרק ד' לחוק, לפי סעיף 23ד(ב).

דוגמה: אם מדובר בגוף ציבורי שלא מינה ממונה על הגנת הפרטיות (DPO), ובמאגר המידע של הגוף הציבורי קיים מידע על 100,000 איש וקיים בו מידע בעל רגישות מיוחדת – סכום העיצום הכספי בגין ההפרה יעמוד על 400,000 ש"ח.

דוגמה נוספת: אם נעשתה פניה לקבוצה בלתי מסוימת של אנשים לשם איסוף מידע אישי אודותיהם (כגון באמצעות לינק באתר אינטרנט), מבלי שהפניה לוותה בהודעה כנדרש בסעיף 11, במאגר נאסף מידע אישי על 500,000 איש, וקיים בו מידע בעל רגישות מיוחדת – סכום העיצום הכספי בגין ההפרה יעמוד על 2,000,000 ש"ח.

עיצומים בגין הפרה של תקנות הגנת הפרטיות (אבטחת מידע)

העיצומים בגין הפרת תקנות אבטחת מידע נחלקים ל-3 רמות של הפרות:

- הפרות בסכומי העיצום: 20,000 ש"ח למאגרים ברמת אבטחה בינונית, ו-80,000 ש"ח למאגרים ברמת אבטחה גבוהה.

בקבוצה זו נכללות ההפרות הבאות:

- ☐ תקנה 5(א) – מבנה המאגר ומערכותיו.
- ☐ תקנה 5(ב) – מסירת פרטי מבנה המאגר ורשימת מצאי.
- ☐ תקנה 6(א) – הגנת מערכות.
- ☐ תקנה 6(ב) – בקרה ותיעוד כניסה לאתרים.
- ☐ תקנה 7(א) – ניהול כוח אדם.
- ☐ תקנה 7(ב) – הדרכת כוח אדם.
- ☐ תקנה 7(ג) - הדרכה תקופתית.
- ☐ תקנה 13(ב) – הפרדת מערכות המאגר (מידור).
- ☐ תקנה 17(א) – תיעוד.
- ☐ תקנה 17(ב), תקנה 18(א) ותקנה 18(ב) – גיבוי נתוני התיעוד;
- ☐ תקנה 19(ב) – הפרת חובות תיעוד.

- הפרות בסכומי העיצום: 40,000 ש"ח למאגרים ברמת אבטחה בינונית, ו-160,000 ש"ח למאגרים ברמת אבטחה גבוהה.

בקבוצה זו נכללות ההפרות הבאות:

- ☐ תקנה 2(א)– הכנת מסמך הגדרות מאגר.
- ☐ תקנה 2(ב) – עדכון מסמך הגדרות מאגר.
- ☐ תקנה 2(ג) ותקנה 19(ב) - בדיקת מידע עודף;

☐ תקנה 4(א) – הכנת נוהל אבטחת מידע.

☐ תקנות 4(ב) עד 4(ד), תקנה 11(ב) ותקנה 15(א)(3) – הוראות בנוהל אבטחת מידע.

☐ תקנות 8(א) עד 8(ב) – קביעה וניהול של הרשאות גישה.

☐ תקנה 9(א) ו-9(ג) – יישום נוהל הרשאות גישה.

☐ תקנות 10(א) עד 10(ה) – מנגנון בקרה ותיעוד גישה.

☐ תקנה 11(א) – תיעוד אירוע אבטחת מידע.

☐ תקנה 11(ג) ותקנה 19(ב) - דיון תקופתי באירועי אבטחת מידע;

☐ תקנה 13(ג) – עדכון מערכות המאגר.

☐ תקנה 14(א) – אבטחת חיבור ברשת.

☐ תקנה 16(א) ותקנה 16(ג) - ביקורת תקופתית.

■ הפרות בסכומי העיצום: 80,000 ש"ח למאגרים ברמת אבטחה בינונית, ו-320,000 ש"ח למאגרים ברמת אבטחה גבוהה.

בקבוצה זו נכללות ההפרות הבאות:

☐ תקנה 5(ג) – ביצוע סקר סיכונים (רק לגבי מאגרים ברמת האבטחה הגבוהה).

☐ תקנה 5(ד) – ביצוע מבדקי חדירות (רק לגבי מאגרים ברמת האבטחה הגבוהה).

☐ תקנה 11(ד)(1) – דיווח לרשות על אירוע אבטחה חמור.

☐ תקנה 15(א)(2) ותקנה 15(א)(4) – הפרת חובות בקרה ופיקוח על גורם חיצוני (מיקור חוץ).

במאגרי מידע בהם מעל מיליון נושאי מידע כל סכומי העיצום יוכפלו.

