29 אוקטובר, 2020
י"א חשון, תשפ"א

מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו

1. תקציר

מסמך זה נועד להבהיר את עמדת הרשות להגנת הפרטיות לפיה, על מנת להבטיח עמידה בהוראות דיני ההגנה על מידע אישי בישראל, מומלץ למנות ממונה הגנה על הפרטיות (להלן – **הממונה**), שיופקד על יישום דיני ההגנה על מידע אישי בארגון. תפקידו המרכזי של הממונה הוא להביא להפנמה של עקרונות ושיקולי פרטיות בתהליכי העבודה בארגון, ולסייע לארגון במימוש אחריותו וחובותיו לפי דיני הגנת הפרטיות. כדי שיוכל למלא באופן מיטבי את תפקידיו והמשימות המוטלות עליו, מומלץ כי הממונה יהיה חלק מההנהלה הבכירה של הארגון.

2. רקע

כיום, הדין בישראל אינו כולל חובה כללית למינוי בעל תפקיד בארגון שיהא אמון על הגנה על הפרטיות. זאת, למעט בחוק נתוני אשראי הקובע כי הנגיד ימנה ממונה על הגנת הפרטיות, אשר יהיה עובד בנק ישראל.[1] למרות זאת, סבורה הרשות כי מינויו של ממונה הגנת פרטיות **באופן וולונטארי** מהווה פרקטיקה ראויה ומומלצת (**Best Practice**) לארגונים האוספים ומעבדים מידע אישי. פרקטיקה זו נושאת בחובה יתרונות רבים, הן לארגון הן לנושאי המידע. מינוי ממונה הגנה על הפרטיות מסייע לארגון לוודא כי הוא עומד בהוראות דיני ההגנה על מידע אישי בישראל, מהווה אינדיקציה כי הארגון נקט ונוקט צעדים לצמצום הסיכון לפגיעה במידע האישי הנשמר ברשותו, וכן מאפשר שיתוף פעולה מיטבי עם הרשות להגנת הפרטיות.

ממונה הגנת הפרטיות יכול שיהיה מינוי פנימי, עובד החברה, או מינוי חיצוני לחברה. היה ומדובר במינוי פנימי, יש לוודא כי העובד אינו נתון לניגוד עניינים עקב תפקיד אחר שהוא ממלא בארגון. ככל שמדובר בארגון גדול, או כאשר ליבת העיסוק של הארגון כרוכה בעיבוד מידע אישי, או במקרים בהם מעובד מידע אישי בקנה מידה רחב, ראוי כי ממונה הגנת הפרטיות יהיה מינוי פנימי ובעל תפקיד בכיר בארגון. ככל שמדובר בארגון בינוני או קטן, שליבת עיסוקו אינה כרוכה בעיבוד מידע אישי, קיימת אפשרות למנות ממונה חיצוני, שאינו עובד הארגון.

[1] סעיף 18 לחוק נתוני אשראי, התשע"ו-2016.

מינוי ממונה הגנה על הפרטיות נהוג במקומות שונים בעולם. באירופה, החובה למנות ממונה (**DPO**) קבועה ברגולציית הגנת המידע של האיחוד האירופי (**GDPR**).[2] מינוי ממונה הגנה על הפרטיות מחויב בכל ארגון הכפוף ל-GDPR, בנסיבות המפורטות בה. בין היתר כאשר עיבוד המידע מתבצע על ידי גוף ציבורי;[3] כאשר ליבת העיסוק של הארגון כוללת פעולות עיבוד מידע אישי אשר מתוקף טיבן, היקפן או מטרותיהן, מחייבות ניטור שיטתי של נושאי מידע בהיקף רחב;[4] או במקרים בהם ליבת העיסוק של הארגון כוללת פעולות עיבוד מידע אישי רגיש בהיקף רחב.[5]

על פי ה-GDPR, ממונה ההגנה על הפרטיות נדרש להיות בעל מומחיות בדינים ובנהלים העוסקים בהגנה על מידע אישי. משימותיו כוללות ייעוץ בנוגע ליישום החובות המוטלות ב-GDPR ובחוקים אחרים של האיחוד האירופי או של המדינה הרלוונטית, בנושא הגנה על מידע אישי; פיקוח על ציות הארגון לרגולציה בנושא הגנה על מידע אישי ועל מדיניות הארגון בנושא; הקצאת אחריות לבעלי התפקידים הרלוונטיים, העלאת מודעות והדרכת העובדים; ייעוץ ופיקוח על תהליך גיבוש תסקיר השפעה על פרטיות בארגון; ושיתוף פעולה עם הרשות המאסדרת[6].

