כ״ז תמוז תשפ״ה
23 ביולי 2025

גילוי דעת:

מינוי ממונה על הגנת הפרטיות בארגון לפי דרישות תיקון 13 לחוק הגנת הפרטיות

טיוטה להערות הציבור

מבוא

1. ביום 5 באוגוסט 2024, אישרה הכנסת את תיקון מס׳ 13 לחוק הגנת הפרטיות,[1] המהווה את העדכון המקיף והמהותי ביותר לדיני הפרטיות בישראל מאז נחקק לראשונה חוק הגנת הפרטיות, התשמ״א-1981 (להלן: **״חוק הגנת הפרטיות״ או ״החוק״**). **אחד החידושים החשובים ביותר בתיקון מס׳ 13, הוא החובה למנות ממונה על הגנת הפרטיות** בגופים ציבוריים ובשורה ארוכה של ארגונים נוספים מכל רחבי המשק שפעולתם כרוכה בסיכון גבוה לפרטיות. יחד עם כל הוראות תיקון מס׳ 13, גם חובה חדשה זו **תיכנס לתוקף ביום 14.8.25**. מטרתו של גילוי הדעת להציג את עמדת הרשות ביחס להיקף החובה, מהות תפקידיו של הממונה, הידע והכישורים הנדרשים ממנו, וביחס להוראות נוספות בחוק המסדירות את מעמדו של הממונה בארגון ומתכונת העסקתו. הפרשנות המוצגת בגילוי הדעת תשמש את הרשות בעת הפעלת הסמכויות המוקנות לה, לרבות הסמכות להטיל עיצומים כספיים בגין הפרה של החובה למנות ממונה על הגנת הפרטיות ושל הוראות אחרות בחוק הנוגעות למעמדו ולמתכונת העסקתו. עם זאת, בעת הפעלת סמכויותיה ובכללן סמכויות האכיפה, תתחשב הרשות בכך שגילוי הדעת בשלב זה אינו מסמך סופי אלא עדיין בגדר טיוטה להערות הציבור.

רקע

2. מינוי ממונה ארגוני להגנה על הפרטיות, או Data Protection Officer, הוא רכיב מרכזי בתפיסת האחריותיות (accountability). עיקרון האחריותיות קובע את אחריות הארגון לקיום הוראות הדין הנוגעות לשימוש במידע, ואת חובתו לנקוט בשיטות עבודה פנימיות שיישמו את אחריותו ויאפשרו לו להציג ולהוכיח אותה.

3. אחריותיות מקובלת זה מכבר כדרך התנהלות ראויה בהגנה על מידע אישי, אשר מסייעת לארגון לוודא כי הוא מקיים את ההוראות המהותיות של הדין, מצמצמת את חשיפתו לסיכונים משפטיים ותפעוליים, ותורמת לביסוס האמון בו בעיני לקוחות, שותפים עסקיים, רגולטורים וצדדים שלישיים נוספים.[2]

---

[1] חוק הגנת הפרטיות (תיקון מס׳ 13), התשפ״ד-2024. למען הסר ספק, כלל ההפניות להוראות חוק הגנת הפרטיות בגילוי דעת זה מתייחסות לחוק כנוסחו לאחר כניסתו לתוקף של תיקון מס׳ 13.

[2] להרחבה ראו: OECD Privacy Guidelines Implementation Guidance: Foreword and Chapter on Accountability (2023).

4. האחריותיות כעיקרון כללי לעיבוד מידע, ודרישות קונקרטיות הנגזרות ממנו, הפכו לעקרון יסוד ולחובות בנות אכיפה בחקיקת הגנת מידע אישי מתקדמת בעולם, כולל ברגולציית הגנת הפרטיות של האיחוד האירופי (GDPR). היבטים מסוימים של אחריותיות באים לידי ביטוי גם בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת המידע**").

5. חשיבות מיוחדת למינוי ממונה ארגוני להגנה על הפרטיות נובעת גם מן הצורך להבטיח מנגנוני בקרה נאותים נוכח הצמצום המשמעותי של חובת רישום מאגרי מידע בתיקון מס' 13 בנוגע לגופים במגזר הפרטי, בפרט ביחס למאגרים שניהולם כרוך בסיכון גבוה לפרטיות.

6. החובה למנות ממונה ארגוני להגנה על הפרטיות קבועה בחקיקת פרטיות והגנת מידע אישי במדינות רבות בעולם, כדוגמת מדינות האיחוד האירופי, בריטניה, דרום אפריקה וברזיל. באיחוד האירופי סעיף 37 ל-GDPR מחייב למנות Data Protection Officer בין היתר כאשר עיבוד המידע מתבצע על ידי גוף ציבורי, או כאשר ליבת העיסוק של הארגון כוללת פעולות עיבוד מידע אישי אשר מתוקף טיבן, היקפן או מטרותיהן, מחייבות ניטור שיטתי של נושאי מידע בהיקף רחב, או במקרים בהם ליבת העיסוק של הארגון כוללת פעולות עיבוד מידע אישי רגיש בהיקף רחב.[3]

7. בשנים האחרונות הלכו ורבו הארגונים בישראל אשר מינו ממונה הגנה על הפרטיות שלא מכוח חובה בדין הישראלי, אם בשל כפיפותם לרגולציה זרה הדורשת זאת; ואם מיוזמתם החופשית, מתוך הבנה כי מידת העיסוק של הארגון בתחום הגנת הפרטיות מצדיקה מינוי בעל תפקיד ייעודי לנושא.[4] **כבר בראשית 2022 פרסמה הרשות להגנת הפרטיות המלצות בנושא "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו". במסמך זה הבהירה הרשות את עמדתה לפיה מינויו של ממונה הגנת פרטיות באופן וולונטרי מהווה פרקטיקה ראויה ומומלצת (Best Practice) לארגונים האוספים ומעבדים מידע אישי, בעלי מאגרים ומחזיקים כאחד**. הרשות הסבירה כי פרקטיקה זו נושאת בחובה יתרונות רבים, הן לארגון הן לנושאי המידע. מינוי ממונה על הגנת הפרטיות מסייע באופן ממשי לארגון לעמוד בהוראות דיני הגנת המידע האישי בישראל, מהווה אינדיקציה כי הארגון נקט ונוקט צעדים לצמצום הסיכון לפגיעה במידע האישי הנשמר ברשותו, וכן מאפשר שיתוף פעולה מיטבי עם הרשות להגנת הפרטיות.

8. כאמור, בתיקון מס' 13 נוספה לראשונה בחוק הגנת הפרטיות **החובה** למנות ממונה על הגנת הפרטיות בשורה ארוכה של ארגונים במשק (סעיפים 17ב1 – 17ב3 לחוק).

---

[3] להשוואה והרחבה על תפיסת הדין האירופי את תפקיד ה-DPO ראו הנחיות הועדה המקצועית של רשויות הפרטיות במדינות האיחוד האירופי(EDPB – European Data Protection Board), אשר אימצה בשנת 2018 את ההנחיות בנושא DPO שפורסמו על ידי הגוף שקדם לה (Article 29 Data Protection Working Party). ראו גם מדריך פרקטי של רשות הגנת הפרטיות הצרפתית CNIL.

[4] למחקר אמפירי בנוגע לממוני הגנת הפרטיות המכהנים כיום בגופים שונים בישראל, ראו: Birnhack, Michael D. and Mundlak, Guy, *The Brussels Effect(s) and the Rise of a Privacy Profession*, International Data Privacy Law (forthcoming, 2025).

