



לקוחות נכבדים,

ביום 21 במרץ 2017, אושרו בוועדת חוקה, חוק ומשפט של הכנסת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "התקנות"). התקנות מהוות מהפכה של ממש בתחום רגולציית אבטחת המידע בישראל, והן מטילות חובות משמעותיות על בעלי מאגרי מידע לאבטחת המידע שברשותם. בין החובות הכלולות בתקנות: אימוץ מדיניות מחייבת ונוהלי אבטחת מידע מקיפים, מיפוי מערכות המידע בארגון וביצוע סקר סיכונים, הטמעת תפיסות אבטחת מידע בניהול כוח האדם בארגון, וחובות דיווח על אירועי אבטחה. בנוסף, ביחס למאגרי מידע בעלי רגישות גבוהה, התקנות קובעות גם ביצוע מבדקי חדירות והטמעת אמצעי אבטחה מתקדמים. התקנות ייכנסו לתוקף בתום שנה מיום פרסומן.

רמות אבטחה שונות של מאגרי מידע

ככלל, התקנות יחולו על כל מאגר מידע שחייב ברישום לפי חוק הגנת הפרטיות. עם זאת, חלק מההוראות יחולו רק על מאגרי מידע ברמת אבטחה בינונית או גבוהה, אשר יהיו כפופים לנהלים מחמירים יותר. מאגרי מידע **ברמת אבטחה בינונית** כוללים, בין היתר, מאגרים הכוללים מידע רפואי, מידע על צנעת חייו של אדם, מידע על דעותיו הפוליטיות או אמונותיו של אדם, מידע ביומטרי, מידע כלכלי לרבות מידע על הרגלי צריכה של אדם, וכן מאגרי מידע שנועדו לצורך דיוור ישיר. מאגרי מידע **ברמת אבטחה גבוהה** הם מאגרים הכוללים מידע רגיש כמפורט לעיל הכוללים פרטים על 100,000 אנשים ומעלה, או שמספר מורשי הגישה אליהם עולה על 100.

מסמכי מדיניות, נהלים ובעלי תפקידים

התקנות מחייבות כל בעל מאגר מידע לאמץ מסמך מדיניות המגדיר את מטרות המאגר, את סוגי השימושים בו, את הסיכונים העיקריים לפגיעה באבטחתו ואת דרכי ההתמודדות עמם. על מסמכי המדיניות להתעדכן מעת לעת ולשקף נכונה את אופן השימוש במאגרים כפי שנעשה בפועל על ידי הארגון.

*
תקנות אבטחת
מידע

מוזמנים לבקר אותנו:

<http://www.fbclawyers.com>

ולעקוב אחרינו:



בנוסף, כל בעל מאגר מידע יחויב לקבוע נוהל אבטחת מידע בהתאם להגדרות מאגרי המידע שברשותו. הנוהל יחייב את כל עובדי הארגון ויטייחס, בין היתר, למיפוי מערכות המידע בארגון ואבטחתן, למדיניות הרשאות הגישה למאגרי המידע ולמערכות המידע, לאמצעי אבטחת המידע המוטמעים בארגון, לסיכוני אבטחת המידע הקיימים בארגון ודרכי ההתמודדות עמם ולאופן ההתמודדות עם אירועי אבטחת מידע בזמן אמת. בעלי מאגרי מידע ברמת אבטחה בינונית או גבוהה יצטרכו לכלול גם התייחסות לגיבוי המידע שברשותם, לעריכת בדיקות תקופתיות ולשימוש בהתקנים ניידים בארגון.

בנוסף, התקנות קובעות כי ממונה אבטחת המידע לפי חוק הגנת הפרטיות (בין אם חלה חובה חוקית למנותו ובין אם מונה באופן וולונטרי), לא ימלא תפקיד אחר בארגון שעלול לגרום לו להימצא בניגוד עניינים (למשל, מנהל מערכות המידע בארגון), ויהיה כפוף למנכ"ל או לנושא משרה בכיר אחר. עוד קובעות התקנות, כי על הארגון להעמיד לרשות הממונה את המשאבים הנדרשים כדי לציית להוראות התקנות.

מיפוי מערכות מידע, סקרי סיכונים ומבדקי חדירות

בנוסף למסמכי המדיניות ולנהלים הפנימיים, בעלי מאגרי מידע יחויבו לערוך ולהחזיק מסמך הממפה את מערכות המידע הנוגעות לכל מאגר ומאגר (לרבות חומרה, תוכנה וציוד קצה) ואת אמצעי האבטחה החלים עליהן. בעלי מאגרי מידע ברמת אבטחה גבוהה יידרשו גם לערוך סקרי סיכונים ומבדקי חדירות למערכות המידע שברשותם אחת ל-18 חודשים, לדון בתוצאותיהם ולאמץ נהלים ואמצעי אבטחה בהתאם למסקנות הנובעות מהם.

