



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

תמצית מנהלים - איך תערכו נכון ובזמן אמת בנושא אבטחת מידע

ביום 8.5.2017 פורסמו **תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017**. מטרת התקנות הינה להגדיר בצורה מעשית מהם הצעדים שעל בעל מאגר מידע, לנקוט על מנת להגן על מידע פרטי ומניעת הפרת פרטיות של נושאי המידע. **התקנות ייכנסו לתוקף שנה מיום פרסומן**. התקנות מהוות שינוי דרמטי בגישת המחוקק למאגרי מידע ואבטחת מידע פרטי.

התקנות חלות על כל גוף המחזיק מאגר מידע. למותר לציין כי ברשות רוב חברות הסטארט-אפ או כל עסק אחר (בין אם גדול בינוני או קטן) מאגרי מידע אשר יהיו כפופים לתקנות אלו. דוגמא אחת יכולה להיות רשימת משתמשים של אפליקציה ומידע הנאסף על משתמשים אלה תוך כדי שימוש בה.

התקנות מחייבות היערכות מחדש של הארגון, לרבות קביעת נהלים, רכש והטמעת טכנולוגיות, בדיקה של שירותי ה- outsourcing, ביצוע הדרכות, ביקורות תקופתיות ועוד.

המלצתי היא להבין את התקנות לעומק, ולבחון את מערכות מאגרי המידע בארגון שלכם לאור התקנות החדשות יחד עם מומחי אבטחה ועורכי דין.

רקע:

חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**החוק**"), על תיקוניו השונים, מסדיר את נושא ההגנה על פרטיות במאגרי מידע¹. החוק קובע חובות על בעל מאגר מידע ועל מחזיק במאגר מידע, ביניהן חובות רישום מאגרי מידע מסוימים אצל רשם מאגרי המידע. מאגר מידע החייב ברישום אם הוא כולל **אחד** מאלה:

1. מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;
2. יש במאגר מידע רגיש²;
3. המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;
4. המאגר הוא של גוף ציבורי;
5. המאגר משמש לשירותי דיוור ישיר

יחד עם חובת הרישום הטיל המחוקק חובות מהותיות על בעל מאגר המידע והמחזיק בו, ביניהן איסור על שימוש במידע שלא לשם המטרה עברה נמסר המידע, חובה לאפשר לנושאי המידע זכות עיון ותיקון המידע, וכן חובות אבטחת מאגר המידע ושמירת סודיות המידע.

¹ ס' 7 לחוק קובע כי מאגר מידע הוא: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט: (1) אוסף לשימוש אישי שאינו למטרות עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף";

² מידע רגיש- נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו.



עד לאחרונה חובות אבטחת המידע לא היו ברורות ומוגדרות דיין ולשם כך, לאחר עמל של מספר שנים של משרד המשפטים, ביום 8.5.2017 פרסם המחוקק את **תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017**, (להלן: "**התקנות**"). מהלך חקיקתי זה משתלב יפה באקלים המשתנה בעולם וההבנה שיש צורך בחקיקה מוגברת להגנת הפרטיות, כדוגמת אירופה בה מתחולל כעת שינוי חקיקתי בנושא, (על כך בעדכון אחר)³. התקנות אף קובעות כי הרשם רשאי לקבוע כי מי שיעמוד בהוראות מסמך מנחה בעניין אבטחת מידע כדוגמת תקן ישראלי או בינלאומי או הנחיה ספציפית למגזר מסוים, יראו אותו כמקיים את הוראות התקנות. טרם נקבעו מסמכים או תקנים אשר יאושרו ע"י הרשם, אך צפויות לצאת הנחיות בעניין.

נציין כי לאור השינויים הצפויים, גייסה רשות המדע והטכנולוגיה במשרד המשפטים (רמו"ט) גיוסים רבים, וקיבלה תקציבים נוספים, לרבות לאכיפה.

בתקנות יש ניסיון להבחין בין סוגים שונים של מאגרי מידע ובעלי מאגרי מידע ולהטיל אחריות וחובות פרופורציונליים לגודל ואופי המאגר.

סוגי מאגרי המידע ורמת אבטחת המידע הנדרשת מכל סוג:

