טיוטת גילוי דעת רשות הגנת הפרטיות: מינוי ממונה על הגנת הפרטיות (DPO)

לקוחות יקרים.ות,

ביום 23.7.2025 פרסמה רשות הגנת הפרטיות טיוטת גילוי דעת מהותית בעניין חובת מינוי ממונה על הגנת הפרטיות (DPO) בארגונים, בהתאם לתיקון 13 לחוק הגנת הפרטיות, אשר ייכנס לתוקף בימים הקרובים ביום 14.8.2025.

הטיוטה פתוחה להערות הציבור עד 23.9.2025, אך כבר עתה יש לה השלכות רגולטוריות וישימות מובהקות, שכן הרשות ציינה כי הפרשנות המוצגת בה תשמש אותה בעת הפעלת הסמכויות המוקנות לה.

לאור העובדה שתיקון 13 קובע לראשונה חובת מינוי DPO, התעורר צורך משמעותי בקבלת הנחיות או פרשנות מצד הרשות באשר לסעיפי החוק החדשים, וניכר כי הרשות נתנה דעתה על כלל הנושאים הרלוונטיים. למרות שלא תמיד סיפקה וודאות בכל נושא או העמידה פרשנות פרקטית, הטיוטה מתייחסת לקריטריונים בהם מתקיימת החובה למינוי ממונה על הגנת הפרטיות, כישורי הממונה, תפקידיו ותחומי אחריותו, כמו-גם מיקומו בארגון וניגודי עניינים אפשריים.

להלן עיקרי גילוי הדעת:

1. על מי חלה החובה למנות ממונה?

בהתאם לסעיפים 17ב1(א)(1)-(4) לחוק החובה למנות ממונה על הגנת הפרטיות חלה על:

1. **גופים ציבוריים** (כהגדרתם בחוק) וכן **מחזיק של גוף ציבורי**.

בהקשר זה, הרשות מזכירה כי מחזיק של גוף ציבורי ייחשב **כל** גורם חיצוני שמבצע אחסון או עיון במידע אישי של גוף ציבורי, ולכן יחוב במינוי DPO. המשמעות המעשית היא כי חברות טכנולוגיה, IT ו-Back office שמספקות שירותים למשרדי ממשלה, רשויות או חברות ממשלתיות עלולות להיכנס לתחולת החובה גם אם פעילותן תומכת בלבד. מומלץ לבצע סקר הסכמי מתן שירותים עם לקוחות שהם גופים ציבוריים, לצורך בחינת הצורך במינוי ממונה על הגנת הפרטיות.

2. **גופים העוסקים בסחר במידע אישי** (data brokers)

מדובר בגופים שאוספים מידע אישי לשם מסירתו לאחר כדרך עיסוק או בתמורה, לרבות שירותי דיוור ישיר, ורק אם יש במאגר מידע אישי על יותר מ-10,000 בני אדם. הרשות מרחיבה וקובעת כי "כדרך עיסוק או בתמורה" **מתפרש כתנאים חלופיים**. כך, החובה תחול אם מטרת המאגר היא מסירת מידע לצד שלישי במסגרת עיסוקו הרגיל של הארגון, **אף אם המסירה היא ללא תמורה**, או לחלופין אם הארגון מוסר מידע לצד שלישי בתמורה, **אף אם המסירה איננה נעשית כדרך העיסוק**. שנית, הרשות מפרשת את המונח "סחר במידע אישי" **באופן רחב**, תוך הפניה לעמדתה של רשות הגנת המידע הבריטית, לפיה סוכנויות דירוג אשראי נכללות תחת קטגוריה זו של הארגונים העוסקים בסחר במידע, ולכן מחויבים במינוי DPO.

3. **גופים שפעילות הליבה שלהם כוללת עיבוד מידע אישי תוך ניטור שוטף ושיטתי**

זוהי החובה ה"רכה" או "עילת סל", אשר בדומה להוראתה המקבילה ב-GDPR, מחייבת מינוי ממונה בהתקיים שלושה קריטריונים איכותיים: (א) ארגונים **שעיסוקם העיקרי כולל** פעולת עיבוד מידע אישי או כרוכים בפעולות כאמור; (ב) טיבן, היקפן או מטרתן של פעולות העיבוד מחייבות **ניטור שוטף** ושיטתי של בני אדם, כולל מעקב או התחקות שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם; (ג) **ובהיקף ניכר**. החוק אף קובע במפורש דוגמאות (שלא בהכרח מסייעות) כי הסעיף חל גם על ספקי תקשורת סלולארי ועל ספקי שירותי חיפוש מקוון. מאחר ומדובר במושגי שסתום הרשות התייחסה לכך בהרחבה:

"עיסוק עיקרי" – כאשר עיבוד מידע אישי המהווה 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).

