




הרשות
להגנת
הפרטיות



משרד המשפטים

מדריך לארגונים: מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו



PPA@justice.gov.il  | 02-6467064  | 03-7634050 
WWW.PPA.JUSTICE.GOV.IL | 6107202 תל אביב ת.ד. 7360, קרית הממשלה, ת.ד.

חפשו אותנו גם בפייסבוק 

היתרונות לארגון וללקוחות

מינויו של ממונה על הגנת הפרטיות באופן וולונטארי מהווה פרקטיקה ראויה ומומלצת (Best Practice) לארגונים האוספים ומעבדים מידע אישי, בעלי מאגרים ומחזיקים כאחד.

מדוע?



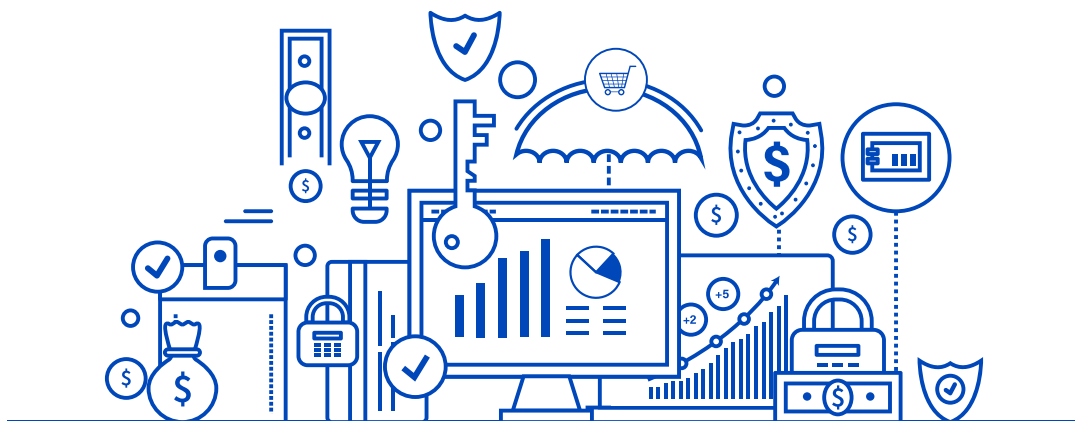
מינוי הממונה
יחסוך לארגון
זמן וכסף.



עצם המינוי הוא אינדיקציה
כי הארגון שלכם נקט ונוקט
צעדים לצמצום הסיכון לפגיעה
בפרטיות ולהגנה על המידע
האישי הנשמר ברשותו.



הממונה יסייע
לארגונכם לוודא כי
הוא עומד בהוראות
דיני ההגנה על מידע
אישי בישראל.



מיהו ממונה הגנה על הפרטיות בארגון?

מופקד על קידום הזכות לפרטיות ועל יישום דיני ההגנה על מידע אישי בארגון.



תפקידו המרכזי:

להביא להפנמה של עקרונות ושיקולי פרטיות בתהליכי העבודה בארגון, ולסייע לארגון במימוש אחריותו וחובותיו לפי דיני הגנת הפרטיות.



מעמדו בארגון?

חלק מההנהלה הבכירה של הארגון, או לכל הפחות מי שממלא תפקיד זה בארגון ידווח ישירות להנהלה הבכירה, וישולב בהיררכיה של הארגון בעמדה בכירה דיה, שיאפשר לו להשפיע באופן אפקטיבי על התהליכים המרכזיים בארגון.



באילו ארגונים כדאי למנות ממונה הגנה על הפרטיות?

- ארגונים שעסקיהם או השירותים שמספקים הם מבוססי מידע (data driven).
- ארגונים שקיימת סבירות שפעילותם תיצור סיכון מוגבר לפרטיות, בין היתר מהטעמים הבאים:
 - מאפייני הארגון** (למשל גופים ציבוריים וגופים הסוחרים במידע).
 - סוג המידע ורגישותו** (למשל מידע רפואי רגיש או מידע ביומטרי).
 - מידע על **אוכלוסיות מיוחדות** (למשל קטינים).
 - היקף המידע או מספר מורשי הגישה** אליו.

