



www.nblaw.com

דיני פרטיות ומידע

תיקון 13 לחוק הגנת הפרטיות (עדכון שני בסדרה)

ספטמבר 2024

אנו שמחים להביא בפניכם/ן ניזולטר נוסף בסדרה בנושא תיקון 13 לחוק הגנת הפרטיות אשר פורסם לאחרונה ברשומות ויוכנס לחוקף ב-14 באוגוסט 2025. בעדכון זה נתמקד בחידושים המרכזיים הבאים של התיקון לחוק: עדכון הגדרת בעלי התפקידים ("בעל שליטה", "מחזיק" ו"ביטול תפקיד מנהל המאגר"), החובה החדשה למנות DPO - ממונה על הגנת הפרטיות, ושינויים בחובה למנות ממונה אבטחת מידע. **הניזולטר הראשון** בסדרה דן בהרחבת תחולת החוק מבחינת המידע עליו חל והשימושים במידע אותם החוק תופס, בעדכון מונחים, ובצמצום חובת הרישום והטלת חובת הודעה לרשות להגנת הפרטיות על מאגרי מידע מסוימים.

מהים "שחקנים" העיקריים של רגולציית הגנת המידע במאגרי מידע?

- עד היום החוק הגדיר את המונחים "מחזיק" ו"מנהל מאגר". החידוש המרכזי בעניין זה בתיקון 13 הוא הוספת הגדרת המונח "**בעל שליטה**". בדומה להגדרת "Controller" ב-GDPR (רגולציית הגנת הפרטיות של האיחוד האירופי), בעל שליטה הוגדר בתיקון 13 כ-"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 מידע". יש לשים לב שבניגוד ל-GDPR, ההגדרה הישראלית לא כוללת את הרכיב של קביעת האמצעים לעיבוד המידע, מתוך הבנה שבמקרים רבים, דוגמת אחסון ענן, האמצעים לעיבוד המידע נקבעים דווקא על ידי המחזיק ומתוך רצון לשמר את אחריות בעל השליטה גם במקרים אלה.
- התיקון לחוק קובע הגדרה רחבה יותר למונח "**מחזיק**" מזו הקיימת כיום בחוק. ההגדרה החדשה פותרת אי בהירויות לגבי השאלה מי נחשב "מחזיק", ודומה כעת להגדרת "Processor" ב-GDPR. התיקון לחוק מגדיר "מחזיק" כ-"גורם חיצוני לבעל השליטה במאגר מידע המעבד מידע עבור". שינוי ההגדרה של "מחזיק" מעלה שאלות לגבי המונח "גורם חיצוני" בתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (אשר קובעת את החובה לערוך הסכם עיבוד מידע), שנוטר בעינו ולא הובהר או נוסח במדויק במסגרת התיקון לחוק. לפיכך, הרשות להגנת הפרטיות יחדש להבהיר מה נותר תחת הגדרת "גורם חיצוני" לאחר שהגדרת "מחזיק" הורחבה כאמור.
- ומה בנוגע ל"**מנהל המאגר**"? עד היום הוגדר המונח בחוק כ"מנהל פעיל של ארגון שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור. הסימיו לעניין זה". החוק הטיל על "מנהל מאגר" אחריות אישית ביחד עם בעל המאגר. התיקון לחוק קובע כעת כי "מנהל המאגר" הוא "בעל שליטה במאגר מידע, ולעניין גוף ציבורי, כהגדרתו בסעיף 23 לחוק – המנהל הכללי של ארגון שבבעלותו או בהחזקתו מאגר מידע או מי שהמנהל הכללי הסמיכו לנהל את החובה לערוך הסכם עיבוד מידע, שנוטר בעינו ולא הובהר או נוסח במדויק במסגרת התיקון לחוק. לפיכך, הרשות להגנת הפרטיות יחדש להבהיר מה נותר תחת הגדרת "גורם חיצוני" לאחר שהגדרת "מחזיק" הורחבה כאמור.

