

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017

ביום 21 במרץ 2017, אישרה ועדת חוק, חוקה ומשפט את תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("התקנות"). בכך מסתיים הליך חקיקה שהחל ברשות למשפט, טכנולוגיה ומידע בשנת 2010 ובמסגרתו פורסמו טיוטות לתגובות הציבור. התקנות כוללות רפורמה מרחיקת-לכת בהשוואה לתקנות המיושנות משנת 1986 שזה מכבר לא התאימו לאתגרי הזמן הזה. בין השאר, לראשונה בישראל, הן מטילות במקרים מסוימים חובה לדווח לרשם מאגרי המידע על אירועי אבטחה במאגר. חובות כאלה מצויות במדינות זרות והן הובילו לגל של תובענות ייצוגיות נגד בעלי מאגרים שנפרצו.

ממתי התקנות בתוקף?

התקנות ייכנסו לתוקף תוך שנה מיום פרסומן.

על מי יחולו התקנות?

על כל הבעלים, המנהלים והמחזיקים של מאגרי מידע בישראל. כל הארגונים, החברות והגופים הציבוריים בישראל כפופים לתקנות, שהוצאו מכוח חוק הגנת הפרטיות, התשמ"א-1981 ("החוק") ובעקבות פרסומן יהיה עליהם לבחון את נהלי אבטחת המידע שברשותם ולהתאימם לדרישות החדשות.

הגדרות מאגרי מידע ברמת אבטחה בינונית וגבוהה

התקנות מחלקות את המאגרים לארבע קבוצות, הנדרשות לרמת אבטחה הולכת וגוברת: (א) מאגרי מידע המנהלים על-ידי יחיד; (ב) מאגרי מידע שרמת האבטחה בהם היא בסיסית; (ג) מאגרי מידע שרמת האבטחה בהם היא בינונית; (ד) מאגרי מידע הנדרשים לרמת אבטחה גבוהה.

- **מאגר מידע המנוהל על-ידי יחיד.** מאגר מידע שמנהל יחיד או תאגיד בבעלות יחיד שרשות הגישה אליו מסורה ללא יותר משלושה אנשים, ובלבד שמטרתו אינה איסוף מידע לצורך מסירתו לאחר (לדוגמה: שירות דיוור ישיר), הוא אינו מכיל מידע על מעל 10,000 אנשים ואינו כולל מידע הכפוף לחובת סודיות מקצועית לפי דין או לפי אתיקה מקצועית.
- **מאגרי מידע ברמת אבטחה בסיסית.** מאגרי המידע שאינם מנהלים בידי יחיד ואינם באים בגדר הקבוצות הבאות – כלומר אינם נדרשים לרמת אבטחה בינונית או גבוהה.
- **מאגר מידע ברמת אבטחה בינונית.** מאגר מידע שמספר מורשי הגישה אליו גדול מעשרה, ומטרתו היא איסוף מידע לצורך מסירתו לאחר (לדוגמה: שירות דיוור ישיר), או שהוא בבעלות גוף ציבורי או שיש בו מידע רגיש. מידע רגיש כזה כולל, בין השאר, מידע רפואי, מידע גנטי, מידע על אמונותיו ודתו של אדם, על הרשעותיו בפלילים, מידע ביומטרי ומידע על נכסיו של אדם, התחייבויותיו הכלכליות ומצבו הכלכלי ("מידע כלכלי"). לראשונה, מהותו של מידע כלכלי מובהרת כך שהיא כוללת גם מידע על הרגלי הצריכה של אדם.
- **מאגרי מידע ברמת אבטחה גבוהה.** (א) מאגר מידע, לרבות מאגר של גוף ציבורי, שמטרתו לאסוף מידע לצורך מסירתו לאחר ויש בו מידע אודות 100,000 אנשים ומעלה או שמספר מורשי הגישה למידע עולה על 100; (ב) מאגר המכיל מידע רגיש אודות 100,000 אנשים ומעלה או שמספר מורשי הגישה למידע בו עולה על 100.

