

מרץ 2020

עדכון לקוחות: עמידה בתקנות הגנת הפרטיות ביחס לעבודה מרחוק בעקבות התפשטות נגיף הקורונה

זמן קריאה: 1 דקה

לאור להתפרצות נגיף SARS-CoV-2 הגורם למחלת Covid-19 (להלן – "הקורונה") ובשים לב להנחיות המתעדכנות של משרד הבריאות והממשלה, חברות וארגונים רבים במשק עוברים לשיטת עבודה מרחוק/עבודה מהבית. פתרון זה שומר על מהלך העסקים, אך עלול לחשוף את הארגון לסיכוני סייבר ולחשיפה ביחס לעמידה בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן – "התקנות").

נזכיר, כי התקנות חלות ביחס לכל מאגר מידע אשר כולל מידע אישי (כגון מידע על עובדי החברה, לקוחותיה וכדומה) (להלן – "מאגר מידע") ועל כן מחייבות למעשה את רוב החברות במשק. בעדכון זה נבקש לעמוד על החובות העיקריות החלות, מכח התקנות, בקשר עם עבודה מרחוק.

התקנות קובעות חובות ספציפיות ביחס לאבטחת התקשורת אל מאגר המידע ומערכות המשמשות את המאגר:

- יש להימנע מלחבר את המערכות המשמשות את מאגר המידע לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב (למשל, התקנת תוכנת Firewall או תוכנת אנטי-וירוס).
- העברת מידע אישי באינטרנט (או ברשת ציבורית אחרת) תיעשה תוך שימוש בשיטות הצפנה מקובלות.
- במאגר מידע שניתן לגשת אליו מרחוק (למשל – "חיבור מהבית"), יש לעשות שימוש באמצעים שמזהים את המתקשר ומאמתים את זהותו. במאגרי מידע ברמת אבטחה בינונית או גבוהה (בהתאם לסיווג שנקבע על פי התקנות) ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה (כגון כרטיס חכם).

בהקשר זה, נציין כי על רקע משבר הקורונה, מערך הסייבר הלאומי פרסם לאחרונה [המלצות הגנה לארגונים לעבודה מהבית](#). מטרת ההמלצות היא לצמצם את סיכוני הסייבר כתוצאה מעבודה מהבית של עובדים.

קיימת חשיבות רבה לנקיטת אמצעי אבטחת סייבר הולמים (לרבות העלאת מודעות בקרב עובדים) כדי להבטיח את הרציפות התפקודית של הארגון ולצמצם חשיפה משפטית. הדברים נכונים ביתר שאת בימים אלה, בהם אנו עדים לעליה חדה במספר המתקפות על ארגונים בחסות המשבר.

צוות הסייבר והפרטיות במשרדנו ערוך לסייע גם בנסיבות מאתגרות אלו ויהיה זמין לכל הבהרה שתידרש בעניינים שבנדון ובכלל.

לפרטים נוספים:

אסתר שנטר, עו"ד
astars@gornitzky.com



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