מינוי DPO

מינוי DPO היא חובה חדשה בדיון הישראלי, אך היא קיימת מזה כמה שנים ברגולציית הגנת המידע האירופית (GDPR). באופן כללי, תפקידו של ה-DPO לשמש כתובת מקצועית לנהלת הגוף ולעבדיו בכל הקשור להיבטי הגנת הפרטיות בארגון וכן לוודא עמידה בהוראות החוק ותקנותיו.

מהים הגופים הנדרשים למנות ממונה על הגנת פרטיות (DPO)?

- גופים ציבוריים** (משדרי ממשלה, רשויות מקומיות) וכן גופים המנויים בצו הגנת הפרטיות (קביעת גופים ציבוריים), כגון אוניברסיטאות וקופות חולים.
- סחרי מידע** – בעל שליטה במאגר מידע הכולל מידע אישי על יותר מ-10,000 בני אדם, שמטרתו העיקרית היא איסוף מידע אישי לשם מסירתו לאחר, כדרך עיסוק או בתמורה, לרבות שירותי דיור ישרי. מזכיר כי מאגרים אלה חייבים בחובת רישום לפי התיקון לחוק.
- בעל שליטה או מחזיק במאגר מידע שעיסוקיו העיקריים כוללים פעולות עיבוד מידע, אשר נוכח טיבן, היקפן או מטרתן מחייבות ניטור שוטף ושיטתי של בני אדם, ובכלל זה מעקב או התחזקת שיטתית אחר התנהגותו, מיקומו או פעולותיו של אדם, בהיקף ניכר. הדוגמאות המוזכרות בתיקון הן ספק מורשה לפי חוק התקשורת (בזק ושידורים), ספק סלולר, ספק אינטרנט, רשתות כבלים ולוויין וספק שירותי חיפוש מקוון. דוגמאות שניתנו על ידי ה-EDPB (המועצה להגנת מידע של האיחוד האירופי) לדרישה המקבילה ב-GDPR ועשויות להיות רלוונטיות גם בישראל כוללות, בין היתר, חברת אבטחה המפעילה מצלמות אבטחה בכמה קניונים או מרכזים מסחריים; אפיון אנשים על בסיס מידע אישי ("פרופילאות") למטרות הערכת סיכונים (לצרכי קביעת פרמיות ביטוח, מניעת הונאות וכדומה); מעקב אחר נתוני מיקום באמצעות אפליקציות סלולריות; מעקב אחר נתוני בריאות באמצעות טכנולוגיה לבישה; ואיסוף מידע מקלי רכב חכמים.**
- בעל שליטה או מחזיק שעיסוקו העיקרי כולל עיבוד מידע בעל רגישות מיוחדת בהיקף ניכר, לרבות בנק, חברת ביטוח, בית חולים כללי וקופת חולים.** זוהי הקטגוריה הרלוונטית ביותר למרבית הגופים הפרטיים, אשר יצטרכו לבחון אם הם מעבדים מידע בעל רגישות מיוחדת (ראו על כך בניזולטר הראשון בסדרה) ואם העיבוד הינו בהיקף ניכר.

מהו אותו עיבוד מידע ב"היקף ניכר" המוזכר בשתי הקטגוריות מעלה?

התיקון לחוק קובע שלשם כך יש לבחון את כמות בני האדם שמידע מעובד לגביהם, שיעורם באוכלוסייה מסוימת, היקף המידע, כמותו, טווח סוגי המידע המעובד, משך ותדירות פעולות העיבוד, משך השמירה, והתחום הגיאוגרפי של פעולות העיבוד.

מהם תפקידי ה-DPO (ממונה הגנת פרטיות)?

