

יולי 2019

שנה לתקנות הגנת הפרטיות (אבטחת מידע) – 5 דברים שחשוב שתדעו

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("התקנות"), שנכנסו לתוקף לפני מעט יותר משנה, הרחיבו משמעותית את החובות, בתחום הגנת הפרטיות, שחלות על רוב החברות במשק. בעדכון לקוחות זה, נבקש לשתף אתכם ב-5 תובנות עיקריות מהשנה שחלפה מאז נכנסו התקנות לתוקף.

1. מה דורשות התקנות?

התקנות החילו שורה של דרישות מפורטות בתחום אבטחת מידע על כל ארגון שברשותו מאגר מידע הכולל מידע אישי, כגון מידע על עובדי החברה, מועמדים לעבודה, לקוחות וכדומה. בלב התקנות עומדת הדרישה לאמץ (וליישם) מדיניות כתובה לאבטחת המידע האישי בחברה, תוך התייחסות להיבטים כמו אבטחה פיסית, ניהול הרשאות גישה, אבטחת רשתות וניהול סיכונים.

כשלב ראשוני ביישום התקנות, החברה נדרשת למפות ולתעד את סוגי המידע האישי הנאספים או נשמרים על ידה, מטרות השימוש במידע, הגורמים שלהם גישה למידע ועוד. בנוסף, התקנות מחייבות, בנסיבות מסוימות, דיווח לרשם מאגרי המידע על שימוש במידע אישי בלא הרשאה או בחריגה מהרשאה או על פגיעה בשלמות המידע ("אירוע אבטחת מידע חמור"). כמו כן, התקנות מחייבות את החברה לבחון ולהסדיר (בהסכם) את היבטי אבטחת המידע והגנת הפרטיות בכל התקשרות עם גורם חיצוני המקבל גישה למידע אישי.

המשמעות היא יצירה של סטנדרט חדש ומחייב של אבטחת מידע אשר חל על רוב החברות במשק, שרבות מהן כבר נקטו או החלו לנקוט צעדים להטמעת התקנות.

2. כיצד התקנות השפיעו על הסכמים מסחריים?

בשנה שחלפה מאז כניסתן לתוקף, היבטי אבטחת מידע והגנת הפרטיות מוצאים ביטוי משמעותי מבעבר בהסכמים מסחריים. בין היתר, להסכמי שירותים רבים, המערבים גישה למידע אישי, נוספו הוראות בתחום הגנת הפרטיות ואבטחת מידע, כנדרש על-פי התקנות. כמו כן, אנו מזהים עליה ניכרת בהיקף העיסוק בהיבטי הגנת הפרטיות ואבטחת מידע במסגרת מיזוגים בין חברות והשקעות בהן (כחלק מבדיקת הנאותות, במסגרת המצגים שהמוכרת או חברת היעד נדרשות למסור וכו').

בין היתר, המשמעות היא שהפרה של התקנות לא רק שתחשוף את החברה המפרה לסנקציות מצד הרשות להגנת הפרטיות (כמפורט להלן), היא עשויה אף לחשוף את החברה לתביעה אזרחית בשל הפרת התחייבות חוזית, מקום שהחברה התחייבה לעמוד בדרישות לפי התקנות בהסכמים המסחריים עליהם היא חתומה.

3. האם חברה שהטמיעה את דרישות ה-GDPR עומדת בהכרח בדרישות התקנות?

ה-GDPR ("General Data Protection Regulation") של האיחוד האירופי קובעת עקרונות כלליים בתחום אבטחת המידע, בעוד שהתקנות כוללות הוראות פרטניות בדבר הצעדים שעל חברה לנקוט בתחום זה. לכן, אף שה-GDPR מציבה רף גבוה בתחום הגנת הפרטיות, ישנן חובות בתקנות שאינן מוצאות ביטוי מפורש ב-GDPR.

4. האם ישנה אכיפה?

הרשות להגנת הפרטיות נוקטת שורה של צעדי אכיפה ופיקוח בקשר עם הפרות של חוק הגנת הפרטיות, התשמ"א-1981 ("החוק") והתקנות. בין היתר, הרשות הקימה בשנת 2018 [מערך אכיפה - פיקוח רחב](#) הפועל, בין היתר, לאיתור הפרות. כחלק מהביקורות שמקיים המערך, נדרשים גופים המנהלים או מחזיקים מאגרי מידע אישי לספק מידע מפורט על האופן שבו הם מיישמים את התקנות. אמנם הרשות טרם פרסמה נתונים מדויקים על פעילות המערך, אך להערכתנו, נכון לעת כתיבת עדכון זה, נערכו ביקורות במאות חברות. כמו כן, על-פי פרסומי הרשות, במחצית השנייה של 2018 קיימה הרשות 86 הליכי אכיפה בעקבות אירועי אבטחת מידע חמורים.

5. מהן הסנקציות האפשריות?

בשל הפרה של התקנות, רשם מאגרי המידע רשאי להתלות או לבטל את רישומו של מאגר המידע הרלוונטי, באופן שלמעשה יאסור שימוש במאגר. כמו כן, במקרים מסוימים בהם נקבע כי חברה הפרה את החוק והתקנות, הרשות להגנת הפרטיות עשויה לפרסם את דבר ההפרה בפומבי. מעבר לפגיעה האפשרית במוניטין החברה, פרסום כזה עלול לחשוף את החברה לתביעה אזרחית בקשר עם ההפרה. נציין, כי בתחילת 2018 אישרה הכנסת, בקריאה ראשונה, הצעת חוק ממשלתית שתאפשר הטלה של עיצומים כספיים משמעותיים בגין הפרת התקנות. סביר להניח כי הממשלה והכנסת יפעלו לקדם את הצעת החוק לאחר הבחירות הקרובות.

לסיכום, התקנות מהוות ציון דרך חשוב מבחינת החקיקה בתחום הגנת הפרטיות בישראל והן חלק ממגמה גלובלית להחמרת הדרישות בתחום זה. בחלוף כשנה מכניסתן של התקנות לתוקף, ניכר שהן משפיעות על חברות ועסקאות רבות בישראל. על רקע האמור, ובשים לב לחשיפה שהפרת התקנות עלולה ליצור לחברה, קיימת חשיבות רבה להטמעת הדרישות לפי התקנות. הטמעה הולמת של דיני הגנת הפרטיות בחברה עשויה לא רק להפחית את החשיפה המשפטית והרגולטורית שניצבת בפני החברה, אלא גם לתרום למוניטין שלה ולהגביר את האמון בחברה מצד עובדיה ולקוחותיה.

לפרטים נוספים:



עו"ד אסף הראל, שותף
assafh@gornitzky.com