הרשות מציינת כי מבחן "ניטור שוטף ושיטתי" הוא **מבחן אובייקטיבי שבודק אם עיסוקיו המרכזיים היו כרוכים בניטור שוטף ושיטתי בפועל**, ואין זה משנה אם זו לא הייתה מטרת מאגר המידע.

הרשות מספקת רשימת דוגמאות מייצגות:

- כאשר יש התחקות אחרי פעילות משתמשים באפליקציות ובאתרי אינטרנט, כגון תדירות שימוש, סוגי הפעולות שמתבצעות וזמני הפעולות.
- כאשר עיבוד מידע נעשה במטרה ליצור פרופיל של תכונות, התנהגויות, תחומי עניין או העדפות של אנשים (profiling), למגוון מטרות, לרבות פרסום ממקוד, התאמה אישית של תוכן ושירותים, וניהול סיכונים (דירוג אשראי, חיתום ביטוחי, איתור הונאות ועוד).
- כאשר מדובר במתן שירות באמצעות אפליקציות אוספות נתוני מיקום במרחב הפיזי.
- כאשר השירות כרוך בשימוש באפליקציות והתקני מחשוב לביש העוקבים אחרי נתוני בריאות.
- כאשר מדובר בהפעלת מתקנים מחוברים לאינטרנט כגון כלי רכב חכמים ומכשירי חשמל ביתיים המחוברים לרשת (IoT).
- כאשר יש שימוש במאגרי הצילומים של מצלמות מעקב.
- ספקי אינטרנט.

בנוסף, הרשות מבהירה כי לא מדובר ברשימה סגורה, והארגונים המתלבטים אם החובה חלה עליהם, רשאים לפנות לרשות לצורך הבירור.

להשקפתנו, הדוגמאות שמציינת הרשות מרחיבות משמעותית את המונח באופן שתחייב ארגונים רבים למנות ממונה על הגנת הפרטיות.

"היקף ניכר" - אין סף כמותי חד ערכי ויש לבחון אותו לפי מכלול הנסיבות והשיקולים הנוגעים לכל מקרה לגופו ובכלל זה 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. מפתיע למצוא את האמירה לפיה ככל שמתקיימים שיקולים אחרים בסעיף תיטה הכף לפרש היקף ניכר גם כאשר מספר נושאי המידע עליהם מעובד המידע איננו גדול.

4. גופים שעיסוקם כולל עיבוד מידע רגיש בהיקף ניכר

ארגונים שעיסוקם העיקרי כולל עיבוד מידע אישי בעל רגישות מיוחדת, כפי שהוא הוגדרה בתיקון 13, ובהיקף ניכר כאמור לעיל, ובכלל זה בנקים, חברות ביטוח, בתי חולים וקופות חולים.

מובהר כי הכוונה היא לארגונים שזהו עיסוקם העיקרי ואין הכוונה ל**עיבוד מידע כאמור בהיקף ניכר רק לצורך ביצוע מטרות עזר כגון העסקת עובדים**, אם אינן בעלות זיקה ישירה למטרות עיקריות של הארגון.

גילוי הדעת בנוסחו הנוכחי עדיין משאיר אי וודאות רבה ביחס לתנאים שמחייבים מארגונים למנות DPO. לפיכך, ולשם הפחתת חשיפה רגולטורית, מומלץ לתעד את תהליך קבלת ההחלטה בעניין מינויו או אי מינויו של הממונה ולשקול הנמקה פורמלית בפרוטוקול הנהלה.

2. מה דרישות הסף לממונה על הגנת הפרטיות?

הרשות קובעת כי הממונה חייב להיות בעל הידע והכישורים הנדרשים למילוי תפקידו, תוך היכרות עם ערך ההגנה על הפרטיות, יכולת עבודה בצוות, כושר שכנוע והובלת תהליכים ומתייחסת לקריטריונים הקבועים בחוק:

- **ידע מעמיק בדיני פרטיות בישראל** – דרישה להיות בעל שליטה מלאה ומקיפה בדיני הגנת הפרטיות בישראל לרבות פסקי בתי המשפט ובתי דין לעבודה בנושאים שקשורים לזכות לפרטיות. החוק אינו מחייב הסמכה פורמלית, אך הרשות מדגישה את הציפייה להכשרה ייעודית של לפחות 40 שעות, ורצוי גם ניסיון קודם בתחום או תעודת הסמכה רשמית.