לתשומת לב: הדרישה שמספר מורשי הגישה למידע רגיש יעלה על 100 מכניסה להערכתנו מאגרי מידע רבים לגדר המאגרים שרמת האבטחה הנדרשת בהם היא המחמירה ביותר. הסיבה נמצאת בהכללתו של "מידע כלכלי" בגדר מידע רגיש.

חובות החלות על כל מאגרי המידע מלבד מאגרי מידע המנוהלים על-ידי יחיד

- **ניסוח מסמך הגדרות המאגר.** על בעל מאגר לערוך מסמך הגדרות המפרט באופן ברור בין היתר: תיאור כללי של פעולות האיסוף והשימוש במידע, תיאור מטרת השימוש במידע, פירוט סוגי המידע, פרטים בנוגע שימוש במידע מחוץ לגבולות המדינה, שמו של מנהל מאגר המידע, מחזיק במאגר ושל הממונה על אבטחת מידע. בנוסף עליו להכיל פירוט פעולות עיבוד מידע באמצעות מחזיק המאגר והסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עמם.
- **אבטחה פיזית.** יש לשמור את מערכות המאגר במקום מוגן המונע חדירה וכניסה בלא הרשאה.
- **ממונה על אבטחת מידע.** החוק מחייב למנות ממונה על אבטחת מידע בגופים ציבוריים, חברות פיננסיות או בחברות המחזיקות בחמישה מאגרי מידע החייבים ברישום. במטרה להבטיח את עצמאותו, התקנות מגדירות כי הממונה יוכפף במישרין למנהל המאגר או למנהל הפעיל של הגוף שהוא בעל המאגר או המחזיק בו. הן אוסרות על ממונה האבטחה להימצא במצב של ניגוד עניינים, ומחייבות אותו להכין נוהל אבטחת מידע ותכנית לבקרה שוטפת על העמידה בתקנות. את ממצאי התכנית עליו להביא לידיעת בעל המאגר ומנהלו.
- **נוהל אבטחה.** הנוהל יחייב את כל העובדים ויכיל בין היתר הוראות בדבר האבטחה הפיזית והסביבתית באתרי המאגר, ניהול ושימוש בהתקנים ניידים, פירוט הרשאות הגישה, הנחיות למורשי גישה למאגר המידע, תיאור של אמצעים שמטרתם הגנה על מערכות המחשוב והסיכונים אליהם חשוף המאגר. בנוסף, על נוהל האבטחה להכיל נוהל התמודדות עם אירוע אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע.
- **מיפוי מערכות.** בעל המאגר נדרש לערוך רשימה מעודכנת של כל רכיבי מערכות המחשב הקשורות למאגר המידע. על הרשימה להכיל מערכות חומרה ותוכנה המפורטות בתקנות, ותיאור של ארכיטקטורת הרשת שבה מוצב המאגר.
- **ניהול כח אדם, הרשאות גישה, זיהוי ואימות.** על בעל המאגר לקלוט לעבודה הקשורה למאגר עובדים שרמת סיווגם תואמת לרגישות המאגר. בנוסף עליו לנהל רישום של בעלי הרשאות גישה בהתאם לתפקידם ולנקוט אמצעים על-מנת לוודא כי גישה למידע תינתן למורשי גישה ובמידה הנדרשת לביצוע תפקידם.
- **תיעוד אירועי אבטחה.** על בעל המאגר לנהל תיעוד של כל אירוע המעלה חשש לפגיעה במידע או חריגה מהרשאות הגישה במערכות המידע. עליו להתבסס ככל הניתן על רישומים אוטומטיים של האירועים הללו.
- **התקנים ניידים.** יש להגביל התחברות של התקנים ניידים – לאפטופים, סמארטפונים וגם Disk on Keys לסוגיהם - למערכות המאגר, באופן המתחייב מרגישות המידע ורמת האבטחה של המאגר.
- **הפרדת מערכות.** על בעל מאגר להפריד, ככל האפשר, בין מערכות המאגר מהן יש גישה למידע לבין מערכות מחשוב אחרות שבבעלותו.
- **אבטחת תקשורת.** במידה ומערכות המאגר מחוברות לאינטרנט יש להתקין אמצעי הגנה מתאימים מפני חדירה בלתי מורשית ומפני נזקות. בנוסף, חובה להשתמש בהצפנה בעת העברת מידע באינטרנט ולהסדיר את גישת העובדים למאגר המידע מרחוק באמצעי זיהוי.