<u>על מי מוטלת החובה למנות ממונה על הגנת הפרטיות?</u>

9. לפי סעיף 17ב1(א) לחוק, החובה למנות ממונה על הגנת הפרטיות חלה על כל אחד מסוגי הגופים הבאים:

<u>גופים ציבוריים – סעיף 17ב1(א)(1)</u>

9.1. החובה למנות ממונה חלה על כל בעל שליטה במאגר מידע שהוא גוף ציבורי כהגדרתו בסעיף 23 לחוק, על שתי חלופותיו: הן משרדי הממשלה, רשויות המדינה, רשויות מקומיות[5] וגופים אחרים הממלאים תפקיד ציבורי על פי דין (כגון המוסד לביטוח לאומי ותאגיד השידור הציבורי);[6] והן גופים אחרים הכלולים בצו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו-1986 שקבע שר המשפטים מכוח סעיף 23(2) לחוק, לרבות **קופות חולים, בתי חולים, מוסדות להשכלה גבוהה, ארגוני עובדים ועוד**. חובת המינוי חלה על הגוף הציבורי גם אם מאגר המידע שבשליטתו פטור מחובת הרישום, למשל מן הטעם שהוא כולל מידע על עובדי הגוף הציבורי בלבד.[7] חובת המינוי מכוח סעיף 17ב1(א)(1) לחוק אינה חלה על גוף ציבורי שהוא גם "גוף בטחוני" כהגדרתו בסעיף 23כ לחוק, מאחר שביחס לגופים אלו נקבע בתיקון מס' 13 הסדר נפרד, המחייב מינוי מפקח פרטיות פנימי (סעיפים 23כ-23כד לחוק).

9.2. חובת המינוי חלה גם על כל "**מחזיק**"[8] **במאגר מידע של גוף ציבורי**, כלומר גורם חיצוני לגוף הציבורי המעבד עבורו מידע אישי. יובהר, כי בהתאם להגדרה החדשה של "עיבוד, שימוש" כפי שנקבעה בתיקון 13, עיבוד מידע אישי הוא כל פעולה המבוצעת על מידע אישי, לרבות עצם אחסון המידע או העיון בו.[9] ככל שאלו נעשים עבור הגוף הציבורי על ידי גורם חיצוני, אותו גורם הוא בבחינת "מחזיק" לפי החוק, המחויב במינוי ממונה על הגנת הפרטיות.

<u>גופים העוסקים בסחר במידע – סעיף 17ב1(א)(2)</u>

9.3. בעל שליטה במאגר מידע שמטרתו העיקרית היא **איסוף מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה**,[10] לרבות שירותי דיוור ישיר,[11] ויש במאגר מידע אישי על יותר מ-10,000 בני

---

[5] יובהר כי חברה ממשלתית או תאגיד עירוני אינם חלק מן האישיות המשפטית של המדינה או הרשות המקומית, לפי העניין, ולכן לא ייחשבו "גוף ציבורי" אלא אם כן הם ממלאים "תפקיד ציבורי על פי דין" או נכללים בצו שפורסם מכוח סעיף 23(2) לחוק.

[6] להרחבה בשאלה מהו "גוף הממלא תפקיד ציבורי על פי דין" לעניין סעיף 23 לחוק הגנת הפרטיות ראו פסק דינו של בית המשפט העליון בע"א 8825/03 **שירותי בריאות כללית נ' משרד הביטחון** (נבו 11.4.2007).

[7] סעיף 8א(א)(1)(ב) לחוק.

[8] בהתאם להגדרה המעודכנת של "מחזיק" בסעיף 3 לחוק.

[9] ראו הגדרת "עיבוד, שימוש" בסעיף 3 לחוק, כפי שעודכנה בתיקון מס' 13.

[10] תנאים אלה חלופיים. כלומר, מאגר שמטרתו העיקרית היא מסירת המידע לצד שלישי באופן קבוע כחלק מעיסוקו של בעל המאגר, **אף אם המסירה היא ללא תמורה**; או מאגר שמטרתו מסירת המידע לצד שלישי בתמורה, **אף אם איננה נעשית כדרך עיסוק**.

[11] סעיף 3 לחוק מגדיר "דיוור ישיר" כ-"פנייה אישית לאדם, בהתבסס על השתייכותו לקבוצת אוכלוסין, שנקבעה על פי אפיון אחד או יותר של בני אדם ששמותיהם כלולים במאגר מידע" ומגדיר "שירותי דיוור ישיר" כ-"מתן שירותי דיוור ישיר לאחרים בדרך של העברת רשימות, מדבקות או נתונים בכל אמצעי שהוא". להרחבה על שירותי דיוור ישיר ודיוור ישיר ראו הנחיית הרשות להגנת הפרטיות מס' 2/2017 בנושא "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר". ההנחיה זמינה כאן.

אדם. הכוונה היא לארגונים העוסקים בסחר במידע (Data Brokers) במובן הרחב של המונח,[12] המגלמים סיכון גבוה יותר לפגיעה בפרטיות. יצוין, כי חובת המינוי **לפי סעיף זה** אינה חלה על גוף שהוא בגדר מחזיק במאגרים האמורים, אולם היא עשויה לחול עליו מכוח אחת העילות האחרות, שלגביהן נרחיב להלן.

<u>גופים העוסקים בניטור שוטף ושיטתי של בני אדם – סעיף 17ב1(א)(3)</u>

9.4. חובת המינוי חלה על בעל שליטה במאגר מידע או מחזיק במאגר מידע שעיסוקיו העיקריים כוללים פעולות עיבוד מידע או כרוכים בפעולות כאמור,[13] אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם. **כדוגמה לעיבוד מידע הכולל ניטור שוטף ושיטתי, מציין החוק "מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר"**, ומזכיר גם ספקי תקשורת סלולרית וספקי שירותי חיפוש מקוון (כגון מנועי חיפוש).

9.5. המונח "ניטור שוטף ושיטתי" רלוונטי במיוחד להתחקות אחרי פעילות משתמשים באפליקציות ובאתרי אינטרנט (כגון תדירות השימוש, סוגי הפעולות שמתבצעות, וזמני הפעולות), ולעיבוד מידע אישי במטרה ליצור פרופיל של תכונות, התנהגויות, תחומי עניין או העדפות של אנשים (profiling), למגוון מטרות, לרבות פרסום ממוקד, התאמה אישית של תוכן ושירותים, וניהול סיכונים (דירוג אשראי, חיתום ביטוחי, איתור הונאות ועוד).

9.6. דוגמאות נוספות למאגרי מידע ולשירותים שהפעלתם כרוכה בניטור שוטף ושיטתי של בני אדם: אפליקציות האוספות נתוני מיקום במרחב הפיזי, אפליקציות והתקני מחשוב לביש העוקבים אחרי נתוני בריאות, מתקנים מחוברים לאינטרנט כגון כלי רכב חכמים ומכשירי חשמל ביתיים המחוברים לרשת (אינטרנט של הדברים (IoT),[14] מאגרי הצילומים של מצלמות מעקב וספקי אינטרנט.

9.7. יודגש כי הדוגמאות הנקובות במפורש בחוק או המפורטות במסמך זה אינן ממצות את גדרי החובה הקבועה בסעיף 17ב1(א)(3) לחוק. במקרה של ספק ניתן לפנות בשאלה ספציפית לרשות להגנת הפרטיות.[15]

---

[12] כך למשל, לפי רשות הגנת המידע הבריטית (Information Commission's Office), סוכנויות דירוג אשראי (credit reference agencies) זוהו כארגונים העוסקים בסחר במידע (להרחבה ראו כאן) שכן הם מספקים נתוני אשראי, היסטוריית רכישות והתחייבויות פיננסיות.

[13] כלומר, די בכך שעיסוקיו המרכזיים של הארגון יהיו כרוכים בניטור שוטף ושיטתי **בפועל** – גם אם זו איננה מטרתם.