לאור תחולתה האקס-טריטוריאלית של הרגולציה האירופית, ובשל העובדה כי ה-GDPR משמשת מקור השראה לחקיקת פרטיות במדינות רבות – מינוי ממונה הגנת פרטיות עשוי להיות ממילא חובה חוקית ישירה בארגון ישראלי הכפוף לרגולציה זרה, ומכל מקום תקל עליו לנהל עסקים בשיטות משפט אחרות בעולם.

כך למשל, החוק החדש להגנה על מידע אישי **בברזיל (LGPD)** [7] קובע כי על בעל מאגר מידע למנות קצין הגנה על מידע אישי, שיהיה אחראי על עיבוד מידע אישי בארגון, בדומה לתפקידו של ה-**DPO** הקבוע ב-GDPR. תפקידיו של קצין הגנה על מידע אישי כוללים, בין היתר, טיפול בפניות מנושאי המידע והטמעת אמצעים להתמודדות עמן; טיפול בפניות מהרשות המאסדרת, והטמעת אמצעים להתמודדות עמן; והדרכת עובדי הארגון והמחזיקים בנוגע לטיפול במידע אישי[8].

---

[2] לעיון ברגולציה של האיחוד האירופי

[3] סעיף 37 (1) (a) ל-General Data Protection Regulation (GDPR).

[4] סעיף 37 (1) (b) ל-General Data Protection Regulation (GDPR).

[5] סעיף 37 (1) (c) ל-General Data Protection Regulation (GDPR).

[6] סעיף 39 ל-General Data Protection Regulation (GDPR).

[7] נכנס לתוקפו ביום 19.8.20, תוך שנקבע כי אכיפתו תחל ביום 1.8.21. ניתן לזהות מספר רב של קווי דמיון בין רגולציית ה- GDPR ובין החוק הברזילאי החדש.

[8] סעיף 41 ל - LGPD.

בארה"ב, מלבד הגופים הכפופים ל-"**HIPAA**" (Health Insurance Portability and Accountability Act)[9] – חקיקה פדראלית בנושא העברת מידע רפואי, לא קיימת דרישה כללית למנות ממונה הגנה על הפרטיות. עם זאת, מינוי ממונה הגנה על הפרטיות נחשב כפרקטיקה ראויה ומומלצת (**Best Practice**) בקרב ארגונים גדולים, ולאחרונה אף בקרב ארגונים בינוניים בגודלם.

תפקידיו של הממונה, אשר בארה"ב נהוג לכנותו Chief Privacy Officer (**CPO**) כוללים, בין היתר, ניהול מדיניות ונהלי הארגון בנוגע להגנה על מידע אישי; העלאת מודעות והדרכה בנושא הגנה על מידע אישי בקרב עובדי הארגון; טיפול באירועים הנוגעים להפרה של דיני ההגנה על מידע אישי; הצבת יעדים; תכנון בקרות; הערכת סיכונים הנוגעים לפרטיות; ניהול תהליך ביצוע תסקיר השפעה על פרטיות; פיקוח על האמצעים שנבחרו לצמצום הסיכונים לפרטיות; וציות.[10]

3. <u>תפקידיו של ממונה ההגנה על הפרטיות</u>

היקף תפקידו של הממונה ייקבע על פי מורכבות פעולות עיבוד הנתונים המתבצעות בארגון וגודל הארגון. אלו בין היתר התפקידים והמשימות שמומלץ להטיל על הממונה:

1. <u>הסדרת תהליכי ניהול מידע</u>:

1.1. הממונה ינסח את מדיניות הפרטיות של הארגון ויביא אותה לאישור ההנהלה הבכירה.

1.2. הממונה יהיה מעורב לאורך כל מחזור החיים של תהליכי עיבוד מידע בארגון, על מנת לוודא שפעילות עיבוד המידע מבוצעת באופן המפחית ככל הניתן את הסיכונים לפרטיות נושאי המידע.

1.3. הממונה יהיה מעורב בעיצוב מערכות המידע של הארגון ובתהליכים הקשורים בהן, על מנת לוודא, ככל הניתן מראש, כי מערכות המידע בנויות באופן שיפחית את הסיכון לפגיעה בפרטיותם של נושאי המידע (תפיסת "עיצוב לפרטיות" (**Privacy By Design**) ותפיסת "פרטיות כברירת מחדל" (**Privacy by Default**)).[11]

1.4. הממונה יבדוק את הנהלים ומדיניות הארגון בתחום הפרטיות, ואת עמידתם בהוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן – **חוק הגנת הפרטיות**) וכן יבצע מעקב, בקרה, ועדכון של הנהלים במידת הצורך.

---

[9] <u>the HIPPA privacy rule</u>.

[10] להרחבה, ראו תיאור תפקיד CPO באתר האגודה האמריקנית לניהול מידע רפואי (AHIMA):
<u>"Sample (Chief) Privacy Officer Job Description"</u>.
ראו תיאור התפקיד גם באתר המכון הטכנולוגי של פלורידה (Florida Institute of Technology):
<u>"Chief Privacy Officer Career Guide"</u>.

[11] בנושא תפיסת "עיצוב לפרטיות", ראו סקירה קצרה באתר הרשות להגנת הפרטיות: <u>מאמר - סקירה לפרטיות באתר הרשות</u>. ראו גם מיכאל בירנהק "הנדסת פרטיות ציבורית: המקרה של העברת מידע ממרשם האוכלוסין למפלגות" **דין ודברים** יב 15 (2019). ליישום תפיסה זו בפסיקה ראו עת"מ 28857-06-17 **עמותת חברות הסיעוד נ' משרד הביטחון** (1.7.19), פסקה 16.8 לפסק הדין.

1.5. הממונה ינהל את ביצוע תסקיר ההשפעה על הפרטיות (**Privacy Impact Assessment**) הקרוי גם תסקיר השפעה על הגנת המידע (**Data Protection Impact Assessment**) ויעקוב אחר הטמעת המלצותיו.

1.6. הממונה יפקח על ביצוע סקר סיכוני פגיעה בפרטיות[12] ויעקוב אחר הטמעת המלצותיו.

1.7. הממונה יטפל בתלונות הנוגעות לעיבוד מידע אישי ולזכות לפרטיות, ובפניות של נושאי מידע, לרבות בקשות לעיון במידע או לתיקונו.

2. <u>פיקוח ובקרה</u>:

2.1 הממונה יכין תכנית עבודה שנתית שתובא לאישור ההנהלה הבכירה בארגון, ליישום ופיקוח על קיום הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, ולבירור הפרות של הוראה מהוראות החוק.

2.2 הממונה ידווח להנהלה הבכירה בארגון, בלא דיחוי, על ממצאים של פעולות הפיקוח, הבדיקה, והבירור שביצע.

2.3 הממונה יקיים בקרה על אופן תיקון הליקויים שהתגלו בממצאי הפיקוח והבירור.

2.4 הממונה יגיש להנהלה הבכירה בארגון ולדירקטוריון, אחת לשנה, דין וחשבון על פעילותו בנושא פרטיות. הדוח יכלול את פירוט התלונות והבירור שנעשה לגביהן, פירוט ההפרות של דיני הגנת הפרטיות ודרך הטיפול בהן, דיווח על יישום תכנית העבודה השנתית לפי סעיף 2.1 לעיל, הממצאים והליקויים שנתגלו במסגרתה, וכן המלצות לתיקונם.

2.5 הממונה ינחה את הממונה על אבטחת המידע בארגון בנושאים הקשורים בהגנת פרטיות במידע, ובקיום הוראות חוק הגנת הפרטיות.

2.6 הממונה ישתף פעולה עם הרשות להגנת הפרטיות ככל שיידרש לכך.

2.7 הממונה ידווח לרשות להגנת הפרטיות אם נוכח שאירעה פגיעה מהותית בפרטיות בארגון.

3. <u>הדרכה והטמעה</u>:

3.1 הממונה ישמש סמכות מקצועית ומוקד ידע, וינחה את הנהלת הארגון ועובדיו בנושא הגנת פרטיות.

3.2 הממונה יקדם את ההגנה על הפרטיות במידע ואת הציות להוראות חוק הגנת הפרטיות בארגון, בין היתר, בדרך של הדרכת העובדים.

[12] סעיף 5 (ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

4. <u>סמכויותיו ועצמאותו של הממונה</u>

על מנת שממונה ההגנה על הפרטיות יוכל לממש את אחריותו באופן מיטבי, יש לתת את הדעת לנושאים הבאים -

1. להבטיח כי הממונה מעורב בכל הנושאים הנוגעים להגנה על מידע אישי בארגון.
2. לדאוג כי כל המשאבים והסמכויות הנדרשים למילוי תפקידו עומדים לרשות הממונה, ובכלל זה גישה למידע אישי ותהליכי עיבוד מידע, כמו גם המשאבים הנדרשים לשימור מומחיותו בנושא דיני ההגנה על מידע אישי בישראל.
3. להבטיח כי הממונה יהיה בעל עצמאות מוסדית ומקצועית.
4. מומלץ להגדיר נהלים להחלפת הממונה עם סיום תקופת כהונתו, וכן תנאים לסיום העסקתו בטרם סיום תקופת הכהונה.
5. ככל שהממונה על הגנת הפרטיות משמש במקביל בתפקיד נוסף בארגון, יש לוודא כי אין בכך כדי ליצור ניגוד עניינים.

5. <u>ידע והכשרה רלוונטיים לממונה הגנה על פרטיות</u>

מומחיותו של ממונה ההגנה על הפרטיות נדרשת להיות משולבת, כך שתאפשר לו הבנה מיטבית של התהליכים בארגון ברמה הטכנולוגית והעסקית, לצד יכולת לבחון את התאמתם לדרישות החוק ולמדיניות הארגון. על כן רצוי שהכשרתו של הממונה ותחומי הידע שלו יכללו בין היתר -

1. הכשרה אקדמית או מקבילה במשפטים, חשבונאות, טכנולוגיית מידע, ניהול תהליכים או ברגולציה;
2. ידיעה מעמיקה של דיני ההגנה על מידע אישי בישראל;
3. הבנה נאותה בתחום טכנולוגיות המידע בכלל, ובתחום אבטחת המידע בפרט;
4. היכרות עם דיני ההגנה על מידע אישי באירופה ובארה"ב;
5. היכרות עם הפן העסקי של ניהול ארגון;
6. אתיקה מקצועית.

6. <u>מעמדו של ממונה הגנת הפרטיות בארגון ויחסיו עם בעלי תפקידים אחרים העוסקים בהגנה על מידע אישי</u>

כדי שיוכל למלא באופן מיטבי את תפקידיו ואת המשימות המוטלות עליו, **מומלץ כי הממונה יהיה חלק מההנהלה הבכירה של הארגון**.

חוק הגנת הפרטיות מטיל חובות ואחריות על "**מנהל המאגר**" - מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע, או מי שמנהל כאמור הסמיכו לעניין זה.[13] מנהל מאגר מידע חב באחריות אישית לאבטחת המידע במאגר,[14] וחלה עליו גם חובת הסודיות.[15]
לנוכח החפיפה בתחומי האחריות, ממליצה הרשות כי ארגון הממנה באופן וולונטארי ממונה הגנה על הפרטיות, יסמיך אותו לשמש גם כמנהל המאגר כמשמעותו בחוק הגנת הפרטיות.

באשר לממונה על אבטחת המידע בארגון, חוק הגנת הפרטיות מקים חובה על גופים המחזיקים בחמישה מאגרי מידע, גופים ציבוריים וכן בנקים, חברות ביטוח וחברות העוסקות בדירוג או הערכה של אשראי, למנות אדם בעל הכשרה מתאימה לממונה על אבטחת מידע בארגון[16]. סעיף 3 לתקנות הגנת הפרטיות (אבטחת מידע) קובע תפקידים וסמכויות לממונה אבטחת מידע.

חשוב לשים לב כי תפקידם של השניים אינו זהה. יש להבחין בין **היסוד המשפטי** של דיני הגנת הפרטיות, הקובע את המותר והאסור ביחס לשימושים במידע, ובין **יסוד אבטחת המידע**, שהוא מכלול האמצעים הארגוניים והטכנולוגיים הננקטים למניעת שימוש לא מורשה במידע. אבטחת מידע היא אמצעי שנועד להבטיח את קיומם של עקרונות הגנת המידע המשפטיים והמהותיים.

בעוד שתפקידו של הממונה על אבטחת המידע בארגון הוא לוודא עמידה בתקנים ובנהלים רלוונטיים הנוגעים לאבטחת מידע, וכן להפעיל את מכלול האמצעים הקשורים במניעת שימוש לרעה במידע (מעבר לאיומים הקשורים לפרטיות בלבד), תפקידו של ממונה ההגנה על הפרטיות רחב יותר, ונוגע לעיצוב וגיבוש תהליכי עבודה ונהלים בארגון הקשורים בניהול, עיבוד ושימוש במידע אישי. בין היתר, תפקידו הוא להנחות מקצועית את הממונה על 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.

---

[13] סעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981.
[14] סעיף 17 לחוק הגנת הפרטיות, התשמ"א-1981.
[15] סעיף 16 לחוק הגנת הפרטיות, התשמ"א-1981.
[16] סעיף 17ב לחוק הגנת הפרטיות, התשמ"א-1981.

7. סיכום

החוק הישראלי אינו מטיל כיום חובה כללית למינוי ממונה ארגוני להגנה על הפרטיות. אולם, עמדת הרשות היא כי הסמכה של ממונה הגנה על הפרטיות היא אמצעי ראשון במעלה לשיפור רמת הציות לדיני הגנת המידע בארגון, לקידום האחריותיות ביחס לניהול מידע אישי בו, לקיום דרישת המידתיות בפעילות בעלת פוטנציאל לפגיעה בפרטיות, ולשמירה מיטבית על הזכות לפרטיות בארגון.

יתרה מזו, מינוי ממונה הגנת פרטיות ארגוני עולה בקנה אחד גם עם האינטרס הפנימי של הארגון. שכן, יכולת הארגון להגן על המידע האישי של נושאי המידע היא בעלת חשיבות כלכלית של ממש. מינוי ממונה הגנת פרטיות מאפשר לנושאי המידע לרכוש אמון באשר לטיפול במידע האישי שלהם, ביודעם כי הארגון נקט ונוקט צעדים לצמצום הסיכון לפגיעה בפרטיותם.

כמו כן, תפקידו של הממונה כולל בין היתר הקמת ערוץ תקשורת מול הרשות להגנת הפרטיות. ממונה הבקיא בתהליכי העבודה מול הרשות יאפשר לארגון המתמודד עם הפרה לנהל את האירוע באופן יעיל מול הגורמים המקצועיים, ובמקרים המתאימים גם מול הרשות עצמה, ובכך לחסוך עלויות גבוהות.

יתרון נוסף נוגע לארגונים רבים המכוונים לקהל לקוחות במדינות שונות בעולם. בידו של הממונה ההגנה על הפרטיות לסייע להנהלת הארגון להבין באילו מקרים וכיצד חוקים שונים שנחקקו ברחבי עולם הנוגעים להגנה על מידע, עשויים להשפיע על מהלך העסקים של הארגון, ולהיערך בהתאם.[17] לאור האמור לעיל, קיימת חשיבות גדולה למינוי של ממונה הגנה על הפרטיות בארגון לצורך יישום אפקטיבי של דיני ההגנה על מידע אישי בישראל. מעבר לכך, מינוי אדם בעל הבנה מעמיקה בדיני ההגנה על מידע אישי, ובאופן היישום של דינים אלו, יחסוך לארגון זמן וכסף וימנע טעויות יקרות.

[17] כגון רגולציית הגנת המידע של האיחוד האירופי (GDPR), חוק הגנת פרטיות הצרכן בקליפורניה (CCPA), חוק הגנת המידע האישי בברזיל (LGPD) ועוד.