- **הבנה הולמת בטכנולוגיה** – ההבנה בטכנולוגיה ובאבטחת מידע צריכה לאפשר את הטמעת עיקרון "עיצוב לפרטיות" (privacy by design) בתכנון מערכות הארגון ושימוש בטכנולוגיות מגבירות פרטיות (PETs) ולהיות מעורב באופן אקטיבי בניתוח השלכות השימוש בטכנולוגיות חדשות ובהערכת סיכוני הפרטיות הנובעים מהן.

- **היכרות עם תחומי הפעילות ומטרותיו של הארגון** – נדרש להכיר את ייעודו של הארגון, המגזר, הסביבבה ותהליכי עיבוד המידע בו לעומק כך שניתן יהיה להכיר את הסיכונים הפוטנציאליים ולהתאים את מדיניות עיבוד המידע לצרכים הייחודיים של הארגון ולהטמיע את החוק היעילות בתהליכי העבודה.

3. מהן דרישות התפקיד של הממונה על הגנת הפרטיות?

בהתאם לעמדת הרשות, הממונה הוגדר כשחקן מפתח במערך משילות המידע בארגון (Governance Data) ואת תפקידו אפשר לתאר **כמתאם של תהליכי הציות**, אשר יידרש גם לקדם שיפור הגנה על הפרטיות ואבטחת המידע גם מעבר למינימום הנדרש הקבוע בדין, תוך הפנמת "תרבות פרטיות" בארגון ושל עקרונות ושיקולי פרטיות בכל תהליכי עבודה הנוגעים למידע אישי.

הרשות מתייחסת לכל אחד מתפקידי הממונה בפירוט נרחב.

- **סמכות מקצועית וייעוץ** – על הממונה לנקוט גישה פרואקטיבית ולסייע לכל מחלקות רלוונטיות שמעבדות מידע אישי בארגון, החל מקבלת החלטות מדיניות על ידי הנהלת הארגון ועד לתכנון מערכות, העברת מידע לגורמים שלישיים והחלטה על ביעור המידע. הרשות מדגישה כי **אף על פי שהחוק לא מחייב לאמץ עמדת הממונה, יש לשקול את עמדתו בכובד ראש**, לנמק החלטה שלא לאמץ אותה, ולנהוג בה כחוות דעת של גורם שיש חובת היוועצות עימו.

- **הדרכה** – הממונה חייב להכין תוכנית הדרכה ולפקח על ביצועה. מומלץ על ידי הרשות, כי הממונה יבצע את ההדרכות בעצמו, אך בשים לב לגודל הארגון.

- **בקרה שוטפת** – הממונה חייב להכין תוכנית שנתית לבקרה שוטפת ולכל הפחות לוודא את ביצועה, אך מומלץ כי יהיה מעורב בביצועה בפועל. על הממונה לדווח להנהלת הארגון על ממצאי הביקורת ולהמליץ על פעולות לצורך תיקון פערי ציות שהתגלו. הובהר על ידי הרשות, כי תוכנית בקרה על עמידה בתקנות אבטחת המידע היא באחריות ממונה אבטחת המידע ולא של ממונה על הגנת הפרטיות.

- **נוהל אבטחת מידע ומסמך הגדרות מאגר** – הממונה חייב לכל הפחות לוודא כי קיים נוהל אבטחת המידע שאושר על ידי הנהלה ומוכר לדירקטוריון. הרשות ממליצה כי הממונה ייקח חלק פעיל בהכנת מסמך הגדרות מאגר ובעדכונו.

- **טיפול בפניות ובבקשות נושאי מידע** – הממונה חייב לכל הפחות לוודא כי נעשה טיפול מקצועי וענייני בפניות ובבקשות נושאי המידע למימוש זכויותיהם לפרטיות.

- **איש קשר עם רשות הגנת הפרטיות** – הרשות יכולה לפנות לממונה על הגנת הפרטיות לקבל עמדתו או חוות דעתו מקצועית, טרם קבלת החלטות בנוגע לארגון בה הוא משמש את התפקיד או טרם מתן חוות דעת מקדמית.