[14] להרחבה בנושא היבטי הפרטיות במכשירים אלו, ראו מסמך מקיף שפרסמה הרשות להגנת הפרטיות בעניין "פרטיות במוצרי IoT ביתיים ובבתים חכמים" (2023). המסמך זמין כאן.

[15] כחומר רקע להשוואה ראו סעיף 37(1)(b) ל-GDPR, שנוסחו דומה מאוד לנוסח סעיף 17ב1(א)(3) לחוק, והפרשנות שניתנה לסעיף זה ב-GDPR בהנחיה שאומצה על ידי ה-EDPB, לעיל ה"ש 3. ראו עמ' 21-22 להנחיה זו.

גופים המעבדים מידע בעל רגישות מיוחדת – סעיף 17ב1(א)(4)

9.8. בעל שליטה או מחזיק במאגר מידע שעיסוקו העיקרי כולל עיבוד בהיקף ניכר של מידע אישי הכלול באחת או יותר מן הקטגוריות של הגדרת המונח "**מידע בעל רגישות מיוחדת**" בסעיף 3 לחוק. ב"עיסוקו העיקרי" הכוונה היא לעיבוד מידע אישי שהוא רכיב מרכזי בהגשמת המטרות העסקיות או הארגוניות העיקריות של בעל השליטה במאגר או המחזיק, או חלק אינהרנטי מפעילות הליבה של הארגון (אף אם איננו חיוני להגשמתה). כך לדוגמא, עיבוד מידע רפואי על מטופלים נכלל בעיסוקם העיקרי של מוסדות רפואיים. לעומת זאת, סעיף 17ב1(א)(4) לא יחול על עיבוד מידע בעל רגישות מיוחדת הנדרש **רק** לצורך ביצוע **מטרות עזר משניות** כגון העסקת עובדים, אם אינן בעלות זיקה ישירה למטרות המרכזיות של הארגון.[16]

9.9. החוק קובע במפורש כי בנקים, חברות ביטוח, בתי חולים וקופות חולים חייבים במינוי ממונה לפי דרישות סעיף 17ב1(א)(4). מבלי לגרוע מכלליות ההוראה המהותית או למצות את תחולתה, מאפייני הגופים ברשימה מכלילה זו ("white list") יכולים לשמש דוגמא למאפיינים של גופים נוספים "שעיסוקם העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר".

מהו עיבוד מידע "בהיקף ניכר" – סעיף 17ב1(ב)

9.10. למונח "**היקף ניכר**", שהוא אחד מהתנאים לתחולת הקטגוריות בסעיפים 17ב1(א)(3) ו-(4) לחוק, אין סף כמותי חד ערכי ויש לבחון אותו לפי מכלול הנסיבות והשיקולים הנוגעים לכל מקרה לגופו. סעיף 17ב1(ב) לחוק נוקב במפורש בכמה מן הקריטריונים העיקריים הרלוונטיים לבחינה פרטנית זו, ובהם: מספר בני האדם שמידע מעובד לגביהם; שיעורם באוכלוסייה מסוימת; היקף המידע; כמות המידע; הטווח (המגוון) של סוגי המידע המעובד; משך ותדירות פעולות העיבוד; משך שמירת המידע והתחום הגאוגרפי של פעולות העיבוד. יודגש כי קריטריונים אלה **אינם חייבים להתקיים באופן מצטבר**, והפירוט שלהם בגוף החוק נועד להבהיר את תכלית המונח. כך למשל, ברור שפעולות עיבוד של מידע אישי על **מספר גדול** של בני אדם ייחשבו לפעולות עיבוד "בהיקף ניכר", גם אם לא מתקיים אף אחד משאר השיקולים הנזכרים בסעיף. לעומת זאת, גם כאשר מספר נושאי המידע עליהם מעובד המידע איננו גדול – תיטה הכף להתייחס לפעולות העיבוד כמבוצעות "בהיקף ניכר", ככל שמתקיימים בה אחד או יותר משאר השיקולים המפורטים בסעיף. עוד יודגש כי מתוך לשון סעיף 17ב1(ב), המציין כי עיבוד מידע בהיקף ניכר יהיה "**בין השאר**" בשים לב לשיקולים המפורטים בו, ניתן ללמוד כי יתכנו גם שיקולים נוספים מעבר לאלו המנויים בסעיף, אותם ניתן יהיה לשקול לצורך בחינה האם עיבוד מידע על ידי ארגון מסוים עולה כדי עיבוד בהיקף ניכר.

---

[16] להסיר ספק, על עיבוד מידע הנדרש רק לצורך העסקת עובדים – **כן יחולו שאר הוראות החוק** הנוגעות למידע בעל רגישות מיוחדת, לרבות החובה למסור הודעה לרשות על ניהול מאגר מידע בהתאם לסעיף 8א(ב) לחוק, גובה העיצומים הכספיים בגין הפרת הוראות החוק או התקנות מכוחו, ורמת אבטחת המידע של המאגר לעניין תקנות אבטחת המידע והתוספת השלישית לחוק.

9.11. יש לשים לב גם להגדרת המונח "**עיבוד, שימוש**" בסעיף 3 לחוק, שתוכנה עודכן במטרה להסיר ספק בדבר תחולתה על "**כל פעולה שמבוצעת על מידע אישי**" לרבות קבלת המידע, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו.

<u>מינוי ממונה במקרים של ספק באשר לתחולת החובה ומינוי וולונטרי</u>

9.12. בנוסף לגופים המחויבים במינוי ממונה על הגנת הפרטיות בהתאם להסדר שנקבע בחוק, גם בארגונים עליהם לא מוטלת חובה חוקית, מומלץ לשקול מינוי זה. מינוי ממונה על הגנת הפרטיות תורם משמעותית לשיפור הציות לדיני הגנת הפרטיות, מחזק את תפיסת האחריותיות הארגונית בניהול מידע אישי, ומחזק את היכולת ליישם עקרונות של מידתיות בשמירה על הזכות לפרטיות במסגרת פעילות הגוף, מקום בו יש חובה כזו. מינוי ממונה על הגנת הפרטיות גם תואם את האינטרסים העסקיים של הגוף עצמו. בין השאר, מינוי הממונה מסייע בבניית האמון בקרב לקוחות ונושאי מידע אחרים של הארגון, המעריכים את המאמצים שהגוף נוקט להגנה על פרטיותם, ומכאן תורם גם לחיזוק המוניטין של הארגון. הרשות סבורה כי חשיבות מיוחדת ויתרונות רבים עשויים לקום ממינוי ממונה הגנת הפרטיות בארגונים הכפופים לפחות לחלק מעקרונות המשפט הציבורי (גופים דו-מהותיים), אף אם אינם נכנסים לגדר "גוף ציבורי" כמשמעותו בסעיף 23 לחוק הגנת הפרטיות. לגופים מסוג זה ממליצה הרשות לשקול בכובד ראש מינוי ממונה על הגנת הפרטיות אף אם אינם חבים בכך לפי החוק, וזאת מפני שבעל התפקיד עשוי לסייע בידם לעמוד בדרישות המשפט המנהלי והחוקתי שיש להן זיקה לשמירה על הזכות לפרטיות ולהגנה על מידע אישי (למשל סבירות ומידתיות בקשר לעיבוד מידע).

9.13. יצוין כי לפי פרט 2(4) לתוספת החמישית לחוק, מינוי ממונה הגנה על הפרטיות בארגון שנדרש לכך מכוח סעיפים 17ב1(א)(3) או (4), עשוי לזכות את הארגון בהפחתה בסך 10%, ככל שיוטל עליו עיצום כספי בשל הפרות אחרות של החוק.

