

## עדכון הגנת הפרטיות

### תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017

בחודש מאי 2017, פורסמו ברשומות תקנות חדשות בנושא הגנת הפרטיות. התקנות החדשות משנות הלכה למעשה את הדין הקיים ומייצרות הסדר חדש ומקיף לעניין החובות החלות בקשר להגנת הפרטיות במאגרי המידע.

התקנות קובעות סדרי ניהול וכללי עבודה בקשר עם ניהול והחזקה של מאגרי מידע וחלות על כלל הגופים והחברות במשק הישראלי המנהלים מאגרי מידע או מחזיקים במאגרי מידע.

אמנם התקנות יכנסו לתוקף רק ביום 8 במאי 2018, אך הן מחייבות היערכות מראש ובכלל זה בחינת המידע המוחזק במאגר ודרך ניהולו וביצוע התאמות הדרושות בפעילות הארגון ביחס למידע זה.

התקנות יוצרות הבחנה בין ארבעה סוגים של מאגרי מידע: (1) מאגר המנוהל בידי יחיד; (2) מאגר שחלה עליו רמת אבטחה בסיסית; (3) מאגר שחלה עליו רמת אבטחה בינונית; (4) מאגר שחלה עליו רמת אבטחה גבוהה.

החובות הקבועות בתקנות, שעיקריהן יפורטו להלן, חלות באופן שונה על סוגי המאגרים השונים. לפיכך, בשלב הראשון יש לקבוע את סיווג מאגר המידע, שעל פיו ייקבע היקף החובות החלות על בעל מאגר המידע, מנהל מאגר המידע וגם על מחזיק במאגר מידע, כהגדרתם בחוק הגנת הפרטיות.

נפרט להלן את עיקרי החובות:

**הגדרות המאגר** - יש לגבש מסמך הגדרות אשר יפרט להלן, חלות באופן שונה על סוגי המאגרים השונים. לפיכך, בשלב הראשון יש לקבוע את סיווג מאגר המידע, שעל פיו ייקבע היקף החובות החלות על בעל מאגר המידע, מנהל מאגר המידע וגם על מחזיק במאגר מידע, כהגדרתם בחוק הגנת הפרטיות.

**נוהל אבטחה** - יש לקבוע נהל אבטחת מידע בהתאם למסמך הגדרות המאגר ורמת האבטחה הנדרשת למאגר בהתאם להוראות התקנות. נהל אבטחה יקבע בין היתר הוראות בעניין האבטחה הפיזית והסיבית של אתרי המאגר, הרשאות גישה למאגר, תיאור אמצעים שמטרתם הגנה על מערכות המאגר, הוראות למורשי גישה למאגר לצורך הגנה על המאגר, הוראות לעניין התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע.

**מיפוי מערכות המאגר וביצוע סקר סיכונים** - יש לערוך מיפוי בכתב של מבנה המאגר וכן רשימה של המערכות בהן נעשה שימוש במאגר ובכלל זה, תשתיות ומערכות חומרה, מערכות התוכנה המשמשות להפעלתו של המאגר וניהולו, תוכנות וממשקים המשמשים לתקשורת עם מערכות המאגר, תרשים הרשת בה פועל המאגר, סקר לאיתור סיכונים אבטחת המידע, מבדקי חדירות למערכות המאגר לצורך בחינת עמידותן בפני סיכונים, ועוד.

**אבטחה באופן פיזי של המאגר** - יש להבטיח כי מערכות החומרה יישמרו במקום מוגן אליו תימנע כניסה ללא הרשאה. המקום צריך להתאים לאופי פעילות המאגר ורגישות המידע המצוי במאגר. כמו כן, יש לנקוט אמצעי בקרה ותיעוד של הכניסה והיציאה מהאתרים בהם מצויות מערכות בהן נעשה שימוש במאגר.