1. **מאגר המנוהל בידי יחיד:**
הוא מאגר מידע המנוהל בידי יחיד או תאגיד בבעלות יחיד, ואשר רק היחיד ולכל היותר עוד שני בעלי הרשאה נוספים רשאים לעשות בו שימוש, ולמעט מאגר מידע שמטרתו העיקרית הוא איסוף מידע לצורך מסירתו לאחר (לדוג' דיור ישר), מאגר מידע שיש בו מידע על מעל 10,000 איש או מאגר מידע שבעל מאגר המידע כפוף בשלו לחובת סודיות מקצועית.
2. **מאגרי מידע שחלה עליהם חובת אבטחה הבסיסית:**
מאגרי מידע שאינם נכללים באף אחת מהקבוצות האחרות.
3. **מאגרי מידע שחלה עליהם רמת אבטחה בינונית:**
מאגר מידע שמספר בעלי ההרשאה אליו עולה על עשרה והוא אחד מאלה:
 - מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר, לרבות דיור ישר;
 - מאגר מידע שבעליו הוא גוף ציבורי;
 - מאגר מידע הכולל מידע שהוא אחד מאלה: צנעת חייו האישיים של אדם, מידע רפואי, מידע על מצב נפשי, מידע גנטי, דעות פוליטיות אמונות דתיות, עברו הפלילי של אדם, נתוני תקשורת⁴, מידע ביומטרי, מידע על נכסיו של אדם או הרגלי הצריכה שלו. במקרים מסוימים מחריג החוק מהצורך ברמת אבטחה מוגברת מאגרי מידע שהיו נכללים ברשימה זו ובלבד שנושאי המידע הם מועסקים ו/או ספקים ומאגר המידע נועד רק לצורך ניהול העסק.
4. **מאגרי מידע שחלה עליהם חובת אבטחה מוגברת-** מאגר מידע שהיתה חלה עליו חובת אבטחה בסיסית או בינונית ובלבד שיש בו מידע על אודות מעל 100,000 אנשים או שבמספר עלי ההרשאה לגישה אליו עולה על 100.

³הכוונה ל EU General Data Protection Regulation (GDPR) – אשר ייכנס לתוקף במאי 2018.

⁴ נתוני תקשורת מוגדרים ב חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח- 2007 והם כוללים בין היתר, נתוני תעבורה, מיקום, נתוני תעבורה, אמצעי תשלום וכד'.



עיקרי חובות האבטחה במאגרי מידע שחלה עליהם חובת אבטחה בסיסית או בינונית⁵:

- **ניסוח מסמך הגדרות המאגר**- הכולל לכל הפחות תיאור כללי של פעולות האיסוף, תיאור מטרות השימוש במידע, סוגי המידע הכלולים במאגר, פרטים בנוגע להעברה ושימוש מאגר המידע לחול, פעולות עיבוד בידי מחזיק המאגר, שמו של מנהל המאגר, המחזיק, ממונה על אבטחה ככל שיש והסיכונים העיקריים של פגיעה באבטחת המידע.
- **מינוי ממונה על אבטחת מידע**- במקרים מסוימים, כגון בחברות המחזיקות בחמישה מאגרי מידע החייבים ברישום, יש למנות ממונה על אבטחת מידע אשר יהיה אחראי לבקרה שוטפת לעמידה בתקנות. הממונה יהיה כפוף ישירות למנהל או בעלי המאגר ואסור לו להיות בניגוד עניינים.
- **קביעת נוהל אבטחת מאגר המידע**- אשר יכלול הוראות לעניין האבטחה הפיזית של המאגר, הרשאות הגישה למאגר, תיאור אמצעי ההגנה על המאגר, הוראות למורשי הגישה למאגר, סיכונים שחשוף להם המאגר ואופן הטיפול בהם, אופן התמודדות עם ארועי אבטחה לפי חומרת העניין, והוראות לעניין טיפול בהתקנים ניידים. לגבי מאגר מידע ברמת אבטחה בינונית או גבוהה, בנוסף לאמור לעיל, יכלול הנוהל גם פרטים לעניין אמצעי הזיהוי והאימות לגישה למאגר, אופן בקרה על השימוש במאגר, הוראות לעניין עריכת ביקורות תקופתיות, גיבוי נתונים, פעולות פיתוח במאגר. נוהל אבטחת המידע ייבדק אחת לשנה לפחות ע"י בעל מאגר המידע.
- **מיפוי מערכות וביצוע סקר סיכונים**- יש להחזיק מסמך מעודכן של מבנה מאגר המידע, לרבות תשתיות ומערכות חומרה, רכיבי תקשורת, אבטחת מידע, תוכנות וממשקים המשמשים לתקשורת עם מאגר המידע, תרשים רשת ותאריך עדכון המסמך.
- **אבטחה פיזית וסביבתית**- מערכות מאגר המידע יישמרו במקום מוגן, המונע חדירה או כניסה ללא הרשאה והתואם את אופי המאגר והמידע הכלול בו. במאגר מידע בעל רמת אבטחה בינונית או גבוהה, ינקטו אמצעים לבקרה ותיעוד של הכניסה והיציאה מהאתר בו שמור המאגר.
- **ניהול כח אדם**- בעל מאגר מידע לא יתן גישה או הרשאה לאחר אלא נקיטת אמצעים המקובלים בהליכי מיון כח אדם, בשים לב לסוג המידע ורגישותו. יש לקיים הדרכות לעובדים טרם מתן גישה למאגר המידע. במאגרי מידע בעלי רמת אבטחה בינונית וגבוהה, יתקיימו אף הדרכות תקופתיות.
- **ניהול הרשאות גישה**- בעל מאגר המידע יקבע הרשאות גישה בהתאם לכל תפקיד ובמידה הנדרשת לביצוע התפקיד, וכן ינהל רישום מדויק של בעלי ההרשאות.
- **זיהוי ואימות**- יש לנקוט באמצעים מקובלים בנסיבות העניין כדי לוודא שהגישה למאגר המידע נעשית בידי מורשים לכך בלבד. במאגרי מידע בעלי רמת אבטחה בינונית או גבוהה, אופן הזיהוי יעשה ככל הניתן ע"י זיהוי פיזי הנתון לשליטתו הבלעדית של בעל מאגר המידע. כמו כן ייקבעו אופן הזיהוי, טיפול תקלות, ניתוק עקב אי שימוש בנוהל האבטחה של המאגר. בנוסף, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות מאגר המידע.
- **תיעוד ודיווח של אירועי אבטחה**- על בעל מאגר מידע לנהל תיעוד של אירועי אבטחה המעלים חשש לפגיעה בשלמות המידע. ככל הניתן יש להתבסס על רישום אוטומטי. יש לקבוע נהלים