<u>הידע והכישורים הנדרשים מן הממונה</u>

10. סעיף 17ב3(א) לחוק קובע כי הממונה על הגנת הפרטיות "**יהיה בעל הידע והכישורים הנדרשים למילוי תפקידו בצורה נאותה**" – כלומר הידע והכישורים הנחוצים למילוי כלל התפקידים המוטלים על הממונה בסעיף 17ב2 לחוק. **זו הדרישה המהותית והכללית שאת תוכנה והיקפה יש לקבוע בכל מקרה לגופו "בשים לב לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו".**

11. לנוכח מהות התפקיד, ראוי שגישתו המקצועית של הממונה תכיר בערך ההגנה על הזכות לפרטיות. הממונה על הגנת הפרטיות נדרש להיות בעל יכולת עבודה בצוות וכושר שכנוע, ובהתאם למהות התפקיד בעל יכולת עבודה והובלת תהליכים מול דרגים בכירים. בארגונים גדולים עשוי הממונה להידרש לכישורי ניהול אם יהיה צוות עובדים שיסייע לו בביצוע תפקידיו. החוק אינו מחייב במפורש את ידיעת השפה העברית, אולם ככלל שליטה בשפת העבודה המקובלת בארגון והשגורה בקרב

נושאי המידע היא חיונית לביצוע אפקטיבי של התפקיד, ובהיעדרה על הארגון לספק לממונה סיוע של כוח אדם ואמצעים נוספים לגישור על פערי השפה. מעבר לכך, מי שאינו דובר עברית יתקשה ממילא לעמוד בתנאי הקבוע בחוק בדבר "ידע מעמיק בדיני הגנת הפרטיות" הישראלים, שלגביו נרחיב בהמשך. דוגמאות אלה כמובן אינן ממצות. על כל ארגון לבחון, בהתאם למאפייניו הספציפיים ובשים לב לאופי עיבוד המידע, נסיבותיו, היקפו ומטרותיו, מהם תחומי הידע והכישורים שבהעדרם תיפגע יכולתו של הממונה לבצע באופן אפקטיבי כל אחד מן התפקידים המוטלים עליו בסעיף 2ב17 לחוק.

12. בלי לגרוע מהדרישה הכללית, סעיף 3ב17(א) לחוק מפרט **תחומי ידע ספציפיים בהם חייב כל ממונה לשלוט** -

12.1. **<u>ידע מעמיק בדיני הגנת הפרטיות</u>**: זהו תחום הידע הבסיסי והחשוב ביותר החיוני לממונה כדי שיוכל למלא את תפקידו בצורה נאותה. על הממונה להיות בעל שליטה מלאה ומקיפה במכלול החקיקה והרגולציה הישראלית בתחום הגנת הפרטיות,[17] הרלוונטית לעיבוד מידע אישי ולהגנה על הפרטיות בישראל, לרבות: חוק הגנת הפרטיות; פסיקת בתי המשפט ובתי הדין לעבודה בסוגיות של הגנת פרטיות; התקנות וההוראות שפורסמו מכוח חוק הגנת הפרטיות; הפרשנות שניתנה להן על ידי הרשות להגנת הפרטיות בהנחיותיה ובשאר מסמכי המדיניות שפרסמה; חקיקה ורגולציה מגזרית בתחום הגנת המידע האישי הרלוונטיים לפעילות הארגון בו מכהן הממונה;[18] וכללי המשפט החוקתי והמנהלי הנוגעים להגנה על הזכות לפרטיות, בארגונים הכפופים למשפט הציבורי.

12.2. על פי רוב, ידע מעמיק בדיני הגנת הפרטיות נרכש באמצעות ניסיון מעשי משמעותי[19] בעיסוק בהיבטים משפטיים או רגולטוריים בתחום הגנת הפרטיות (לרבות ניסיון קודם בתפקיד ממונה על הגנת הפרטיות או ליווי תחום הפרטיות בארגון בפן המשפטי). בנוסף, רצוי שיעבור גם **הכשרה בסיסית לממוני הגנת פרטיות** בטרם כניסתו לתפקיד. לעניין זה, השתלמות תעודה לממוני הגנת פרטיות או השתלמות תעודה בנושא הגנת מידע אישי, מטעם הרשות להגנת הפרטיות או בחסותה, המתקיימות בהיקף של 40 שעות לפחות,[20] ייחשבו ל-"הכשרה בסיסית לממוני הגנת פרטיות". מובן כי ניתן לרכוש ידע מעמיק בדיני הגנת הפרטיות גם בדרכים אחרות, אך בכל מקרה המומחיות **צריכה להיות ניתנת להוכחה**, למשל באמצעות אסמכתאות על לימודים או ניסיון מעשי.

---

[17] חקיקת פרטיות של מדינות זרות, כדוגמת ה-GDPR של האיחוד האירופי, היא לא **דין** בישראל ולכן איננה נכללת "בדיני הגנת הפרטיות" בהם נדרש ידע מעמיק מכל ממונה באופן גורף. עם זאת, היכרות עם משטרי Data Protection מובילים בעולם היא בכל מקרה רצויה ומומלצת בארגונים בעלי פעילות בינלאומית משמעותית, כחלק מחובת **"הידע והכישורים הנדרשים למילוי תפקידו בצורה נאותה"** הנדרשת מכל ממונה מכוח הרישא לסעיף 3ב17(א).

[18] כך לדוגמא, ממונה על הגנת הפרטיות בתאגיד בנקאי ידרש גם לידע מעמיק בחקיקה המסדירה היבטי פרטיות ואבטחת מידע בפעילותם של בנקים, בהוראות ובנהלים של בנק ישראל בתחומים אלו.

[19] תקופת הניסיון המינימאלית הנדרשת תהיה בשים לב למאפייני הארגון וביחס ישר לפוטנציאל הסיכון לפרטיות הכרוך בפעילותו.

[20] לפרטים אודות קורסים לממוני הגנת הפרטיות המתקיימים בחסות הרשות להגנת הפרטיות ראו: https://www.gov.il/he/pages/dpo_course24.

12.3. יודגש שהשתתפות בהשתלמויות הנערכות מטעם הרשות או בחסותה **איננה חובה** לצורך עמידה בתנאים הקבועים בסעיף 17ב3(א) למינוי כממונה על הגנת הפרטיות, ומאידך בפני עצמה היא גם **לא מספיקה** כדי לעמוד בדרישת **הידע המעמיק** בדיני הגנת הפרטיות, אם היא אינה מלווה בניסיון או בהשכלה נוספת כמפורט בסעיף 12.2 לעיל.