אמצעי אבטחת מידע

בעלי מאגרי מידע יחויבו לפי התקנות להטמיע אמצעי אבטחת מידע שונים בארגון. כך למשל, יהיה על בעלי מאגרי מידע לדאוג, בין היתר, לאבטחה פיזית של המאגר, לניהול הרשאות גישה בארגון, לקביעת מנגנוני זיהוי ואימות (לרבות סיסמאות חזקות ואמצעי זיהוי חכמים), לתיעוד של אירועי אבטחה במערכות המידע, להפרדה בין מערכות המידע השונות הנוגעות למאגר ולהצפנת העברת מידע מהמאגר ברשתות ציבוריות.

בנוסף, בעלי מאגר מידע ברמת אבטחה בינונית וגבוהה יחויבו לתעד את הגישה הפיזית למערכות המידע בארגון, להנהיג מנגנון קפדני של זיהוי ואימות משתמשים (לרבות מנגנוני ניתוק אוטומטיים וזיהוי באמצעים פיזיים), לתעד באופן אוטומטי את הגישה האלקטרונית למערכות המידע בארגון, ולשמור את נתוני התיעוד במשך 24 חודשים לפחות. עוד מורות התקנות כי על בעל המאגר לקבוע נהלים הנוגעים לגיבוי ושחזור המידע ולבצע אחת ל-24 חודשים לפחות ביקורת פנימית או חיצונית שמטרתה לבחון את הציות להוראות התקנות.

אבטחת מידע בניהול כוח אדם

התקנות מחייבות בעלי מאגרי מידע לנקוט בהליכים הולמים על מנת לוודא שעובדים שיש להם גישה למאגר מידע מתאימים לקבלת המידע המצוי בו, וזאת בשים לב לרגישות המידע. בנוסף, בעלי מאגרי מידע יחויבו לקיים הדרכות לעובדים בטרם יקבלו גישה למאגרי המידע. בעלי מאגרי מידע ברמת אבטחה בינונית וגבוהה יחויבו לקיים פעילות הדרכה תקופתית לעובדיהם אחת לשנה לפחות. חובות אלה תחולנה גם על **עובדים המועסקים בארגון כיום** ולהם גישה למאגר המידע.

דיווח על אירועי אבטחת מידע

בנוסף להוראות הנוגעות לאמצעי אבטחת המידע שעל הארגון לנקוט, התקנות מטילות על ארגונים שחוו אירוע אבטחת מידע, לדווח על כך – במקרים מסוימים – לרשם מאגרי המידע. התקנות מעניקות לרשם מאגרי המידע סמכות להורות לאותו ארגון לדווח על אירוע האבטחה גם לכל מי שמידע אודותיו נחשף בעקבות אותו אירוע.

סיכום

התקנות מהוות מהפכה של ממש ברגולציית אבטחת המידע בישראל ותחולתן רחבה מאוד. נבהיר בשנית, כי כל בעל מאגר מידע החייב ברישום יהיה **כפוף לפחות לחלק מהתקנות**. על אף שהתקנות אינן קובעות אלו אמצעי אבטחת מידע על בעל מאגר המידע להטמיע, הן מחייבות נקיטת שורה של אמצעים תאגידיים, ניהוליים וטכנולוגיים המותאמים לסוגי המידע השמורים על ידי הארגון ולשימושים שנעשים בו, ולכן הן מחייבות בחינה פנימית והיערכות מתאימה על ידי כל חברה וחברה.

על אף שהתקנות תיכנסנה לתוקף בתום שנה מיום פרסומן, אנו ממליצים להתחיל להיערך לקראת מועד זה כבר כעת, שכן היערכות זו כוללת היבטים משפטיים וטכנולוגיים אשר עשויים להצריך שיתוף פעולה בין אנשי מקצוע שונים, בתוך הארגון ומחוצה לו.

עדכון זה נכתב על-ידי עו"ד עמרי רחום-טוויג.

אנו עומדים לרשותכם בכל שאלה או הבהרה ונשמח לסייע ככל הנדרש.
למידע נוסף ניתן לפנות אל :

03-6941320

adat@fbclawyers.com

עמית דת

.....
הכלול באגרת מידע זו הוא מידע כללי בלבד, הוא אינו חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו. כל הזכויות שמורות לפישר בכר חן וול אוריון ושות'.
<mailto:newsletter@fbclawyers.com> - להסרה מרשימת התפוצה