- **מיקור חוץ.** עיבוד מידע בידי צד ג' מחייב בחינה מוקדמת של סיכויי אבטחת המידע בהתקשרות וקביעת הוראות חוזיות מפורשות בנושאים כדוגמת מטרות השימוש במידע, סוג העיבוד, משך ההתקשרות, אופן החזרת המידע בסיום ההתקשרות ועוד.

חובות החלות על מאגרים ברמת אבטחה בסיסית

בנוסף לחובות הכלליות, התקנות מטילות חובות נוספות על בעלי מאגרים אלה:

- **בחינת נוהל האבטחה.** אחת לשנה בעל מאגרי מידע יבחן את הצורך בעדכון נוהל האבטחה.
- **אבטחת מידע בניהול כח אדם.** לפני הענקת הרשאה או לאחר שינוי היקף הרשאות גישה, בעל מאגר יעביר הדרכה למורשי גישה למאגר בנוגע לנוהל האבטחה והוראות אבטחת מידע לפי התקנות והחוק.
- **משך שמירת מידע אודות יישום התקנות.** מידע שנאסף בקשר ליישום הוראות התקנות - ובכלל זה תיעוד אירועי אבטחת מידע, מידע בדבר אבטחת תקשורת, הרשאות גישה, תהליכי זיהוי ואימות ועוד – יישמר למשך 24 חודשים.

חובות החלות על מאגרים ברמת אבטחה בינונית

בנוסף לחובות החלות על כל המאגרים, התקנות מטילות חובות ייעודיות על בעלי מאגרים אלה:

- **אבטחה פיזית וסביבתית.** חובה לתעד את הכניסות והיציאות ממתקני המאגר, ולתעד הכנסה והוצאה של ציוד על מנת לבצע מעקב ובקרה במקרה של כשל אבטחתי.
- **הרחבת נוהל האבטחה.** עליו לכלול בין היתר התייחסות לאמצעי הזיהוי במאגר, לגיבוי המידע, לבקרת הגישה למערכות ולעריכת ביקורות תקופתיות.
- **אבטחת מידע בניהול כח אדם.** חובה על בעל המאגר לבצע הדרכה תקופתית אחת לשנה למורשי הגישה למאגר בנוגע למסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי התקנות והחוק.
- **זיהוי ואימות.** בעת כניסה למאגר יזוהה בעל הרשאת הגישה באמצעות אמצעי פסי כדוגמת כרטיס חכם, וכן ייקבע בנוהל אופן הזיהוי, תדירות החלפת סיסמאות ואופן הטיפול בתקלות בנושא הרשאות גישה.
- **בקרה ותיעוד גישה.** יש לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על הגישה למערכות המאגר. התייעוד יישמר למשך שנתיים לפחות.
- **ביקורות תקופתיות.** לכל הפחות אחת ל-24 חודשים, יש לבצע ביקורת פנימית או חיצונית שתכלול דו"ח על התאמת אמצעי האבטחה לנוהל האבטחה והתקנות, זיהוי ליקויים והצעת תיקונים לליקויים אלו. יש לדון בדו"ח הביקורת ולבחון את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה.
- **גיבוי ושחזור.** יש לקבוע נהלי עבודה לגיבוי ושחזור נתונים.
- **אירועי אבטחה.** לפחות אחת לשנה יש לקיים דיון בנושא אירועי אבטחה ולבחון אם יש לעדכן את נוהל האבטחה.
- **הודעות על אירועי אבטחה.** יש למסור לרשם מאגרי המידע באופן מידי על אירוע אבטחה חמור, שבו נעשה שימוש בחלק מהותי ממאגר המידע בלא הרשאה או בחריגה מהרשאה או שנפגעה שלמות המידע במאגר. אירוע אופייני כזה הוא פריצה למאגר וגניבת מידע מתוכו. הרשם רשאי להורות לבעל המאגר להודיע על האירוע לכל נושאי המידע שפרטיהם כלולים במאגר. התקנות אינן קובעות סנקציות על אי-קיום ההוראה.