12.4. **<u>הבנה הולמת בטכנולוגיה ואבטחת מידע</u>**: 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 האישי שהארגון מבצע והטכנולוגיות המשמשות אותן, לרבות הכרת מחזור חיי המידע וזרימת המידע בארגון ומבנה של המערכות המנהלות והמאחסנות את המידע. הממונה אינו חייב להיות דווקא בעל תואר אקדמי במדעי המחשב או טכנולוגיות מידע או בעל ניסיון מעשי בתחום התוכנה, אם הדבר לא נחוץ למילוי התפקיד בארגון בו הוא מכהן. אולם, לכל הפחות עליו להיות בעל אוריינטציה טכנולוגית ברמה שתיתן בידיו כלים לבחון האם אופן השימוש בטכנולוגיה עומד בדרישות החוק, לקדם הטמעה של עיקרון "העיצוב לפרטיות" (Privacy by Design) בתכנון מערכות הארגון ושימוש בטכנולוגיות מגבירות פרטיות (PETs – Privacy Enhancing Technologies), ולהיות מעורב באופן אפקטיבי בניתוח השלכות השימוש בטכנולוגיות חדשות ובהערכת סיכוני הפרטיות הנובעים מפעילות הארגון (למשל באמצעות ביצוע תסקיר השפעה על הפרטיות). גם הבנתו של הממונה על הגנת הפרטיות **בתחום אבטחת המידע** אינה חייבת לכלול דווקא ניסיון מעשי ספציפי ביישום אמצעי אבטחה, או הסמכות פורמאליות. זאת במיוחד כאשר מדובר בארגון שמכהנים בו בעלי תפקידים אחרים האחראים על אבטחת המידע, לרבות ממונה על אבטחת מידע שמונה לפי סעיף 17ב לחוק, CISO וכדומה.[21] הבנתו של הממונה בהיבטים הטכנולוגיים והתהליכיים של **אבטחת המידע** צריכה להיות ברמה שתיתן בידיו כלים למלא את תפקידיו בארגון באופן הולם, ובכלל זה הבנה של סיכוני האבטחה הכרוכים בפעילות הארגון ושל נאותות הפתרונות המוצעים להם. עם זאת, **בהיבטים המשפטיים והרגולטוריים** של אבטחת המידע כנדבך של דיני הגנת הפרטיות, חייב הממונה להיות בעל ידע **מעמיק**, כמפורט בסעיף 12.1 לעיל.

12.5. **<u>היכרות עם תחומי פעילותו של הארגון ומטרותיו</u>**: הממונה על הגנת הפרטיות נדרש להכיר את ייעודו של הארגון ותחומי העיסוק שלו; המבנה התאגידי; חלוקת תחומי האחריות ותהליכי העבודה הנהוגים בו, **בדגש על תהליכי עיבוד מידע**; המגזר או השוק במסגרתו הארגון פועל ועיקרי הרגולציה המגזרית (מעבר לרגולציית הפרטיות הייחודית למגזר); גופים אחרים איתם מקיים הארגון שיתוף פעולה עסקי או אחר; ומאפייני נושאי המידע עליהם הארגון אוסף ומעבד מידע, בדגש על אוכלוסיות מיוחדות (למשל קטינים, אזרחים ותיקים, בעלי צרכים מיוחדים, עולים חדשים). ההיכרות עם תחומי פעילות הארגון יכולה לנבוע למשל מעבודה קודמת בתפקיד אחר בארגון עצמו, מניסיון מעשי בארגונים אחרים באותו מגזר או בתחומים המשיקים באופן ממשי לפעילותו או מלימוד יזום של תחום התוכן בו עוסק הארגון, ועליה

[21] תפקידיו של ממונה על אבטחת המידע בארגון (לרבות CISO) קבועים בתקנה 3 לתקנות אבטחת מידע, וזאת בין אם חלה חובה חוקית למנותו לפי סעיף 17ב(א) לחוק, ובין אם מונה באופן וולונטרי.

להיות ברמה שתאפשר לממונה לזהות סיכונים פוטנציאליים בתחום הפרטיות, להתאים את מדיניות עיבוד המידע לצרכים הייחודיים של הגוף, וליישם ביעילות את החוק, התקנות ועקרונות הגנת הפרטיות בתהליכי העבודה.

<u>ייעוד הממונה על הגנת הפרטיות ותפקידיו</u>

13. ייעודו של הממונה על הגנת הפרטיות, כפי שנקבע ברישא לסעיף 17ב2(א) לחוק, הוא להבטיח את קיום הוראות החוק בארגון, וגם **לפעול לקידום ושיפור ההגנה על הפרטיות ואבטחת המידע גם מעבר למינימום הקבוע בדין**. כלומר, עליו לשאוף לצמצום הפגיעה בפרטיות הכרוכה בפעילות הארגון, גם אם ביצוע הפגיעה אינו אסור לפי דין. לצורך כך, תפקיד מרכזי של הממונה הוא להביא **להפנמה של "תרבות פרטיות" בארגון ושל עקרונות ושיקולי פרטיות בכל תהליכי העבודה הנוגעים למידע אישי ולמערכות המידע בארגון**, תוך הטמעה של תפיסת **"עיצוב לפרטיות" (Privacy by Design)**[22] ושל **טכנולוגיות מגבירות פרטיות (PETs)**,[23] ככל שיש בהן רלוונטיות לפעילות הארגון. גם עריכת **תסקיר השפעה על הפרטיות** היא כלי ראשון במעלה לשמירה מיטבית על הפרטיות בארגון, ומומלץ לכל ממונה על הגנת הפרטיות לקדם את השימוש בו ולהוביל או להיות מעורב באופן משמעותי בביצועו.[24]

14. הממונה על הגנת הפרטיות הוא שחקן מפתח במערך משילות המידע בארגון (Data Governance), ואת תפקידו אפשר לתאר **כמתאם של תהליכי הציות** (Compliance) לא רק **לדרישות המתחייבות** מלשונם של דיני הגנת הפרטיות, אלא **גם לפרקטיקות הרצויות** (Best Practices) הנובעת מרוחו של הדין ומן הרציונאלים העומדים בבסיסו. חוק הגנת הפרטיות אינו מטיל על הממונה אחריות אישית במקרה של אי-ציות להוראותיו, ועיקר שליחותו היא בתחומי הייעוץ, ההדרכה, הפיקוח והבקרה.

15. סעיף 17ב2(א) לחוק קובע **שתפקיד הממונה על הגנת הפרטיות כולל בין השאר גם את כל המשימות הבאות**:

15.1. **סמכות מקצועית וייעוץ**:[25] הממונה ישמש מוקד ידע וייעץ להנהלת הגוף ולעובדיו בשני הנדבכים של תפקידו: הן בהוראות המחייבות של דיני הפרטיות והן בעקרונות לקידום השמירה על הפרטיות החורגים מהוראות הדין. לשם כך מצופה מהממונה **לנקוט גישה פרואקטיבית ולהציע את סיועו באופן יזום, נגיש וזמין** לכל המחלקות הרלבנטיות ולאורך כל שלבי מחזור החיים של עיבוד המידע האישי בארגון, החל מקבלת החלטות מדיניות ברמת ההנהלה, דרך תכנון מערכות המידע ובנייתן "ברצפת היצור", מעורבות בהחלטות על שדרוג ורכישה של מערכות מידע חדשות בארגון, איסוף המידע, עיבודו בארגון, וכלה בהעברתו לצדדים שלישיים או ביעורו. חוק הגנת הפרטיות אמנם לא **מחייב** את הארגון לנהוג לפי חוות

---

[22] להרחבה על תפיסת "עיצוב לפרטיות" ראו אתר הרשות: https://www.gov.il/he/pages/privacy_by_design.
[23] להרחבה ראו מדריך לטכנולוגיות מגבירות פרטיותPETs שפרסמה הרשות בפברואר 2025.
[24] להרחבה ראו מדריך עזר מתודולוגי לעריכת תסקיר השפעה על הפרטיות (2022), שפרסמה הרשות.
[25] סעיף 17ב2(א)(1) לחוק.

דעתו של הממונה על הגנת הפרטיות, אולם מאחר שסעיף 17ב2(א)(1) לחוק קובע שהממונה על הגנת הפרטיות "ישמש **סמכות מקצועית**" בתחומי פעילותו, **הרי שיש לשקול את עמדתו בכובד ראש, לנמק החלטה שלא לאמץ אותה, ולנהוג בה כבחוות דעתו של גורם שיש חובת היוועצות עמו**. כידוע, בארגונים רבים היועץ המשפטי הוא המכריע בשאלות משפטיות, וגם בענייני אבטחת מידע או הגנת סייבר עשויים להיות גורמים אחרים האחראים לאבטחת המידע בארגון,[26] או מוסמכים להנחות את הארגון בתחומים אלו.[27] הרשות סבורה כי על מנת שהממונה על הגנת הפרטיות יוכל להצליח במילוי תפקידו, עליו לקיים שיח שוטף עם הגורמים הללו, להיוועץ בהם, ולפעול בשיתוף פעולה מלא איתם.