האם עלינו למנות ממונה הגנה על הפרטיות מתוך הארגון או מחוצה לו?
ממונה הגנת הפרטיות יכול להיות מינוי פנימי, עובד החברה, או מינוי חיצוני לחברה.

איך תדעו מה מתאים עבור הארגון שלכם?

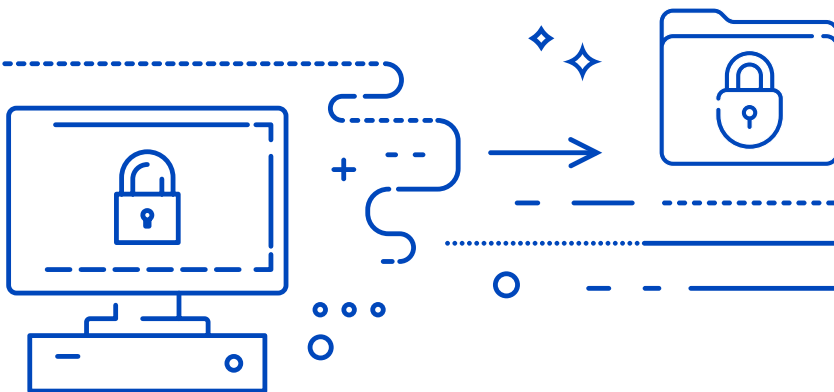
בהתאם למאפייני הארגון שלכם, פעולות עיבוד המידע שמבצע ארגונכם והמשאבים הכספיים והאנושיים שלו.

ארגונכם הוא ארגון גדול או שליבת העיסוק שלו כוללת עיבוד מידע אישי או ארגון העוסק במידע אישי בקנה מידה רחב?

במקרה זה עשוי להיות יתרון משמעותי למינוי עובד פנימי בעל תפקיד בכיר בארגון.
שימו לב! במינוי פנימי, יש לוודא כי העובד אינו נתון לניגוד עניינים על רקע תפקיד אחר שהוא ממלא בתוך הארגון.

ארגונכם כפוף ל-GDPR?

מינוי ממונה הגנת פרטיות ממילא עשוי להיות חובה חוקית ישירה, ומכל מקום תקל על הארגון לנהל עסקים עם חברות שאינן ישראליות.



תפקידיו של ממונה ההגנה על הפרטיות

היקף תפקידו של הממונה על הגנת הפרטיות בארגון ייקבע על פי מורכבות פעולות עיבוד המידע האישי שמתבצעות בארגון וגודלו!

להלן מפורטים תפקידים ומשימות שמומלץ לשקול להטיל על הממונה בהתאם למאפייני הארגון:

הסדרת תהליכי ניהול מידע בארגון:

- לנסח את מדיניות הפרטיות של הארגון ולהביאה לאישור ההנהלה הבכירה.
- להיות מעורב לאורך כל מחזור החיים של תהליכי עיבוד מידע בארגון, על מנת לוודא שפעילות עיבוד המידע מבוצעת באופן המפחית ככל הניתן את הסיכונים לפרטיות לקוחות הארגון.
- מעורבות 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 בהתבסס על תפיסת "עיצוב לפרטיות" (Privacy By Design) ותפיסת "פרטיות כברירת מחדל" (Privacy By Default).

הידעתם?



מהן תפיסות עיצוב לפרטיות ופרטיות כברירת מחדל?

אלו תפיסות הדוגלות בעיצוב מערכת המידע להגנה אופטימאלית על הפרטיות ולצמצום איסוף המידע ועיבודו למינימום ההכרחי, כבר משלב התכנון המוקדם וגם לאורך כל מחזור החיים של המידע והשימוש בו. המטרה היא שעיצוב המערכות ישרת את התכליות העסקיות של הארגון, בד בבד עם מזעור הסיכונים לפרטיות.

- לבדוק את הנהלים ומדיניות הארגון בתחום הפרטיות ואת עמידתם בהוראות חוק הגנת הפרטיות וכן לבצע מעקב, בקרה, ועדכון של הנהלים במידת הצורך.
- לנהל את עריכתו של תסקיר השפעה על הפרטיות (Privacy Impact Assessment) במקרים בהם ביצעו נדרש על פי דין או מבוצע באופן וולונטרי ביזמת הארגון, ולעקוב אחר הטמעת מסקנותיו.
- לקבל דיווח על ביצוע סקר סיכונים אבטחת מידע ולעקוב אחר הטמעת המלצותיו.
- לטפל בתלונות הנוגעות לעיבוד מידע אישי ולזכות לפרטיות, ובפניות של לקוחות הארגון לרבות בקשות לעיון במידע או לתיקונו.