ה-DPO לא הוגדר בתיקון לחוק כגורם מבצע אלא כגורם מתכלל, מפקח ומייעץ. תפקידיו המנויים בתיקון לחוק כוללים:

- לשמש סמכות מקצועית ומוקד ידע בתחום הגנת הפרטיות; לייעץ לנהלת הארגון ולעובדיו; להכין תוכנית הדרכה ולפקח על ביצועה.
- להכין תכנית לבקרה שוטפת על העמידה בהוראות חוק הגנת הפרטיות לגבי מאגרי מידע, לוודא ביצועיה, לדווח לנהלת הארגון על הממצאים ולהציע הצעות לתיקון הליקויים.
- לוודא קיומם של נוהל אבטחת מידע ומסמך הגדרות המאגר, שיובאו לאישור הנהלת הארגון, כנדרש לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.
- לוודא טיפול בפניות של נושאי מידע, ובכלל זה בקשות לעיון במידע או לתיקונו.

ה-DPO נדרש לדווח ישירות למנכ"ל הארגון או לעובד שכפוף ישירות למנכ"ל. הוראה זו מגדישה את מעמדו הבכיר של ה-DPO בארגון ואת החשיבות שבמתן סמכויות מספקות לממונה, באופן שיאפשר לו לבצע את תפקידו באופן מיטבי.

יש לפרסם לציבור באופן גישו ופשוט את דרכי ההתקשרות עם ה-DPO. בדרך כלל מידע זה יכלל במסגרת מסמך מדיניות הפרטיות של הארגון.

מי יכול לשמש DPO?

- מי שהוא בעל ידע מעמיק בדיני הגנת הפרטיות, הבנה הולמת בטכנולוגיה ואבטחת מידע והיכרות עם תחומי פעילותו של הארגון. בוועדת החוקה, חוק ומשפט של הכנסת נערך דיון בשאלת היקף הידע הנדרש בנושא אבטחת מידע, שהר DPO אינו חופף בתפקידיו או בסמכותיו לפונקציה של ממונה אבטחת מידע. הובהר בדיונים כי במונח "הבנה הולמת", להבדיל מ"ידע מעמיק", הכוונה להבנה מספקת שתאפשר לוודא את הציות הארגוני לחובות הרגולטוריות בתחום אבטחת המידע. ואולם הנושא עשוי להגיע בעתיד לפתחם של הרשות להגנת הפרטיות ושל בית המשפט, שיידרשו לפרשנות המונח "הבנה הולמת".
- יובהר כי ניתן למנות DPO חיצוני, שאינו עובד הארגון.
- ה-DPO לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים עם מילוי תפקידיו לפי חוק הגנת הפרטיות. הוראה דומה קיימת ב-GDPR. ה-EDPB מנה כמה בעלי תפקידים שאינם יכולים לשמש, נוסף על תפקידם, גם כ-DPO, כמו המנכ"ל, מנהל משאבי אנוש או מנהל מערכות המידע. כמו כן, אין להכפיף את ה-DPO לנושא משרה בגוף עצמו או בגוף אחר אם הדבר עלול להעמידו בחשש לניגוד עניינים כאמור. הרשות להגנת הפרטיות הבהירה עוד במסמך המלצות למינוי הממונה הגנת פרטיות שפורסם בעבר כי ה-DPO אינו יכול לשמש גם כממונה אבטחת המידע. זאת, משום שתפקידו של DPO רחב יותר, וכולל, בין היתר, הנחיה מקצועית של ממונה אבטחת המידע באשר לאופן בו יש ליישם את דרישות האבטחה כדי לשרת את תכליות דיני הגנת המידע האישיו ו/או להבטיח שמירה מיטבית על הזכות לפרטיות בארגון.
- יצוין בהקשר זה כי בהחלטה משנת 2020 הטיחה הרשות להגנת המידע הבלגית יעצום כספי בסך 50,000 אירו על חברת טלקום שמינתה את קצין הציות שלה כממונה הגנת מידע, באופן שהפר את הוראות ה-GDPR. החלטות דומות התקבלו לאחר מכן במדינות האיחוד האירופי והנושא אף הגיע להכרעת בית הדין האירופי לצדק, שאשרר את איסור ההחזקה בשני כובעים מנוגדים כאמור.

