

תקנות הגנת הפרטיות (אבטחת מידע) – 2017

במרץ 2017 נתקבלו בוועדת חוקה חוק ומשפט של הכנסת תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("התקנות"), שייכנסו לתוקף מחייב ב-8 לחודש מאי 2018 (כמעט במקביל לתחולת הוראות ה-GDPR¹). התקנות קובעות הסדר מקיף שיחול על כל גוף בישראל המחזיק, מנהל או שבבעלותו "מאגר מידע", והמכיל סוגי "מידע" – כהגדרתם בחוק הגנת הפרטיות, תשמ"א-1981 ("החוק").

לתקנות עשויות להיות **תחולה משמעותית על כל מי שמחזיק, מנהל או נותן גישה למאגר מידע** ולפיכך חשוב להכיר, להכיר את החובות העשויות לחול בקשר עימן **וליישמן כנדרש לא יאוחר מיום 8 למאי 2018**.

מאגר מידע מהווה כל אוסף נתוני מידע שמיועד לעיבוד ממוחשב (למעט אוסף לשימוש אישי או כזה הכולל רק שם, מען ודרך התקשרות) ואילו מידע ייחשב כמידע אישי על אדם, מעמדו האישי, הכשרתו המקצועית, בריאותו ומצבו הכלכלי, דעותיו ועוד, כפי שמוגדר בסעיף 7 לחוק. נדגיש, כי אמנם התקנות מכוונות לבעל מאגר המידע אך הן למעשה מחילות את כל ההוראות והחובות שבהן גם כלפי מנהל מאגר מידע (המנהל הפעיל של גוף שבבעלותו או בחזקתו מאגר מידע או מי שהוסמך כאמור) ואת מרביתן אף על המחזיק במאגר מידע (מי שרשאי לעשות במאגר המצוי ברשותו שימוש בדרך קבע, לרבות מעבד מידע מטעם בעל מאגר).

בחינת סוג המאגר

על מנת לבחון את תחולת התקנות לגביו, על בעל מאגר לבדוק **איזה סוג מאגר נמצא ברשותו**, מבין ארבעת הסוגים המנויים בתקנות. היקף החבות ותחולת התקנות ייגזר מסוג המאגר הרלוונטי²:

- **מאגר מידע שמנהל יחיד** (או תאגיד בבעלות יחיד): מאגר שרק היחיד עצמו ולכל היותר שני בעלי גישה נוספים עושים בו שימוש, למעט מאגרים שאינם: (א) למטרת איסוף מידע לצורך מכירתו לאחר; אן (ב) מכילים מידע על פחות מ-10,000 אנשים אן (ג) כוללים מידע שעשוי לחול עליו חובת סודיות מקצועית לפי דין או אתיקה.
- **מאגר שחלה עליו רמת אבטחה בסיסית**: מאגר הכולל מידע על צנעת חייו האישיים של אדם, מידע רפואי או נפשי, מידע גנטי, דעות פוליטיות או אמונות, רישום פלילי של אדם, נתוני מיקום, מידע ביומטרי, מידע על נכסיו של אדם ומידע באשר להרגלי צריכה של אדם שיש בהם ללמוד מידע שכזה ("מידע רגיש") שמספר בעלי ההרשאה בו אינו עולה על 10 אן כשהמידע שמכיל הוא מידע רפואי או נפשי, עבר פלילי, נתוני תקשורת מידע ביומטרי מסוג תמונת פנים או מידע פיננסי ביחס לספקים או מועסקים של בעל מאגר וכן משמש למטרות ניהול העסק.
- **מאגר שחלה עליו רמת אבטחה בינונית**: מאגר שמטרתו העיקרית הינה לאסוף מידע לצורך מסירתו לאחר (כעסק ולרבות שירותי דיור ישיר); אן כל מאגר שמוחזק ע"י רשות ציבורית; אן מאגר הכולל סוגים מסוימים של מידע רגיש, כגון מידע ביומטרי, רפואי, גנטי, מידע על דעות פוליטיות ואמונות, מידע כלכלי, מידע על צנעת חייו של אדם ועוד.
- **מאגר שחלה עליו רמת אבטחה גבוהה**: מאגר שמטרתו העיקרית הינה לאסוף מידע לצורך מסירתו לאחר, או מאגר שמכיל מידע רגיש ושמטקיים לגביו אחד מאלו: מכיל מידע אודות 100,000 אנשים ומעלה אן מספר

¹ למזכר שלנו בעניין Regulation (EU) 2016/679 – General Data Protection Regulation – לחצו כאן.