**אבטחת מידע בניהול כח אדם** - על מנת להבטיח כי הגישה למידע המצוי במאגר המידע תוענק לעובדים המתאימים לקבלת גישה למידע, יש לקבוע כי לא תוענק גישה למידע המצוי במאגר או ישונה היקף ההרשאה שניתנה לבעלי ההרשאה אלא אם כן ננקטו אמצעים סבירים אשר מקובלים בהליכי מיון עובדים ושיבוצם. בנוסף, כלל בעלי ההרשאות יידרשו לעבור הדרכות תקופתיות לעניין החובות הקבועות בחוק הגנת הפרטיות ובתקנות.

**ניהול הרשאות גישה** - הרשאות גישה למאגר ייקבעו בהתאם להגדרות תפקיד של המורשים ובמידה הנדרשת לביצוע התפקיד בלבד. כמו כן, יש לנהל רישום מעודכן של רשימת ההרשאות התקפות.

**תיעוד אירועי אבטחה** – יש לבצע תיעוד של מקרים במסגרתם התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מההרשאה. כמו כן, יש לערוך תחקורים פנימיים בנוגע לאירועי האבטחה ולבחון את מידת האבטחה של המאגר בהתאם לתדירות אשר משתנה לפי סוג המאגר.

**התקנים ניידים** – כידוע, התקנים ניידים הנם גורם סיכון למערכות מידע. התקנות מגבילות את האפשרות לחיבור של התקנים ניידים למערכות המאגר באופן ההולם את מאגר המידע ובהתחשב בין היתר ברמת אבטחת המידע שחלה על המאגר, רגישות המידע, הסיכונים המיוחדים אשר עשויים להיגרם למערכות בהן נעשה שימוש במאגר או הסיכון למידע שבמאגר כתוצאה מחיבור ההתקן הנייד.

**אבטחת תקשורת** - מערכות בהן נעשה שימוש במאגר המידע לא תחברנה לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום לנזק או שיבוש למחשב או לחומר במחשב. כמו כן, העברת המידע ממאגר המידע, ברשת האינטרנט או ברשת הציבורית, תיעשה באופן מוצפן.

**מיקור חוץ (outsourcing)** - במקרה של מתן גישה לגורם חיצוני למאגר אגב שירות של מיקור חוץ, יש לבחון לפני ביצוע ההתקשרות את סיכוני אבטחת המידע הכרוכים בהתקשרות. יש לקבוע בהסכם ההתקשרות עם הגורם החיצוני הוראות הקובעות בין היתר, את המידע שהגורם החיצוני רשאי לעבד, מטרת השימוש המותרת ומערכות המאגר שהגורם החיצוני רשאי לגשת אליהן. כמו כן, יש לקבוע את סוג העיבוד או הפעולה שהגורם החיצוני רשאי לבצע, משך ההתקשרות, אופן השבת המידע לידי בעל המאגר בסיום ההתקשרות, ואופן יישום החובות בתחום אבטחת המידע שהגורם החיצוני חייב בהן כמי שמחזיק במאגר המידע לפי הוראות התקנות. בנוסף, יש לקבוע הוראות לעניין חובות הדיווח של הגורם החיצוני לבעל מאגר המידע באופן ובתדירות הקבועים בתקנות.

**ביקורות תקופתיות** - יש לערוך ביקורת פנימית או חיצונית על ידי גורם בעל הכשרה מתאימה לעריכת הביקורת בנושא אבטחת מידע כדי לוודא שהוראות התקנות מתקיימות.

**גיבוי ושחזור של נתוני אבטחה** - יש לקבוע נהלים לגיבוי ושחזור הנתונים השמורים במאגר.

**לפרטים נוספים: עו"ד ניב סבר, שותף, ראש מחלקת הגבלים עסקיים, תחרות והגנת הפרטיות**  
**מ. פירון ושות', עורכי דין, טלפון: 03-7540800, מייל: [niv\\_s@firon.co.il](mailto:niv_s@firon.co.il)**

מובהר כי הסקירה דלעיל הינה סקירה כללית בלבד, אין בה כדי להוות חוות דעת משפטית ואין בה כדי להוות תחליף לקבלת יעוץ משפטי פרטני.