<u>עדכון לקוחות- תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז- 2017</u>

בתקופה האחרונה אנו עדים לתופעה הולכת ומתגברת של התקפות סייבר, התקפות כופר וכו' כנגד חברות, גופים מוסדיים ואנשים פרטיים.
כיום כשהעולם נמצא בעידן בו רוב המידע אודותינו מאוחסן על גבי פלטפורמת האינטרנט ישנה חשיפה מהותית כלפי כל אחד ואחד מאתנו בהתקפות אלו.
בין אם עסקינן בפרטים אישים כמו העדפות פוליטיות, העדפות צרכניות, קורות חיים פרטי חשבון הבנק, כרטיסי אשראי ועוד ובין אם עסקינן במידע מסחרי הפגיעה יכולה להוביל לפגיעה כלכלית ו/או נפשית.
את הפגיעה הקשה שעלולה לגרום מתקפת סייבר ניתן היה לראות בברור במתקפת הסייבר הנרחבת שהתרחשה לאחרונה עת שותקו מספר בתי חולים בלונדון ונוטרלה הגישה למאגרי המידע של בית החולים בו היו מאוחסנים פרטים אודות המטופלים והטיפולים הנדרשים שהם צריכים לבצע.

מאחר וכיום כמעט כל פלטפורמה אוספת מידע אודות המשתמש בה המחוקק הבין שיש לטפל בסוגיה בוערת זו ועל כן לאחרונה אישרה ועדת חוק, חוקה ומשפט את נוסח תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**התקנות**"), כמענה לצורך הגובר ועולה להתמודד עם סוגית אבטחת המידע הנאסף על ידי גופים שונים.

התקנות קובעות לראשונה הסדר מקיף ומפורט לעניין ההגנה **הנדרשת על מאגרי מידע לרבות לעניין סדרי הניהול וכללי העבודה במאגרי מידע** ובקשר אליהם. התקנות יחולו על כל בעלי, מנהלי ומחזיקי מאגר מידע בישראל. כמו כן, התקנות יחולו גם על כל הארגונים, החברות והגופים הציבוריים אשר ברשותן מאגר מידע בישראל.

התקנות מטילות חובות מוגברות על בעל מאגרי המידע ככל שפעילות עיבוד המידע במסגרת מאגר המידע היא רחבה יותר.

הנטל המוגבר על פי התקנות יחול על גופים אשר מחזיקים בידם מאגרי מידע המכילים מידע אישי רגיש אודות נושאי המידע, מאגרי מידע המכילים מידע אודות היקף רחב של אנשים וכן חברות שמאפשרות למספר רב של אנשים גישה למאגרי המידע שלהן.

התקנות מבחינות בין מאגרי המידע ומחלקות אותם לארבע קבוצות שונות אשר נדרשות לרמת אבטחה שונה, הולכת וגוברת לפי סוג הקבוצה, וזאת בהתאם לקריטריונים שנקבעו בתקנות. חלוקת הקבוצות הינה כדלקמן:

1. מאגרי מידע המנוהלים על ידי יחיד;
2. מאגרי מידע ברמת אבטחה בסיסית;
3. מאגרי מידע ברמת אבטחה בינונית;
4. מאגרי מידע ברמת אבטחה גבוהה.

<u>להלן סקירה חלקית של עיקרי החובות תחת התקנות (כאמור לעיל חלק מן ההוראות המפורטות להלן לא יחולו על כל סוגי המאגרים):</u>