מינוי ממונה על אבטחת מידע

מדובר בחובה שהייתה קיימת עוד לפני התיקון לחוק, אך עברה כמה שינויים. בעקבות התיקון, יהיו ארגונים שיידרשו למנות כעת הן DPO והן ממונה על אבטחת המידע.

מהים הגופים הנדרשים למנות ממונה על אבטחת מידע?

- בעל שליטה או מחזיק בחמישה מאגרי מידע החייבים ברישום או בהודעה לרשות להגנת הפרטיות. זהו תיקון לעומת הנוסח הקיים, שחייב רק מחזיק בחמישה מאגרי מידע במינוי.
- גוף ציבורי – משדרי 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.

אם זכיר כי תקנה 3 לתקנות אבטחת מידע קובעת שבין אם חלה חובה למנות ממונה אבטחת מידע ובין מנייה או למנהל פעיל שחלה חובה כזו, עליו להכין נוהל אבטחת מידע ולהביאו לאישור בעל המאגר. כן עליו להכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אבטחת מידע, לבצע אותה ולהודיע לבעל המאגר על ממצאיו.

בנוסף, תקנה 3 לתקנות אבטחת מידע קובעת כי ממונה אבטחת מידע יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק, או לנושא משרה בכירה אחר המכפוף ישירות למנהל המאגר. בנוסף, מנהל אבטחת המידע לא יכול לשמש כמנהל מאגר המידע וכן לא ישמש בתפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים. עמדת הרשות להגנת הפרטיות היא אפוא שממונה אבטחת המידע לא יכול לשמש גם כמנהל מערכות המידע של הארגון.

בניגוד ל-DPO, התיקון לא מצוין במפורש כי ממונה אבטחת מידע יכול אף הוא להיות חיצוני לארגון, אולם הרשות להגנת הפרטיות הבהירה כי לדעתה הדבר אפשרי.

חשוב לשים לב לכך שהממונה על אבטחת המידע חב באחריות אישית לאבטחת המידע (ס' 17ב(ב) לחוק), בניגוד ל-DPO, שאינו חב באחריות אישית.

הפניות:

- **חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024, ח"א 3287 מיום 14.8.24**
- צו הגנת הפרטיות (קביעת גופים ציבוריים), תשמ"ו-1986
- חוק התקשורת (בזק ושידורים), תשמ"ב-1982
- **מסמך המלצות מינוי ממונה הגנת הפרטיות בארגון ותפקידיו**
- תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017
- **שאלות ותשובות בנושא ממונה על אבטחת מידע**
- **מדריך עזר של ה-EDPB למינוי DPO**
- **ההחלטה של הרשות הבלגית על ניגוד עניינים**

לפרטים נוספים:



עו"ד דלית בן-ישראל, שותפה
ראש מחלקת IT, הגנת פרטיות וסייבר
dbenisrael@nblaw.com



עו"ד נעמה גורני לר
מחלקת IT, הגנת פרטיות וסייבר
ngorni@nblaw.com



עו"ד שריי אסולין
מחלקת IT, הגנת פרטיות וסייבר
sasulin@nblaw.com

שתפו:



עוד לא רשומים? [הירשמו לקבלת הניזולטר השבועי של נשיך ברנדס אמיר.](#)

אתם מזמנים לפנות אלינו באימייל עם כל שאלה ותגובה.

אין באמור בניזולטר כדי להוות עצה. הדרכה, ייעוץ או חוות הדעת בנושא, והוא מוגש כשירות ללקוח להעשרה כללית בלבד ולא לכל מטרה אחרת. בכל נושא ספציפי יש לפנות לעורכי הדין הרלוונטיים במשרד נשיך ברנדס אמיר.