² עם זאת יצוין כי לעיתים התקנות אינן מבהירות באופן חד משמעי את מכלול ההבדלים בין סוגי המאגרים המוזכרים בהן.

בעלי ההרשאה בו עולה על 100.

להלן עיקרי החובות שיחולו על כל מאגר מידע (מלבד מאגר המנוהל ע"י יחיד) בהתאם לתקנות :

- **הטמעת הוראות ונהלים בארגון וחובת תיעוד**, שיכללו את ביצוע הפעולות כדלקמן :
 - **מינוי ממונה אבטחת המידע**, אשר יהיה אמון, בין היתר על הכנת המסמכים המפורטים להלן.
 - **הכנת מסמך הגדרות מאגר** : תיאור פעולות האיסוף והשימוש במידע, מטרות השימוש, סוגי המידע, פרטים על העברות המידע, פעולות עיבוד המידע, הסיכונים ודרכי ההתמודדות עם פגיעות באבטחת המידע וכו'.
 - **נחיצות שמירת המידע והיקפו** ייבחנו מדי שנה ובעת שינויים מהותיים.
 - **הכנת מסמך נוהל אבטחת מידע** : הוראות לגבי האבטחה הפיזית של המאגר, הרשאות הגישה והוראות למורשים, אמצעי ההגנה על המאגר, הוראות לעניין התקנים ניידים ועוד.
 - **הכנת מסמך מבנה המאגר ורשימת מצאי של מערכות המאגר** : מיפוי התשתיות ומערכות החומרה, פירוט סוגי רכיבי התקשורת, מערכות התוכנה בהן משתמשים להפעלת מאגר המידע, לרבות ממשקים המשמשים לתקשורת עם מערכות המאגר ומהן או לניהולו, לתחזוקתו וניטורו.
 - **חובת תיעוד** : תיעוד של כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו ללא הרשאה או לחריגה מהרשאה. תיעוד כאמור עדיף שיבוסס על רישום אוטומטי.
- **שמירה על המידע** : תתבצע, בין היתר, באמצעות קביעת הרשאות גישה של בעל תפקיד למידע, בהתאם להגדרות התפקיד הרלוונטי, כך שהעובד ייחשף למידע הדרוש לביצוע תפקידו בלבד. בנוסף, תנוסח רשימת הרשאות תקפה שתכלול רישום מעודכן של תפקידים בחברה, הרשאות הגישה הצמודות להם וזהות בעלי התפקיד הרלוונטיים. בעל המאגר ינקוט באמצעים מקובלים לזיהוי ואימות כדי לוודא שהגישה למאגר תעשה רק בידי בעלי ההרשאה המורשים לכך מתוך רשימת ההרשאות התקפה. כמו כן קיימת דרישה לקיום אבטחה פיזית וסביבתית למניעת חדירה ללא הרשאה למתקני התשתית ומערכות החומרה, רכיבי התקשורת ואבטחת המידע. התקנות מחילות גם את החובות לנהל ולתפעל בצורה תקינה את מערכות המאגר (למשל בעדכונים שוטפים) ואת האיסור להשתמש במערכות שהיצרן לא תומך בהיבטי אבטחה בהן (אלא אם סופקה אבטחה מתאימה אחרת). בנוסף, מוטלות חובות משלימות : (א) החובה להפריד (בהיקף ובמידה אפשריים וסבירים) בין מערכות המאגר לבין מערכות מחשוב אחרות המשמשות את בעל המאגר ; (ב) הגבלה על חיבור התקנים ניידים למערכות מאגר המידע. במקרה של שימוש בהתקנים ניידים כחלק משגרת העבודה, ינקטו אמצעי הגנה תוך התייחסות לסיכונים אלו ; (ג) איסור על חיבור המערכת לרשת האינטרנט (או רשת ציבורית כלשהי) ללא התקנת אמצעי הגנה מתאימים ותוך שימוש בהצפנה (בחיבור מרחוק – יש להשתמש באמצעים בטיחותיים נוספים שמטרתם לזהות ולאמת את המתקשר והרשאתו).
- **שמירת נתונים, גיבוי ושחזור** של הנתונים שמופקים כחלק מיישום התקנות למשך 24 חודשים.
- **חובות משלימות** : בעת הליכי מיון ושיבוץ עובדים, בעל מאגר (כמעסיק) לא ייתן לעובד גישה למידע בטרם נקט באמצעים סבירים כדי לוודא שאין חשש שהעובד אינו מתאים לקבל גישה כזו (ויקיים הדרכות בנושא התקנות, החובות ונהלי האבטחה במקום העבודה). בעת קבלת שירותים מנותן שירות חיצוני במיקור חוץ, הכרוך בקבלת גישה למאגר (כגון לצורך עיבוד המידע במאגר וכו'), בעל המאגר יבחן בטרם ההתקשרות את סיכוני אבטחת המידע הכרוכים בהתקשרות ויקבע, בין היתר : את סוג המידע שאותו גורם חיצוני רשאי לגשת אליו ומטרות השימוש בו ; מערכות המאגר הרלוונטיות ; סוג השימוש באותו מידע ; ויפקח ויבקר את