15.2. **הדרכה**:[28] החוק דורש שהממונה יכין תכנית הדרכה ויפקח על ביצועה. בהתאם לגודל הארגון ופריסתו, רצוי ככל הניתן שהממונה הוא שידריך את העובדים בעצמו. מטרת ההדרכה היא להעלות את מודעות ההנהלה וכלל העובדים לחובותיהם על פי דין ולחשיבות השמירה על פרטיות המידע האישי, ולצייד אותם בכלים מעשיים לציות להוראות החוק ולהתמודדות עם אתגרי הפרטיות. את תוכן תכנית ההדרכה ומתכונתה יש להתאים למאפייני הארגון והעובדים, לתחומי פעילותו וסיכוני הפרטיות הייחודיים לו, ואפשר לכלול בה גם את ההדרכות הנדרשות בתקנה 7 לתקנות אבטחת המידע.[29] תוכנית הדרכה עשויה לכלול סדנאות, קורסים מקוונים, לומדות אינטראקטיביות, הדרכות פרונטליות, תרגילים לבחינת ערנות, הפצת עלונים, תליית פוסטרים במתחם ועוד, בהתאם לצרכי הארגון ומאפייניו.

15.3. **בקרה שוטפת על העמידה בהוראות החוק**:[30] הממונה על הגנת הפרטיות נדרש להכין תוכנית לבקרה שוטפת על העמידה בהוראות החוק, לכל הפחות **לוודא** את ביצועה (אם כי רצוי שיהיה גם מעורב בביצוע שלה בפועל), ולדווח להנהלת הארגון על ממצאיו והמלצותיו לתיקון ליקויים. בקרה היא תהליך שוטף ומתמשך שמטרתו מניעת הפרות ושיפור תהליכים תוך כדי התרחשותם. רצוי שתוכנית הבקרה תהיה שנתית ושגם הדיווח להנהלה ייעשה לפחות אחת לשנה, אלא אם ממצאי היישום שלה יצביעו על צורך בתכיפות גבוהה יותר. יצוין שבארגונים בהם חלה חובה למנות ממונה על אבטחת מידע,[31] **הכנת תכנית בקרה שוטפת על העמידה בתקנות אבטחת המידע היא אחד מתפקידיו של ממונה אבטחת המידע**, ולפי תקנה 3(3) לתקנות אלו הוא גם מי שנדרש לבצע אותה ולדווח להנהלה על ממצאיו.

---

[26] כגון בגופים המחויבים במינוי ממונה אבטחת מידע לפי סעיף 17ב לחוק הגנת הפרטיות.
[27] כגון בגופים המנויים בתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998.
[28] סעיף 17ב2(א)(1) לחוק.
[29] תקנה 7(ג) לתקנות אבטחת המידע קובעת כי "במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור תיערך אחת לשנתיים לפחות, ולגבי הסמכה של בעל הרשאה לתפקיד חדש – סמוך ככל האפשר למועד תחילת הסמכתו."
[30] סעיף 17ב2(א)(2) לחוק.
[31] לפי הנדרש בסעיף 17ב לחוק.

15.4. **נוהל אבטחת המידע ומסמך הגדרות המאגר**:[32] בהתאם לחוק, הממונה על הגנת הפרטיות נדרש לכל הפחות **לוודא** כי הארגון ערך נוהל אבטחת מידע ומסמך הגדרות מאגר בהתאם לכלל הדרישות על פי תקנות 2 ו-4 לתקנות אבטחת המידע, ושאלו אושרו בידי הנהלת הארגון, על דעת הדירקטוריון.[33] עם זאת לאור חשיבותו הרבה של מסמך הגדרות המאגר, שבאה לביטוי גם בדרישה למעורבות הדירקטוריון בתהליך אישורו ובחובה למסור עותק ממנו לרשות להגנת הפרטיות, במסגרת חובת ההודעה לרשות על מאגר שבו מידע בעל רגישות מיוחדת על מעל 100 אלף נושאי מידע[34] - רצוי שהממונה ייקח חלק פעיל יותר בהכנת המסמך ובעדכונו. בכל הנוגע לנוהל אבטחת המידע, כאשר קיים בארגון ממונה אבטחת מידע, הוא שאחראי להכין את נוהל האבטחה ולהביאו לאישור האורגנים המוסמכים.[35] אולם בארגון שבו אין ממונה על אבטחת מידע, רצוי שהממונה על הגנת הפרטיות יפגין מעורבות גדולה יותר גם בהכנתו של הנוהל האמור.

15.5. **טיפול בפניות ובקשות של נושאי מידע**:[36] הממונה על הגנת הפרטיות נדרש לוודא טיפול בכל פניה של נושא מידע הנוגעת לעיבוד מידע אודותיו בארגון, לרבות בקשות למימוש זכויות אישיות הנתונות להם לפי החוק: כגון בקשות לעיון במידע אישי, לתיקונו או למחיקתו,[37] בקשות להימחק ממאגר המשמש לדיוור ישיר או להגביל מסירת מידע ממאגר המשמש לשירותי דיוור ישיר,[38] או בקשות למחיקת מידע ממאגר הכולל מידע שהועבר מהאזור הכלכלי האירופי.[39] על הממונה לדאוג לכך שהבקשות ושאר הפניות יקבלו מענה מקצועי ועניינים בהתאם לדרישות החוק ובמסגרת הזמן שנקבעה בדין, או תוך זמן סביר. רצוי שהממונה יטפל או ירכז בעצמו את הטיפול בפניות ובבקשות נושאי המידע. בהתאם לדרישת החוק, על הארגון לפרסם לציבור באופן נגיש ופשוט[40] את דרכי ההתקשרות עם הממונה, ורצוי שאלה יכללו כתובת דוא"ל, מספר טלפון לשיחות ולהודעות ווטסאפ, ומען למשלוח דואר פיזי.

15.6. **הממונה ישמש איש הקשר של הארגון עם הרשות להגנת הפרטיות**:[41] המשמעות היא שהרשות יכולה (אך אינה חייבת) לפנות אל הממונה או לנהל עמו שיח בכל עניין הקשור להגנת מידע אישי בארגון בו הוא מכהן. כל פניה של הרשות אל הממונה או תקשורת איתו כמוה כפניה לגורמים המוסמכים והרלוונטיים בארגון או כתקשורת עימם. גם במקרים בהם הארגון הוא שפונה לרשות, הפניה אינה חייבת להישלח דווקא מאת הממונה, אבל לכל הפחות על הממונה

---

[32] סעיף 17ב2(א)(3) לחוק.
[33] לעניין החובה לקיים דיון בדירקטוריון בעקרונות המרכזיים של נוהל אבטחת המידע הארגוני ובמסמך הגדרות המאגר, ראו סעיף 10 להנחיית הרשות להגנת הפרטיות מס' 1/2024 "תפקיד הדירקטוריון בקיום חובות התאגיד לפי תקנות הגנת הפרטיות (אבטחת מידע)". זאת, בכל הנוגע לארגונים שעליהם חלה ההנחיה האמורה, כאמור בסעיף 8 להנחיה.
[34] כנדרש בסעיף 8א(ב) לחוק.
[35] תקנה 3(2) לתקנות אבטחת המידע.
[36] סעיף 17ב2(א)(4) לחוק.
[37] לפי סעיפים 14-13 לחוק.
[38] לפי סעיפים 17ו(ב)-(ג) לחוק; להרחבה ראו: הנחיית הרשות להגנת הפרטיות מס' 2/2017 "פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר".
[39] בהתאם לתקנה 3(א) לתקנות הגנת הפרטיות (הוראות לעניין מידע שהועבר לישראל מהאזור הכלכלי האירופי), תשפ"ג-2023.
[40] סעיף 17ב2(א)(4) לחוק. כגון פרסום באתר האינטרנט של הארגון, במדיניות הפרטיות ובערוצי תקשורת רלוונטיים נוספים, במטרה להקל על הציבור בפנייה ובקבלת מענה.
[41] סעיף 17ב2(א)(5) לחוק.