ביחס למאגרי מידע ברמת אבטחה בסיסית ומאגרים המנוהלים בידי יחיד, נקבעו עיצומים כספיים בסכומים של 1,000 -2,000 ש"ח ביחס להפרות הבאות:

- ☐ תקנה 2(א) – הכנת מסמך הגדרות מאגר.
- ☐ תקנה 2(ב) – עדכון מסמך הגדרות מאגר.
- ☐ תקנה 2(ג) ותקנה 19(ב) - בדיקת מידע עודף.
- ☐ תקנה 4(א) – הכנת נוהל אבטחת מידע (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנות 4(ב) עד 4(ג), תקנה 11(ב) ותקנה 15(א)(3) – נוהל אבטחת מידע (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 5(א) – מבנה המאגר ומערכותיו (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 5(ב) – מסירת פרטי מבנה המאגר ורשימת מצאי (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 6(א) – הגנת מערכות.
- ☐ תקנה 7(א) – ניהול כוח אדם (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 7(ב) – הדרכת כוח אדם (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 8(א) עד 8(ב) – קביעה וניהול של הרשאות גישה (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 9(א) – יישום נוהל הרשאות גישה.
- ☐ תקנה 9(ג) – יישום נוהל הרשאות הגישה לגבי בעל הרשאה שסיים את תפקידו (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 11(א) – תיעוד אירוע אבטחת מידע.
- ☐ תקנה 13(ג) – עדכון מערכות המאגר.
- ☐ תקנה 14(א) – אבטחת חיבור ברשת.
- ☐ תקנה 15(א)(2) ותקנה 15(א)(4) – בקרה ופיקוח על גורם חיצוני (מיקור חוץ) (רק ביחס למאגרים ברמת אבטחה בסיסית, עיצום כספי בסכום של 4,000 ש"ח).
- ☐ תקנה 17(א) – תיעוד (רק ביחס למאגרים ברמת אבטחה בסיסית).
- ☐ תקנה 19(ב) – הפרת חובות תיעוד (רק ביחס למאגרים ברמת אבטחה בסיסית).

עיצומים בגין הפרה של תקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר מהאזור הכלכלי האירופי)

◀ סכום העיצום בגין הפרת התקנות לעניין מידע שהועבר מהאזור הכלכלי האירופי, אשר ניתן להטיל עליהן עיצום כספי במישרין, ללא הוראה מקדימה של הרשות להפסקת ההפרה:

☐ 2 ש"ח בגין כל נושא מידע במאגר.

☐ 4 ש"ח בגין כל נושא מידע במאגר, אם קיים בו מידע בעל רגישות מיוחדת.

בקבוצה זו נכללות ההפרות הבאות:

- אי-הפעלת מנגנון שמטרתו להבטיח כי במאגר לא מוחזק מידע שאינו נחוץ עוד, לפי תקנה 4(א).
- אי-הפעלת מנגנון שמטרתו להבטיח כי המידע שבמאגר נכון, שלם, ברור ומעודכן, לפי תקנה 5(א).
- אי-נקיטת כל אמצעי לתיקון או מחיקת מידע לאחר שנמצא כי במאגר קיים מידע שאינו נכון, שלם, ברור או מעודכן, לפי תקנה 5(ב).

◀ סכום העיצום בגין הפרת התקנות שלגביהן נדרשת תחילה הוראה של הרשות להפסקת ההפרה:

☐ 4 ש"ח בגין כל נושא מידע במאגר.

☐ 8 ש"ח בגין כל נושא מידע במאגר, אם קיים בו מידע בעל רגישות מיוחדת.

בקבוצה זו נכללות ההפרות הבאות:

- אי-מחיקת מידע אישי לבקשת נושא המידע ואי-ביצוע פעולות המבטיחות שלא יתאפשר, באמצעים סבירים, לזהות את נושא המידע, לפי תקנה 3(ג), לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה.
- אי-מחיקת מידע אישי לאחר שבעל השליטה מצא כי במאגר מוחזק מידע שאינו נחוץ, ולא בוצעו פעולות המבטיחות שלא יתאפשר באמצעים סבירים לזהות את נושא המידע, לפי תקנות 4(ב)-(ג), לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה.
- אי-מסירת הודעה לאדם על כך שהתקבל לגביו מידע מהאזור הכלכלי האירופי, לפי תקנה 6(א), לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה.
- אי-מסירת הודעה לאדם שהתקבל לגביו מידע מהאזור הכלכלי האירופי על כך שבכוונת בעל השליטה במאגר המידע להעביר את המידע לצד שלישי, לפי תקנה 6(ב), לאחר שניתנה הוראה על ידי הרשות להפסקת ההפרה.
- אי-מסירת הודעה לנושא המידע בדבר החלטה בבקשתו למחיקת מידע אודותיו, לפי תקנה 3(ד) – 15,000 ש"ח.