קיום הוראות אלו ע"י אותו נותן שירות.

החובות שיחולו ביחס למאגרים ברמת האבטחה הבינונית או הגבוהה, בנוסף להוראות שפורטו עד כה, הינן:

- נוהל אבטחת המידע יכלול גם התייחסות לאמצעי הזיהוי והאימות בעת גישה למאגר; אופן הבקרה על השימוש במידע שבמאגר; נהלים לעניין ביקורות תקופתיות וגיבוי נתונים; והוראות לעניין פעולות פיתוח במאגר.
- אופן הזיהוי והאימות בעת כניסה של מורשה למאגר מידע יבוצע על ידי אמצעי פיזי שיהיה בשליטה בלעדית של אותו מורשה (כגון כרטיס חכם) וכן ייקבעו בנוהל אבטחה הוראות לעניין אופן זיהוי, חוזק הסיסמאות, מספר הניסיונות השגויים, תדירות החלפת הסיסמאות וניתוק אוטומטי של המערכת. בנוסף, יופעל במנגנון תיעוד אוטומטי שיבקר את הגישה למערכות המידע ויתעד, בין השאר, את זהות המשתמש, התאריך והשעה של הגישה, לאיזה חלק מהמערכת בוצע ניסיון גישה, סוג הגישה, היקפה ונתונים נוספים.
- דרישת האבטחה הפיזית והסביבתית של מערכות מאגר המידע תכלול גם נקיטת אמצעים לתיעוד של כניסה ויציאה מאותם אתרים בהם מצויות המערכות.
- קיום פעולות הדרכה (אחת לשנתיים לפחות) לבעלי הרשאה בדבר מסמך הגדרות המאגר, נוהל האבטחה ובהוראות לאבטחת המידע שבתקנות ובחוק, וכן בסמוך לתחילת עבודה של כל מורשה גישה חדש.
- קיום דיון שנתי באירועי האבטחה ובחינת עדכונם של נוהל האבטחה.
- ביקורת (פנימית או חיצונית) תקופתית כל 24 חודשים כדי לבדוק את עמידתו של המאגר בהוראות התקנות.
- דיווח על אירועי אבטחה חמורים לרשם מאגרי המידע ("**הרשם**") והרשם מצדו עשוי להורות על מסירת הודעה לנושא מידע שעשוי להיפגע מן האירוע.
- החובה בגיבוי ויכולת שחזור הנתונים המופקים כולל את החובה לשמירתם שבאופן שיבטיח את שחזורם למצב המקורי בכל עת. לעניין זה קמה גם החובה להחזיק במסמך נהלים והוראות לעניין הבטחת השחזור.