להיות מכותב להתכתבות או מזומן לפגישות עם הרשות, אם ישנן. הרשות עשויה בנסיבות מסוימות לדרוש עמדה של הממונה טרם מתן מענה לפניה של הארגון או לבקשה לקבלת חוות דעת מקדמית.[42] הרשות ממליצה לכל ממונה על הגנת הפרטיות לעדכן אותה בפרטי ההתקשרות עמו ולציין את הארגון בו מונה לכהן. כמו כן, דיווח לרשות על זהות הממונה על הגנת הפרטיות ופרטי ההתקשרות עמו הוא חובה במסגרת הודעה לרשות על ניהול מאגר הכולל מידע בעל רגישות מיוחדת על 100 אלף נושאי מידע או יותר,[43] ובמסגרת בקשה לרישום מאגר,[44] והחוק אף מחייב לעדכן את הרשות כאשר חל שינוי בפרטים אלו.[45] החוק לא מטיל על הממונה חובה אישית לדווח לרשות על הפרות שבוצעו בארגון בו הוא מכהן. במקרה של דיווח לרשות להגנת הפרטיות על אירוע אבטחה חמור, בהתאם לחובה המוטלת על הארגון לפי תקנה 11(ד)(1) לתקנות אבטחת המידע, הממונה אינו חייב לבצע את הדיווח בעצמו, אך עליו להיות מעורב בתהליך הדיווח ולוודא שהוא מבוצע באופן התואם את דרישות הדין.

15.7. רצוי כי הממונה יהיה מעורב באופן משמעותי גם בטיפול במקרים של "אירוע אבטחה חמור" כהגדרתו בתקנה 1 לתקנות אבטחת המידע, אף מעבר ליישום חובת הדיווח הראשוני לרשות. בין השאר לעניין הערכת הסיכונים והנזק שנגרם, האמצעים להתמודדות עם האירוע, בחינת הצורך בעדכון נושאי המידע ותוכן ההודעה שתישלח אליהם.

<u>מתכונת העסקתו של הממונה והיקפה</u>

16. החוק מתיר להעסיק את הממונה גם במתכונת של נותן שירותים חיצוני, שאיננו עובד שכיר של הארגון.[46] **אופטימאלית רצוי שהממונה יהיה עובד הארגון** וחלק אינטגרלי מן הארגון, באופן שיאפשר לו היכרות מעמיקה ואינטימית עם מבנה הארגון, תחומי פעילותו ותרבותו הארגונית, כמו גם זמינות ונגישות בלתי אמצעית לעובדים ולמנהלים – כולם יתרונות חשובים אשר יגבירו את יכולת ההשפעה של הממונה בתוך הארגון ויעצימו את יכולתו לבצע את תפקידו באופן מיטבי.

17. **מתכונת ההעסקה והיקף המשרה שתוקצה לממונה (פנימי או חיצוני) צריכים להיבחן לגופו של כל ארגון בהתאם למאפייניו הספציפיים. אולם, בין אם הממונה הוא עובד הארגון או נותן שירותים חיצוני, יש להבטיח כי הוא יוכל להקדיש את הזמן הדרוש למילוי נאות של תפקידו, ולקיים את שאר דרישות החוק לגבי הממונה ואופן העסקתו, לרבות החובה המפורשת בחוק לספק לו את התנאים והמשאבים הדרושים למילוי נאות של תפקידו, לוודא כי הוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות, ולהבטיח כי לא יוטל עליו תפקיד נוסף או כפיפות לנושא משרה אשר עלולים להעמידו בחשש לניגוד עניינים**. על מתכונת ההעסקה (פנימי או מיקור חוץ) ועל היקף המשרה (מלאה או חלקית) להתאים לתפקידים ולתחומי האחריות של הממונה ולהיקבע בשים לב

---

[42] לפי סעיף 17ט2 לחוק.
[43] בהתאם לסעיף 8א(ב)(1) לחוק.
[44] סעיף 9(ב)(1) לחוק.
[45] לעניין מסירת הודעה לרשות על מאגרים גדולים בהם מידע בעל רגישות מיוחדת, חובת העדכון קבועה בסעיף 8א(ב)(2) לחוק. לעניין מאגרים שחלה עליהם חובת הרישום, חובת העדכון קבועה בסעיף 9(ד) לחוק.
[46] סעיף 17ב3(ב) לחוק.

לגודלו של הגוף בו הוא ממלא את תפקידו, להיקף ורגישות המידע המעובד בידי הגוף ולנסיבות נוספות המלמדות על מורכבות תפקיד הממונה באותו הגוף.

18. רק יחיד (אדם טבעי) יכול להתמנות בידי ארגון לכהונת ממונה על הגנת הפרטיות בו, בין אם מדובר בעובד הארגון או בנותן שירותים חיצוני, אם כי אין מניעה שהתקשרותו עם הארגון תתבצע באמצעות חברה בה הוא מועסק. אין בחוק חובה מפורשת שהממונה יהיה אזרח או תושב ישראל, אולם עליו להיות זמין ונגיש גם באופן פיזי בארגון ככל הנדרש לביצוע נאות של תפקידיו, בהתאם למאפייני הארגון בו הוא מכהן, מתכונת העבודה בו וצרכיו הקונקרטיים.

<u>מעמד הממונה, מקומו בארגון והמשאבים והאמצעים שיש להקצות לו</u>

19. חלק זה של המסמך סוקר את הוראות החוק בעניין מעמדו ומקומו של הממונה בארגון והמשאבים והאמצעים שיש לספק לו. הן נועדו לתת בידי הממונה את הכלים והאמצעים **למלא באופן מיטבי את ייעודו, במטרה לחזק את יכולתו לגבש את עמדותיו באופן עצמאי** ולצמצם השפעות חיצוניות ושיקולים שלא ממין העניין, **ולפי תכלית זו יש לפרש אותן**.

20. בהתאם לחוק, הארגון **נדרש לספק לממונה "את התנאים והמשאבים הדרושים למילוי נאות של תפקידו" ולוודא שהוא "מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות"**.[47] בהתאם לגודל הארגון, אופי פעילותו ורגישות והיקף עיבוד המידע, עשויה דרישה זו להתייחס בין השאר למשאבים ולתנאים הבאים: היקף המשרה ודרגת השכר של הממונה, גיוס צוות מקצועי שיסייע לממונה, גובה תקציב הפעילות של הממונה כולל בקרה והדרכה, שימור ועדכון הידע המקצועי של הממונה באמצעות השתתפותו בהשתלמויות, כנסים וכדומה. כמו כן יש לאפשר לממונה גישה לכל המסמכים, המידע והמערכות הטכנולוגיות הדרושים לו באופן סביר במסגרת מילוי תפקידו, וכן ליידע אותו מבעוד מועד על כל עניין שיש לו השלכה מהותית על הגנת המידע האישי בארגון, ולשתף אותו בדיונים ותכתובות העוסקים בשאלות מהותיות של איסוף וניהול המידע האישי בארגון.