החל מ-1 בינואר 2025 התקנות חלות גם על מידע "ישראלי" המצוי באותו מאגר יחד עם מידע שהתקבל מהאזור הכלכלי האירופי.

נסיבות להפחתת עיצום כספי

בהתאם לתוספת החמישית לחוק הרשות להגנת הפרטיות רשאית, **על פי בקשת המפר**, להפחית את סכום העיצום הכספי בנסיבות הבאות, ובשיעורים המפורטים מטה, ובלבד ששיעור ההפחתה לא יעלה על 70% מסכום העיצום שהוטל.

- לא הוטל על המפר עיצום כספי בשל הפרת אותה הוראה ב-5 השנים שקדמו להפרה – הפחתה של 20%, ובשלוש השנים שקדמו להפרה – הפחתה של 10%.
- המפר הפסיק את ההפרה מיוזמתו ודיווח עליה לרשות – הפחתה של 30%.
- המפר נקט פעולות למניעת הישנות ההפרה ולהקטנת הנזק, להנחת דעת הרשות – הפחתה של 20%.
- המפר חב במינוי ממונה על הגנת הפרטיות (DPO), ומינה אותו בפועל, ובלבד שאיננו גוף ציבורי או מי שעוסק בסחר במידע – הפחתה של 10%.
- המפר שילם פיצוי או שנפסק לחובתו פיצוי בשל אותן הפרות – הפחתה של עד 30%.
- לגבי מפר שהוא יחיד, מצאה הרשות כי קיימות נסיבות אישיות קשות המצדיקות זאת – הפחתה של עד 20%.
- לעסקים קטנים (מחזור שנתי בין 4-10 מיליון ש"ח) ולעסקים זעירים (מחזור שנתי עד 4 מיליון ש"ח) נקבעו תקרות לסכום העיצום שניתן להטיל בגין הפרות שונות, במסגרת אותו הליך אכיפה.
- בכל מקרה לא יוטל עיצום כספי כולל העולה על 5% ממחזור העסקאות השנתי של המפר.

צו שיפוטי להפסקת עיבוד מידע במאגר או למחיקתו

במסגרת תיקון 13, הוסמך בית המשפט לעניינים מינהליים, לבקשת הרשות, לתת צו לבעל שליטה במאגר מידע או למחזיק במאגר להפסקת פעולות עיבוד מידע הגורמות להפרה, לרבות צו למחיקת המידע האישי במלואו, לפי סעיף 23מט לחוק.

בית המשפט יוכל לתת צו שכזה אם התקיימו התנאים המצטברים הבאים - אין אמצעי אחר שפגיעתו פחותה למניעת ההפרה, הנזק שעלול להיגרם מההפרה עולה על הנזק ממתן הצו לרבות הפגיעה בחופש הביטוי, חומרת ההפרה מצדיקה את מתן הצו, ובית המשפט שוכנע כי מתבצעת או עומדת להתבצע במאגר אחת ההפרות הבאות:

- שימוש בידיעה על ענייניו הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה (סעיף 2(9) לחוק).
- עיבוד מידע אישי במאגר בניגוד למטרת המאגר שנקבעה לו כדין (סעיף 8(ב) לחוק).
- עיבוד מידע אישי ללא הרשאה מבעל השליטה או בחריגה מהרשאה (סעיף 8(ג) לחוק).
- עיבוד מידע אישי אשר נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק הגנת הפרטיות או להוראות כל דין אחר המסדיר עיבוד מידע (סעיף 8(ד) לחוק).
- הפרת חובת אבטחת המידע או הפרת תקנות הגנת הפרטיות (אבטחת מידע) (סעיף 17 לחוק ותקנות אבטחת מידע).
- מסירת מידע מגוף ציבורי שלא כדין (סעיף 23ב לחוק).

עבירות פליליות חדשות ביחס למאגרי מידע

- בנוסף לעבירות הפליליות הקבועות כיום בסעיף 5 לחוק הגנת הפרטיות (אשר קובע עבירה פלילית ביחס למרבית המצבים המנויים בסעיף 2 לחוק) ובסעיף 16 לחוק הגנת הפרטיות שעניינן פגיעה בפרטיות במזיד והפרת חובת סודיות במאגרי מידע, תיקון 13 הוסיף לחוק פרק של עבירות פליליות חדשות הכולל את העבירות הבאות:

- **עיבוד ללא הרשאה** – עיבוד מידע ממאגר מידע בלא הרשאה מאת בעל השליטה במאגר, לפי סעיף 8(ג) – עבירה שדינה מאסר 3 שנים (סעיף 23נה לחוק).

- **הפרת חובת היידוע** – פניה לאדם לקבלת מידע אישי אודותיו לפי סעיף 11, תוך מסירת פרטים לא נכונים בכוונה להטעותו באשר למסירת המידע האישי – עבירה שדינה מאסר 3 שנים (סעיף 23נו לחוק).