חובות החלות על מאגרים ברמת אבטחה גבוהה בלבד

החובות הללו מצטרפות לאלה המוטלות על בעלי כלל המאגרים המפורטים לעיל:

- **ביצוע סקר סיכונים.** בעל המאגר צריך לערוך סקר אחת לשנה וחצי לאיתור סיכוני אבטחת מידע שייערך על-ידי בעל מקצוע עם הכשרה מתאימה במטרה לזהות ולבחון ליקויים באבטחת המידע והנהלים בארגון. על בעל המאגר חלה חובה לתיקון הליקויים שיתגלו ולעדכן את הנהלים בהתאם. במסגרת ביצוע סקר הסיכונים רשאי בעל המאגר לבצע את חובת הביקורת התקופתית.
- **מבדקי חדירות.** אחת לשנה וחצי, יש לערוך מבדקי חדירות למערכות המאגר על מנת לבחון עמידות בפני סיכונים פנימיים וחיצוניים.
- **אירועי אבטחה.** יש לקיים דיון בנושא אירועי אבטחה ובחינה האם יש צורך לעדכן את נוהל האבטחה אחת לרבעון לפחות.
- **גיבוי ושחזור.** יש לשמור עותק גיבוי של הנתונים והנהלים שנועדו לצורך עמידה בתקנות.
- **הודעות על אירועי אבטחה.** חובת ההודעה מורחבת והיא חלה על אירוע שנעשה בו שימוש בחלק כלשהו (לא רק חלק מהותי) מתוך המידע שבמאגר.

חובות החלות על מאגרים המנוהלים על-ידי יחיד

מאגרים אלה זוכים להקלה ויחולו עליהם רק החובות הבאות: ניסוח מסמך הגדרות המאגר; אבטחה פיזית; נקיטת אמצעים לוודא כי גישה למידע ניתנת רק למורשי גישה ובמידה הנדרשת לביצוע תפקידם; תיעוד אירועי אבטחה המעלים חשש לפגיעה במידע או חריגה מהרשאות הגישה במערכות המידע; הגבלת התחברות של התקנים ניידים; הפרדת מערכות; אבטחת תקשורת.

התקנות החדשות מחייבות היערכות פנים-אירגונית מקיפה בתחומים כדוגמת נהלים, הדרכות, רכש והטמעת טכנולוגיה. הן מעוררות שאלות לא טריוויאליות בהקשרים כדוגמת רכישת שירותי ענן, שבהם שליטת בעל המאגר על אמצעי האבטחה היא מינימלית. אנו עומדים לרשותכם בכל שאלה בעניין.

חיים רביה, עו"ד HRavia@PearlCohen.com

שותף בכיר וראש קבוצת האינטרנט, הסייבר וזכויות היוצרים

פרל כהן צדק לצר ברץ

האמור במזכר זה אינו מתיימר למצות את כל הוראות התקנות החדשות לאבטחת מידע. מטרתו היא עדכון כללי בלבד. אין להסתמך על האמור בו כעצה משפטית.