החובות הבאות יחולו ביחס למאגר ברמת האבטחה הגבוהה, בנוסף להוראות שפורטו עד כה:

- ביצוע סקר לאיתור סיכונים אבטחת מידע ומבדקי חדירות למאגר לשם בחינת עמידות האבטחה וזאת אחת ל-18 חודשים לפחות.
- גיבוי ויכולת שחזור של נתונים המופקים במסגרת התקנות גם במקרה של אבדן או הרס (למשל על-ידי עותק פיזי או עותק בענן).
- **כאשר מדובר סוג במאגר המנוהל על ידי יחיד, מחייבות התקנות הבאות בלבד:**
- ניסוח והחזקה של מסמך הגדרות מאגר.
- אבטחה פיזית וסביבתית למניעת חדירה ללא הרשאה למתקני התשתית ומערכות החומרה, רכיבי התקשורת ואבטחת המידע.
- נקיטת אמצעים מקובלים לזיהוי ואימות כדי לוודא שהגישה למאגר תעשה רק בידי בעל הרשאה.
- תיעוד של כל מקרה המעלה חשש לפגיעה בשלמות המידע, או שימוש בו תוך חריגה מהרשאה.
- החובה לנהל ולתפעל בצורה תקינה את מערכות המאגר, בין היתר באמצעות עדכונים שוטפים, הפרדה (ככל שניתן) בין מערכות המאגר לבין מערכות מחשוב אחרות והגבלה על חיבור התקנים ניידים וחיבור המערכת

לרשת ציבורית (לרבות האינטרנט).

רשם מאגרי המידע

התקנות מסמיכות את הרשם להעניק פטור למאגר מחובות אבטחת מידע מטעמים שיצדיקו מתן פטור כאמור או דווקא להחיל חובות אבטחה מסוימות על מאגר מידע לפי נסיבות העניין. בנוסף, הוסמך הרשם להורות כי מי שיעמוד בהוראות "מסמך מנחה" בעניין אבטחת מידע (למשל תקן רשמי, תקן ישראלי או בין-לאומי, או כל מסמך שהרשם יאשר לצורך עניין זה) או בהוראות רשות מוסמכת, ייראו אותו כמקיים את הוראות התקנות, או חלקן.

לסיכום

החל מכניסתן לתוקף, יישנו התקנות החדשות את הדרך שבה מחויבים גופים שונים המחזקים במידע להגן על פרטיותו של אדם וזאת באמצעות החלת חובות רחבות היקף על בעל מאגר מידע. כצעד ראשון, יש להבין האם מאגר המידע, המידע כשלעצמו וכן המחזיק בו, עונים על ההגדרות שבדין והתקנות רלוונטיות בעניינם. לאחר זיהוי סוג המאגר ניתן יהיה לגזור את היקף החבות בתקנות החדשות וקיומם של פטורים רלוונטיים.

בכל מידע נוסף ניתן לפנות לצוות הרלוונטי במחלקת ההי-טק במשרדנו:

עו"ד יריב קסנר yariv@novlaw.com

עו"ד הילה יצחקי hilaizhaki@novlaw.com

עו"ד אורן אברהם oren@novlaw.com

טלפון - 03-5441411

מזכר זה הוכן לצרכים אינפורמטיביים כלליים ואין בו משום ייעוץ משפטי או תחליף לייעוץ משפטי קונקרטי. על הקורא לפנות ולהתייעץ עם עו"ד בטרם נקיטת כל פעולה משפטית או הימנעות מפעולה הקשורה לאמור במזכר זה.