4. מיקומו ומעמדו של הממונה בארגון

הרשות מבהירה כי ניתן להעסיק את הממונה כנותן שירותים חיצוני, אך **עדיף שהממונה יהיה עובד הארגון** באופן שיאפשר לו היכרות מעמיקה עם הארגון, לרבות הבנת המבנה הארגוני ותחומי פעילות שלו, וכן מאפשרת את הזמינות והנגישות הנדרשות.

הרשות אף מבהירה כי רק אדם טבעי יכול לכהן כממונה על הגנת הפרטיות, אף על פי שאין מניעה כי ההתקשרות תתבצע באמצעות החברה בה הוא מועסק.

הרשות מציינת כי כל ארגון יכול להחליט בעצמו איפה למקם בהיררכיה הארגונית את הממונה על הגנת הפרטיות, אך בכפוף לדרישות הדין, כגון חובת דיווח ישיר למנכ"ל או לגורם כפוף למנכ"ל במישרין, הספקת תנאים ומשאבים נאותים לממונה, ואיסור הימצאות הממונה במצב של חשש לניגוד עניינים.

אין חובת דיווח לרשות באופן יזום, אך הובהר כי הרשות עשויה לפנות אל הממונה ולדרוש חוות דעתו שניתנו מסגרת תפקידו. זוהי נקודה רגישה שכן ככלל, לא קיים חסיון על עבודת הממונה להבדיל מחוות דעת משפטית, ולכן יש לקחת זאת בחשבון.

5. מתי עולה חשש לניגוד עניינים?

בהקשר של הימצאות במצב של חשש לניגוד עניינים הרשות מאמצת את גישתה של רשות הגנת הפרטיות הצרפתית CNIL, לפיה "הממונה אינו יכול למלא תפקידים (או להיות כפוף לבעלי תפקידים) הכוללים את הסמכות או האחריות לקבוע מדיניות בעניין עיבוד הידע האישי בארגון, לרבות קביעת מטרות העיבוד וקבלת החלטות מהותיות לגבי שיטות ואמצעים".

באופן קונקרטי, הרשות מתייחסת לתפקידים הבאים:

- **היועץ המשפטי:** הרשות אינה אוסרת למקם את הממונה במחלקה המשפטית של הארגון, אך מדגישה את ההבדלים בין תפקיד היועץ המשפטי (שמבטיח את הציות לחוק בלבד) לבין תפקידו של ממונה על הגנת הפרטיות (שאמון על קידום השמירה על הפרטיות אל מעבר למינימום המתחייב מהדין).
- **תפקידים בכירים:** ככלל, מי שלו הסמכות או האחריות לקביעת מדיניות עיבוד המידע האישי בארגון בדגש על המטרות ואמצעי העיבוד – לא יוכל להיות ממונה. וככלל אצבע מוזכר כי אין על הממונה להיות בעל תפקיד של מנהל שיווק, מנהל לקוחות, מנהל כספים, מנהל מערכות מידע או CTO.
- **ממונה אבטחת מידע (CISO):** על אף היעדר איסור מפורש, הרשות מדגישה את המורכבות המשפטית והיישומית במילוי תפקיד ממונה על הגנת הפרטיות יחד עם תפקיד ממונה אבטחת מידע, לאור השוני המהותי שיש בשני תפקידים אלה – בגין השוני בידע ובכישורים שנדרשים מכל אחד מהתפקידים האלה, סיכוי סביר להיות במצב של ניגוד עניינים (למשל, נקיטת אמצעי אבטחה מוגברים עלולים לפגוע משמעותית בפרטיות); והשוני בדרישה לכפיפות ארגונית כך שה-CISO לא יהיה כפוף במישרין לנושא משרה (להבדיל מה-DPO). בנוסף, בארגונים גדולים האחריות הכבדה של ממונה אבטחת מידע עלולה לא לאפשר לו למלא תפקיד של DPO בצורה נאותה.

כיצד נוכל לסייע?

מחלקת הפרטיות, הסייבר וה-IT במשרדנו עומדת לרשותכם לבחינת תחולת הדרישה על הארגון, לסיוע באיתור מועמד מתאים, בליווי תהליכי מינוי, בבניית תוכניות עבודה ותסקירים, וביצירת מנגנוני בקרה והדרכה.

לקריאת גילוי הדעת המלא – לחצו כאן

אין באמור כדי להוות ייעוץ משפטי והוא מספק מידע כללי בלבד.