- **מסירת מידע מגוף ציבורי** – גוף ציבורי, עובד של גוף ציבורי או מי שפועל מטעם גוף ציבורי, המוסר מידע שחל איסור על מסירתו מגוף ציבורי לפי סעיף 23ב, במטרה שגורם שאינו מוסמך יעבדו – עבירה שדינה מאסר 3 שנים (סעיף 23נז לחוק).

- **הפרעה** – הפרעה לראש הרשות, לחוקר או למפקח מטעם הרשות במילוי תפקידם – עבירה שדינה מאסר של 6 חודשים (סעיף 23נג לחוק).

- **הטעיה** – הטעיית ראש הרשות, מפקח או מומחה חיצוני מטעם הרשות באמצעות מסירת פרטים שאינם נכונים בבקשה לרישום מאגר מידע, בהודעה על מאגר מידע, בהודעה על שינוי פרטי הרישום, או במענה לדרישת ידיעות ומסמכים של מפקח או של מומחה חיצוני – עבירה שדינה מאסר שנתיים (סעיף 23נד לחוק).

הסדר פיקוח מיוחד בגופים ביטחוניים

הגופים עליהם חל ההסדר

- משטרת ישראל.
- צבא הגנה לישראל.
- שירות הביטחון הכללי.
- המוסד למודיעין ולתפקידים מיוחדים.
- מערך הסייבר הלאומי.
- הרשות להגנה על עדים.
- שירות בתי הסוהר.
- משרד הביטחון, הממונה על הביטחון במערכת הביטחון ויחידות הסמך של משרד הביטחון.
- יחידות ויחידות סמך של משרד ראש הממשלה, שעיקר פעילותן בתחום ביטחון המדינה.
- מפעלי מערכת הביטחון, הנכללים בצו של שר הביטחון.

מינוי וכהונת מפקח פרטיות פנימי בגופים ביטחוניים

- בכל גוף ביטחוני ימונה **מפקח פרטיות פנימי**, המינוי ייעשה בהתייעצות עם ראש הרשות להגנת הפרטיות, בהתאם לתנאי כשירות והכשרה שקבע ראש הרשות, ושלגביהן נועץ בראש הגוף הביטחוני.
- תקופת הכהונה של המפקח הפנימי לא תפחת מ-3 שנים.
- המפקח הפנימי יהיה כפוף ישירות לראש הגוף הביטחוני, או למי שכפוף ישירות לראש הגוף, והוא יונחה מקצועית בידי ראש הרשות להגנת הפרטיות.
- הגוף הביטחוני יעמיד לרשות המפקח הפנימי אמצעים נאותים הנדרשים למילוי תפקידו.
- הארכת כהונתו של המפקח הפנימי, הפסקת כהונתו והעברתו מתפקידו ייעשו רק לאחר התייעצות עם ראש הרשות להגנת הפרטיות.

תפקידי מפקח הפרטיות הפנימי

- בירור הפרות של חוק הגנת הפרטיות ותקנותיו.
- בדיקת נהלי הגוף הביטחוני ומדיניותו בתחום הגנת הפרטיות,
- הכנת תכנית עבודה שנתית לפיקוח על הוראות החוק.
- דיווח לרשות להגנת הפרטיות על ממצאי פעולות הפיקוח והבדיקה שביצע.
- קיום הכשרות והדרכות לעובדי הגוף הביטחוני.

הוראות נוספות

- הרשות רשאית להורות למפקח הפנימי לבצע פעולות משלימות או נוספות או לפעול לתיקון ליקויים שהתגלו.
- הרשות רשאית להשתמש בסמכויותיה להורות על הפסקת הפרה, להטיל עיצום כספי או לפתוח בחקירה פלילית על יסוד ממצאי הבירור שביצע המפקח הפנימי.

פניה לרשות להגנת הפרטיות לקבלת חוות דעת מקדמית

בהתאם להוראות סעיף 2ט17 לחוק, על הרשות לתת חוות דעת מקדמית, לבקשת בעל שליטה או מחזיק במאגר המידע, או מי שעומד להיות אחד מאלה, בעניין עמידת מאגר המידע בדרישות חוק הגנת הפרטיות ותקנותיו לעניין עיבוד המידע במאגר המידע.

אופן הגשת הבקשה לקבלת חוות דעת מקדמית, והנסיבות בהן לא תינתן חוות דעת מטעם הרשות, מפורטים בנוהל מתן חוות דעת מקדמית על ידי הרשות להגנת הפרטיות,

הזמין באתר האינטרנט של הרשות.

משרד המשפטים

MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות

THE PRIVACY PROTECTION AUTHORITY

سلطة القانون التكنولوجيا والمعلومات