⁵ חובות האבטחה של מאגר מידע המנוהל בידי יחיד הן בסיסיות ביותר ולא נתמקד בהם כאן. מאגרי מידע שחלה עליהם רמת אבטחה מוגברת יהיו ככלל שייכים לארגונים גדולים במיוחד, ולכן לא אדון בהם כאן. בכל אחד ממקרים אלה אפשר לפנות אלי ליעוץ להמשך בירור.



להתמודדות עם אירועי אבטחה. במאגר מידע בעל רמת אבטחה בינונית על בעל המאגר לנהל דיון לפחות פעם בשנה באירועי האבטחה ובצורך לריענון הנוהל. במקרה של אירוע אבטחה חמור⁶ חלה חובה לדווח לרשם, והרשם אף רשאי, בתנאים מסוימים, להורות להודיע על אירוע האבטחה לנושאי המידע שעלולים להיפגע. יש כאן חידוש מהותי בדרך הטיפול באירועי אבטחה ועולים ממנה שני חששות: יתר דווח לרשויות, מה שישפיע על אפקטיביות הטיפול, וכן סכנה לתביעות ייצוגיות של נושאי המידע.

- **התקנים ניידים** - יש להגביל את ההתחברות למאגר המידע דרך התקנים ניידים (laptops, smartphones, removable hardware), במתכונת ההולמת את המאגר.
- **ניהול מאובטח ומעודכן של המערכות** - יש להקפיד על ניהול ותפעול תקין של המערכות כמקובל בהפעלת מערכות אלה, יש להפריד ככל הניתן בין המערכות, יש להקפיד על גרסאות מעודכנות ועל מענה אבטחה מתאים.
- **אבטחת תקשורת** - אין לחבר את המאגר לרשת האינטרנט ללא התקנת אמצעי הגנה מתאימים, העברת מידע תעשה תוך שימוש בהצפנה. ככל שיש גישה למאגר מרחוק באמצעות הרשת יש לזהות את המתקשר ולאמת את הרשאותו.
- **מיקור חוץ** - התקנות קובעות רשימה של סעיפים שיש לכלול בכל הסכם מיקור חוץ (outsourcing) לצורך קבלת שירותים הכרוכים במתן גישה למידע. התקנה לא חלה על התקשרות של בעל מאגר מידע עם יחיד (freelancer).
- **ביקורת תקופתיות** - בעל מידע שחלה עליו רמת אבטחה בינונית יערוך אחת ל-24 חודשים לפחות ביקורת פנימית או חיצונית, ע"י גורם שהוא אינו מנהל מאגר המידע, כדי לוודא עמידה בהוראות התקנות.
- **שמירת מידע וגיבוי** - יש לשמור את הנתונים הנצברים במאגר באופן מאובטח למשך 24 חודשים. בעל מאגר מידע שחלה עליו רמת אבטחה בינונית גם צריך לדאוג לכך שאפשר יהיה לשחזר את הנתונים למצב המקורי, ולשם כך יקבעו נהלים מתאימים.

אשמח לעמוד לרשותכם בכל שאלה או המשך בירור

אשרת סיתי פרידמן, עו"ד.

מטרת עדכון לקוחות זה הוא סקירה כללית של מצב הדין בישראל לאור השינוי החקיקתי. הוא אינו מהווה ייעוץ משפטי ספציפי או חוות דעת משפטית, אלא הבאת הדגשים חלקיים בלבד.

⁶ ס'1 לתקנות קובע: אירוע אבטחה חמור במאגר מידע שחלה עליו רמת אבטחה בינונית- אירוע שנעשה בו שימוש בחלק מהותי מן המאגר, בלא הרשאה או בחריגה מההרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר.