אכיפת תקנות הגנת הפרטיות – כדאי לדעת

מרץ 5 , 2019

הגנת פרטיות המידע הינה נושא העולה חדשות לבקרים. לא פעם אנו שומעים על פרצות אבטחה המתגלות אצל ענקיות הטכנולוגיה דוגמת פייסבוק, גוגל ואפל, האוספות ומחזיקות בכמות אדירה של מידע אישי אודות המשתמשים שלהן.

אלא שהחובה לשמור ולהגן על פרטיותו של כל אדם אינה מנת חלקן של חברות הענק בלבד, והיא חלה על כל בעל עסק אשר חלק מעיסוקו כרוך באיסוף ושמירה של מידע אודות לקוחותיו, עובדיו וכדומה (מאגרי מידע). תקופת ההסתגלות לתקנות הגנת הפרטיות (אבטחת מידע), התשל"ז ,2017 – אשר נכנסו לתוקף בחודש מאי 2018, הסתיימה והרשות להגנת הפרטיות הודיעה כי החל מחודש ינואר 2019 תתבצע פעולת אכיפה מאסיבית של תקנות אלו, בעיקר בכל הנוגע לאירועי אבטחת מידע חמורים.

הרשות תחמיר במיוחד בעת טיפולה בגופים אשר יימצא לגביהם כי הפרו את החובות המוטלות עליהם מכוח חוק הגנת הפרטיות והתקנות. כך למשל, אם גוף יימנע מדיווח לרשות אודות קיומו של אירוע אבטחה חמור, או שינסה להסתיר את פרטיו, או שיתגלו ממצאים חמורים באופן הטיפול בו, תפעל הרשות במלוא החומרה ואף תישקל התלייתו או ביטול רישומו של מאגר המידע של הגוף המפר, באופן האוסר על השימוש במידע. מלבד הטיפול הישיר בגוף המפר, מתכננת הרשות לפרסם הפרות של חובות שהוגדרו בתקנות (אלא אם מדובר במקרים "קלים")[1].

<u>אז איך נערכים ואיך פועלים במקרה של אירוע אבטחה?</u>

על מנת להבטיח את פרטיות המידע במאגר, על בעל העסק להטמיע ולקיים את הוראות התקנות, תוך שימת דגש על רמת האבטחה של מאגר המידע (בסיסית, בינונית או גבוהה). עם זאת, ייתכנו אירועי אבטחה[2] (בעלי דרגות חומרה שונות) גם כאשר בעל העסק יישם את כל דרישות אבטחת המידע.

עם קרות אירוע אבטחה, יידרש העסק לתעד את האירוע לשם הפקת לקחים ומניעת מקרים דומים בעתיד, וכן יצטרך לתעד את הפעולות שננקטו בעקבות אירוע האבטחה. אירוע אבטחה הנופל לגדר הגדרה של "אירוע אבטחה חמור"[3] יטיל על בעל המאגר את החובה להודיע על כך לרשות הגנת הפרטיות תוך 24 שעות ממועד גילויו ובכל מקרה לא יאוחר מ72- שעות, וכן לדווח על הצעדים שנקט בעקבות האירוע. רשם הגנת הפרטיות מוסמך להורות לעסק שאירע בו אירוע אבטחה חמור לדווח על אירוע כאמור לנושאי המידע שעלולים להיפגע ממנו.

ביום 28 בינואר 2019, המוכרז כיום הגנת הפרטיות הבינלאומי, פרסמה הרשות להגנת הפרטיות נתונים אודות אירועי אבטחה חמורים אשר תועדו מאז כניסת התקנות לתוקף. על פי נתונים אלה, עולה כי הסיבות השכיחות ביותר לקיומו של אירוע אבטחה חמור הן תקיפות סייבר ,(35%) טעויות אנוש ,(15%) שימוש לרעה (7%) ותקלות טכניות. כך שלצד חיזוק אמצעי אבטחת המידע בכל עסק או ארגון, מומלץ לקיים הדרכות לבעלי הרשאות למאגר מידע ולחדד במסגרתן את נהלי האבטחה ושמירה על פרטיות המידע. יש בפעולות אלו כדי לצמצם את הסיכון לאירוע אבטחה.

עם זאת, מאחר שלא ניתן להבטיח הגנה מוחלטת אף כאשר ננקטים כל האמצעים הנדרשים על פי התקנות כחלק משגרת העסק, קיימת חשיבות רבה לנקיטת צעדים מידיים בגין אירוע אבטחה ודיווח לרשות הגנת הפרטיות במועד במידה ומדובר באירוע אבטחה חמור.

<u>אלכסנדרה כהן</u>
עורכת דין

אלכסנדרה כהן הינה עורכת דין
בגילת, ברקת ושות'

[1] ר' https://www.gov.il/he/departments/news/enforcement2

[2] אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה.

[3] רלוונטי למאגרי מידע ברמת אבטחה בינונית / גבוהה – אירוע שנעשה בו שימוש במידע מן המאגר (אם מדובר במאגר ברמת אבטחה גבוהה) או בחלק מהותי מן המאגר (אם מדובר במאגר ברמת אבטחה בינונית), בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע.

These newsletters are provided for general information only. It is not intended as legal advice or opinion and cannot be relied upon as such.