1. **<u>ניסוח מסמך הגדרות המאגר</u>**- על בעל מאגר לערוך מסמך הגדרות המפרט באופן ברור בין היתר: תיאור כללי של פעולות האיסוף והשימוש במידע, תיאור מטרות 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 בנוגע לפעולות עיבוד המידע שהוא מבצע והסיכונים העיקריים של פגיעה באבטחת המידע ואופן ההתמודדות עמם.
2. **<u>ניסוח נוהל אבטחה</u>**- על בעל מאגר לערוך מסמך נוהל אבטחה אשר יכלול בין היתר הוראות לגבי אבטחה פיזית על מאגר המידע, תיעוד אירועי אבטחה, הגבלת שימוש בהתקנים ניידים במערכות המאגר, הפרדת בין מערכות המאגר למערכות רגילות.
בנוסף, על נוהל האבטחה להכיל נוהל התמודדות עם אירוע אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע.
3. **<u>מינוי ממונה על אבטחת מידע</u>**- על פי החוק חלה חובה למנות ממונה על אבטחת מידע בגופים ציבוריים, חברות פיננסיות או בחברות המחזיקות בחמישה מאגרי מידע החייבים ברישום.

4. **<u>ניהול כוח אדם, הרשאות גישה, זיהוי ואימות</u>-** 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.
5. **<u>מיקור חוץ</u>-** עיבוד מידע בידי צד ג' מחייב בחינה מוקדמת של סיכוני אבטחת המידע בהתקשרות וקביעת הוראות חוזיות מפורשות בנושאים כדוגמת מטרות השימוש במידע, סוג העיבוד, משך ההתקשרות, אופן החזרת המידע בסיום ההתקשרות ועוד.
6. **<u>תיעוד אירועי אבטחה</u>-** בעל מאגר מידע ינהל ויתעד אירועי אבטחה המעלים חשש לפגיעה במידע או חריגה מהרשאות הגישה במערכות המידע תיעוד כניסות והיציאות ממתקני המאגר, ויתעד הכנסה והוצאה של ציוד על מנת לבצע מעקב ובקרה במקרה של כשל אבטחתי.
7. **<u>ביקורות תקופתיות</u>-** בעל מאגר מידע יבצע 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.
8. **<u>גיבוי ושחזור נתוני מאגר המידע</u>-** שמירת עותק גיבוי של הנתונים והנהלים שנועדו לצורך עמידה בתקנות.
9. **<u>חובת דיווח לרשם מאגרי המידע</u>**- יש למסור לרשם מאגרי המידע באופן מידי על אירוע אבטחה חמור שנעשה בו שימוש במידע מן המאגר בלא הרשאה או בחריגה מהרשאה.
10. **<u>התקנים ניידים</u>-** על בעל מאגר מידע לפעול להגבלת התחברות של התקנים ניידים ; הפרדת מערכות ; אבטחת תקשורת לרבות הפרדת המאגר מרשת האינטרנט הרגילה עד אשר יותקנו אמצעי הגנה מתאימים מפני חדירה למערכות המאגר ולמידע המצוי בו.

התקנות משאירות לרשם מאגרי המידע שיקול דעת בנוגע להענקת פטור למאגר מסוים מלעמוד בחובות אבטחת המידע או להחיל על מאגר מסוים חובות אבטחה כולן או חלקן לפי הנסיבות, אם לדעת רשם מאגרי המידע מתקיימים טעמים שמצדיקם זאת.
הרשם מוסמך להורות כי מי שיעמוד בהוראות המסמך המנחה בעניין אבטחת מידע או בהנחיות של רשות מוסמכת בעניים אבטחת מידע, יראו אותו כמקיים הוראות תקנות אלה, כולן או חלקן, אם הרשם השתכנע כי עמידה בהוראות אלו מבטיחה את רמת האבטחה הקבועה בתקנות לגבי אותו מאגר מידע.

התקנות עתידות להיכנס לתוקף בחלוף שנה מיום פרסומן, קרי ביום 05.05.2018, התקנות החדשות יחולו גם על מאגרים שטרם נרשמו, ובלבד שמדובר במאגרים שיש לגביהם חובת רישום. התקנות רלוונטיות לכל ארגון אשר ברשותו מאגר מידע החייב ברישום, גופים ציבוריים ופרטיים כאחד.

לפרטים נוספים, הבהרות, הרחבות וכן בכל שאלה נשמח לעמוד לרשותכם בטלפון 03-6042323 או בדוא"ל kg@kg-law.co.il.

קורן גרודברג משרד עו"ד