פיקוח ובקרה:

- להכין תכנית עבודה שנתית שתובא לאישור ההנהלה הבכירה בארגון, ליישום ופיקוח על קיום הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, ולבירור הפרות של הוראות החוק.
- לדווח להנהלה הבכירה בארגון, בלא דיחוי, על ממצאים של פעולות הפיקוח, הבדיקה, והבירור שביצע.
- לקיים בקרה על אופן תיקון הליקויים שהתגלו בממצאי הפיקוח והבירור.
- להגיש להנהלה הבכירה בארגון ולדירקטוריון, אחת לשנה, דוח על פעילותו בנושא פרטיות.
- לשתף פעולה באופן הדוק עם הממונה על אבטחת המידע בארגון בנושאים הקשורים בהגנת פרטיות המידע, ובקיום הוראות חוק הגנת הפרטיות.
- לשמש איש קשר מול הרשות להגנת הפרטיות - להיות אחראי על הגשת דיווחים ועדכונים לרשות, ככל הנדרש על פי דין, לרבות הודעה על שינוי בפרטי רישום המאגר ודיווח על התרחשות אירוע אבטחת מידע חמור.



הדרכה והטמעה:

- לשמש סמכות מקצועית ומוקד ידע.
- להנחות את הנהלת הארגון ועובדיו בנושא הגנת פרטיות.
- לקדם את ההגנה על הפרטיות במידע ואת הציות להוראות חוק הגנת הפרטיות בארגון, בין היתר, בדרך של הדרכת העובדים.

סמכויות ועצמאות:

- הבטיחו כי הממונה יהיה מעורב בכל הנושאים המהותיים הנוגעים להגנה על מידע אישי בארגון.
- דאגו כי כל המשאבים והסמכויות הנדרשים למילוי תפקידו עומדים לרשותו, ובכלל זה גישה למידע אישי ותהליכי עיבוד מידע, כמו גם המשאבים הנדרשים לשימור מומחיותו בנושא דיני ההגנה על מידע אישי בישראל.
- הבטיחו כי הממונה יהיה בעל עצמאות מוסדית ומקצועית.
- במידה והממונה משמש במקביל בתפקיד נוסף בארגון, וודאו כי הדבר אינו יוצר ניגוד עניינים.



ידע והכשרה:

מומחיותו של ממונה ההגנה על הפרטיות נדרשת להיות משולבת, כך שתאפשר הבנה מיטבית של התהליכים בארגון ברמה הטכנולוגית והעסקית, לצד יכולת לבחון את התאמתם לדרישות החוק ולמדיניות הארגון.

כדי שיוכל למלא את תפקידו באופן אפקטיבי, תחומי הידע של ממונה הגנה על פרטיות צריכים לכלול **לכל הפחות** -

- ידיעה מעמיקה של דיני הפרטיות וההגנה על מידע אישי בישראל (לא בהכרח במסגרת השכלה משפטית פורמאלית);
- הבנה מספקת בתחום טכנולוגיות המידע והבנה בסיסית בתחום אבטחת המידע, בשים לב להיקף ולמידה בהם הארגון מבוסס מידע וטכנולוגיה. דהיינו, ככל שליבת העיסוק של הארגון כרוכה בעיבוד מידע אישי, נדרשת מידת הבנה רבה יותר בתחום אבטחת המידע וטכנולוגיות המידע.

הכשרה ותחומי ידע נוספים העשויים לשפר את תפקוד הממונה ואת התועלת שתצמח ממנו לארגון:

- הכשרה אקדמית או מקבילה במשפטים, חשבונאות, טכנולוגיית מידע, ניהול תהליכים או ברגולציה;
- היכרות עם דיני ההגנה על מידע אישי באירופה ובארצות הברית או בשווקים אחרים בעולם הרלוונטיים לארגון;
- היכרות עם הפן העסקי של ניהול ארגון;
- אתיקה.

ההמלצות במדריך מנוסחות בלשון זכר אך פונות לכל המינים.