21. כדי שיוכל להשפיע באופן אפקטיבי על תהליכים בארגון וכאינדיקציה לחשיבות התפקיד, החוק מתייחס גם לסוגיית מקומו של הממונה בהיררכיה הבכירה בארגון וקובע כי **הממונה ידווח ישירות למנכ"ל או לגורם הכפוף למנכ"ל במישרין**.[48] מעבר לדרישה זו, לא נוקט החוק עמדה לגבי זהות האגף או המחלקה בהם יש למקם את הממונה. **לפיכך, בכפוף לדרישה האמורה, לאיסור על הימצאות הממונה במצב של חשש לניגוד עניינים, ולחובה לספק לו את התנאים והמשאבים הנאותים** – רשאי למעשה כל ארגון להחליט על מיקום הממונה במבנה הארגוני לפי שיקול דעתו ובהתאם לצרכיו. הצבתו של הממונה בייעוץ המשפטי של הארגון היא אפשרית (ככל שאינה מביאה למצב של ניגוד עניינים), אולם לא בהכרח תאפשר להפיק ממנו את התועלת המיטבית, בשל ההבדל המהותי בין תפקיד היועץ המשפטי לבין תפקידו של הממונה (הבטחת הציות לחוק, לעומת קידום

[47] סעיף 17ב2(ב) לחוק.
[48] סעיף 17ב2(ג) לחוק.

השמירה על הפרטיות אל מעבר למינימום המתחייב מהדין), והשוני המסוים בידע והכישורים הנדרשים לביצועו.

22. **ניגוד עניינים**: סעיף 17ב3(ג) לחוק קובע כי "**הממונה על הגנת הפרטיות לא ימלא תפקיד נוסף ולא יהיה כפוף לנושא משרה בגוף שבו הוא ממלא את תפקידו או בגוף אחר, אם מילוי התפקיד או הכפיפות כאמור עלולים להעמידו בחשש לניגוד עניינים במילוי תפקידיו לפי חוק זה**". איסור זה נועד לחזק את עצמאות שיקול הדעת של הממונה בביצוע תפקידו, ולצמצם השפעות ושיקולים מתנגשים או שלא ממין העניין לייעודו של הממונה לקדם את השמירה על הפרטיות בארגון. לכן, בראש ובראשונה, **הממונה אינו יכול למלא תפקידים (או להיות כפוף לבעלי תפקידים) הכוללים את הסמכות או האחריות לקבוע מדיניות בעניין עיבוד המידע האישי בארגון, לרבות קביעת מטרות העיבוד וקבלת החלטות מהותיות לגבי שיטות ואמצעי העיבוד**. 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. למען הסר ספק יובהר, כי האיסור על הימצאות בחשש לניגוד עניינים רלוונטי הן לממונה שהוא עובד הארגון במקרים בהם היקף משרתו וצרכי הארגון מאפשרים להטיל עליו תפקיד נוסף, והן על ממונה המועסק כנותן שירות חיצוני.

23. יצוין, כי חוק הגנת הפרטיות אינו מטיל על הממונה חובה אישית לדווח לרשות **באופן יזום** על הפרות שביצע הארגון. אולם לאור תפקידו המרכזי של הממונה במערך הציות לחוק, ובהיותו איש הקשר הסטטוטורי עם הרשות, חוות הדעת שניתנו על ידי הממונה במסגרת תפקידו בארגון עשויות להתבקש במסגרת פעילות הרשות להגנת הפרטיות.

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

24. 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.

25. 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. זאת בין השאר מהטעמים הבאים:

25.1. ראשית, לפי הוראת סעיף 17ב3(א) לחוק, על הממונה על הגנת הפרטיות, בין אם מדובר בתפקידו היחיד ובין אם הוא אמור לשאת בתפקידים נוספים, לעמוד בדרישות הידע והכישורים הנדרשים למילוי תפקידו בצורה נאותה. בהתאם להוראות החוק, עמידה בדרישות אלו תיבחן גם בהתחשב באופי עיבוד המידע האישי בארגון, נסיבותיו, היקפו ומטרותיו של

מאגר המידע הארגוני. 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, הקבועות בסעיף 17ב3(א) לחוק, 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.

25.2. שנית, כאמור סעיף 17ב3(ג) לחוק קובע כי הממונה על הגנת הפרטיות לא ימלא תפקיד נוסף ולא יהיה כפוף לנושא משרה, אם התפקיד או הכפיפות עלולים להעמידו בחשש לניגוד עניינים במילוי תפקידו על פי החוק. הוראה דומה קיימת ביחס לממונה אבטחת המידע הארגוני, בתקנה 3(4) לתקנות אבטחת המידע. לצד החפיפה הרחבה בתכליות ובתוכן של האינטרסים עליהם אמונים ממונה הגנת הפרטיות וממונה אבטחת המידע, קיים ביניהם גם שוני העשוי להביא להתנגשות. כך למשל נקיטת אמצעים מסוימים לשיפור אבטחת המידע (כגון ניטור מסיבי של פעילות העובדים או הלקוחות במערכת המידע הארגונית) עשויה לפגוע באופן משמעותי בפרטיות נושאי המידע ולסתור עקרונות פרטיות מקובלים, גם אם התכלית של ניטור כאמור נועדה בסופו של דבר להגנה על המידע והפרטיות. לפיכך, ממונה אבטחת המידע לא יוכל למלא במקביל גם את תפקיד ממונה הגנת הפרטיות בארגון, אלא רק אם יש באפשרותו לאזן בין התפקידים בצורה נאותה, ומבלי שתיפגע יכולתו למלא כל אחד מהם כראוי. בארגונים החייבים במינוי ממונה אבטחת מידע מכוח סעיף 17ב(א) לחוק, יקשה לכאורה על ממונה האבטחה לאזן בצורה נאותה בין התפקידים, מפני שסעיף 17ב(ב) לחוק מטיל עליו אחריות אישית לאבטחת המידע בארגון. אחריות דומה איננה מוטלת במישרין על מי שנושא בתפקיד הממונה על הגנת הפרטיות, ועובדה זו כשלעצמה עלולה להשליך על מערך השיקולים במקרים של התנגשות בין שני תחומי האחריות.

25.3. שלישית, סעיף 17ב2(ג) לחוק מחייב שהממונה על הגנת הפרטיות ידווח ישירות למנכ"ל הארגון, או לעובד הכפוף במישרין למנכ"ל. ממונה אבטחת המידע הארגוני לא בהכרח יעמוד בדרישה זו של בכירות ודיווח ישיר.

25.4. 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 את דרישת סעיף 17ב2(ב) לחוק, כי הארגון יספק לממונה על הגנת הפרטיות את "התנאים והמשאבים הדרושים למילוי נאות של תפקידו ויוודא כי הוא מעורב כראוי בכל נושא הנוגע לדיני הגנת הפרטיות". יודגש, כי הוראה דומה במהותה קיימת גם ביחס לממונה אבטחת המידע הארגוני, בתקנה 3(6) לתקנות אבטחת מידע.

26. בכוונת הרשות להשתמש בסמכויותיה על מנת לוודא כי מינויו של ממונה הגנת הפרטיות בארגונים השונים נעשה בהתאם לקריטריונים הקבועים בחוק וכי מדובר בבעל תפקיד המחזיק בידע מעמיק בהיבטים המשפטיים והרגולטורים של דיני הגנת הפרטיות - שכאמור, אינם מתמצים בידע בתחום אבטחת המידע.

27. במקרים של ספק, ניתן לפנות לרשות להגנת הפרטיות בשאלות הנוגעות ליישום האמור בגילוי הדעת.