הרגולציה החדשה להגנת סייבר בחברה

התקנות החדשות להגנת הפרטיות בישראל ובאירופה מעוררות שאלות נוקבות בקרב מנהלי חברות ותאגידים. מדריך קצר על הרגולציה החדשה להגנת סייבר בחברה | **יואל צפריר**

בראשית חודש מאי נכנסו לתוקפן תקנות הגנת הפרטיות (אבטחת מידע) המהוות שדרוג משמעותי והכרחי לחקיקה הקיימת. התקנות מגדירות מאגרי מידע שחלים עליהם רמות אבטחה בסיסית, גבוהה ובינונית, ואת הסטנדרטים הנדרשים לכל מאגר בהתאם לרמת האבטחה שלו. בין היתר, קובעות התקנות את הנסיבות בהן יש להכין נוהל אבטחת מידע, לבצע סקר סיכונים, לבצע ביקורות תקופתיות לאבטחת המידע, כיצד להתנהל בעת שמתרחש אירוע אבטחת מידע והאם חובה לדווח על האירוע ועוד.

גם באירופה חל שינוי משמעותי בנושא זה, שינוי המשפיע גם על ישראל. ב- 25.5.2018 נכנסו לתוקף הוראות ה-GDPR (General Data Protection Regulation), רגולציה חדשה של האיחוד האירופאי הקובעת סטנדרטים וכללים לשמירה על פרטיות המידע ואבטחתו.

"אחד המאפיינים הבולטים של ה-GDPR הוא המקום הנרחב שמוענק לזכות של 'נושא המידע' (הגורם אודותיו נאסף המידע) על המידע שלו. בהתאם לזאת, איסוף המידע חייב להיות מאושר ותכליתי", אומר **עו"ד אלון פומרנץ**, השותף המנהל וראש מחלקת ליטיגציה ויישוב סכסוכים במשרד עוה"ד ליפא מאיר ושות' המתמחה בתחום הסייבר. " הוגדרו הזכויות של נושא המידע להחליט לגבי השימוש במידע שלו, כגון, הזכות לבקש 'להישכח' ולמחוק את המידע הנאסף עליו, או להתנגד ליצירת פרופיל התנהגותי. כמו כן, בדומה לתקנות הישראליות, גם ה-GDPR עוסק בהתנהלות הראויה בעת אירוע אבטחת מידע וחובת דיווח על אירוע שכזה, בהתאם לנסיבות".

ה-GDPR חל גם על חברות שמחוץ לאיחוד

לדברי עו"ד פומרנץ, מאפיין בולט נוסף של ה-GDPR הוא האחריות הרבה המוטלת על בעל השליטה במידע ועל מעבד המידע. בעל השליטה במידע מחוייב ליישם אמצעים טכניים וארגוניים הולמים להגנת המידע. על אף הרגולציה, עו"ד פומרנץ מעריך שאנו רק בתחילת הדרך ועוד לא הגענו ליעד. הרגולציה תקבל את הפרשנות שלה בשנים הקרובות, ובהתאם להתפתחות המהירה של הטכנולוגיה, צפויה עוד רגולציה ופרשנות רבה.

כיצד אתה רואה את שילוב התקנות עם המציאות הקיימת בשטח?

"באירופה ובארה"ב שכיח שחברות משקיעות סכומי כסף נכבדים לביצוע צעדים מומלצים להגנת סייבר, אולם בארץ אנו רואים שחברות רבות חששו או נמנעו עד עתה מלהשקיע כספים רבים לשם אבטחת סייבר בחברה. זאת, מהיעדר מודעות או מהיעדר הפנמה של הסיכון, או משיקולי עלות-תועלת: מנהל חברה מעדיף לחסוך בטווח הקצר ומוכן לקחת את הסיכון שהחברה תותקף ותינזק, במקום להשקיע עשרות ואף מאות אלפי שקלים לשם הגנת סייבר טובה לחברה. ואולם, כעת התקנות קובעות סטנדרטים שלמעשה מחייבים את החברות שברשותן מאגרי מידע, כל חברה ונסיבותיה המיוחדות, ברמת אבטחת מידע מסויימת".

עו"ד אלון פומרנץ | צילום: קובי קנטור

בדרך כלל חוק של האיחוד האירופי לא גורם לתסיסה רבה בקרב החברות הישראליות, אולם התחושה הפעם היא כי ה-GDPR יצר בהלה בנושא אפילו בישראל. מה לדעתך גרם לכך?

"זוהי נקודה נכונה. אני סבור כי שני גורמים עיקריים גורמים לכך. האחד, הסנקציות שה-GDPR מטיל, אשר יכולות להגיע בנסיבות מסויימות לקנס בסך של 20 מיליון אירו למי שמפר את הוראות ה-GDPR. השני, ה-GDPR אינו תקף אך ורק כלפי חברות שפעילותן מתרכזת במדינות האיחוד האירופי, אלא בנסיבות מסויימות הוא חל גם על חברות מחוץ למדינות האיחוד אשר מחזיקות ומעבדות מידע על אזרחים הנמצאים באיחוד האירופי. כך, הרבה חברות שיושבות בארץ ומעבדות מידע על נושאי מידע הממוקמים במדינות האיחוד האירופי יתכן וכפופות ל-GDPR, על אף שהפעילות עצמה מתבצעת בישראל".

נוהל מסודר להתמודדות עם אירוע סייבר

אז מה חברה יכולה לעשות כדי להיות בטוחה מפני תקיפות סייבר?

"כדאי להבהיר נקודה חשובה - אף חברה לא תהא חסינה ב-100% מפני התקפות סייבר, גם אם תחשוב שאכן נקטה בכל האמצעים הנדרשים. עם זאת, בדומה לאמצעים הננקטים למניעת פריצה לבית, כגון התקנת סורגים ואזעקה משוכללת, על החברה לנקוט בצעדים הנדרשים על מנת להתריע ולהרתיע מפני ביצוע של התקפות סייבר כלפיה, להקשות על התוקף ולגלות בזמן אמת ניסיון תקיפה. האמצעים המומלצים רבים ומשתנים בהתאם לגוף שזקוק להגנת סייבר והרגישויות שיש לו. לצד צעדי האבטחה בצד הטכנולוגי, כמו גם עריכת סקר סיכוני סייבר, מומלץ לפנות לייעוץ משפטי מקצועי בנושא, על מנת שניתן יהיה לבחון היטב את הנסיבות והמאפיינים של החברה, הרגולציה הרלוונטית לה והשלכות אירוע סייבר פוטנציאלי על החברה. בהתאם, תגובשנה המלצות לנקיטת הצעדים הרלוונטיים להתגוננות אופטימלית, כמו גם הכנה להתמודדות עם אירוע סייבר בזמן אמת".

אתה מעריך שנראה התפתחות בהגשת תובענות ייצוגיות או נגזרות בעקבות תוצאות ונזקי תקיפות סייבר?

"כן. לכן ההמלצה שלי היא להכין נוהל מסודר להתמודדות עם אירוע סייבר בזמן אמת, לרבות צוות תגובה שיודע לנתח את האירוע, לפעול במהירות, לתת המלצות למקבלי ההחלטות ולהדריך אותם במהלך האירוע ולאחריו. ההתמודדות היא לא רק בצד הגנת הסייבר הטכנולוגית, אלא גם בחזית המשפטית ובחזית התקשורתית. הבנת הסיכונים וההשלכות האפשריות מראש, עשויה למנוע נזקי עתק בתביעות ובפגיעה במוניטין של החברה. בכלל, על החברה לקבל ייעוץ משפטי מקצועי האם היא התאימה את התנהלותה ואת אמצעי המיגון שלה להוראות הרגולציה הרלוונטית, וכן האם היא נקטה באמצעים הסבירים הנדרשים לשם הגנה על מערכות המידע שלה ולשם התמודדות עם טענות ותביעות עתידיות בעקבות מתקפת סייבר. גם בעניין זה 'סוף מעשה במחשבה תחילה'".