לקוחות וחברים יקרים,

בתקופה האחרונה פרסמה הרשות להגנת הפרטיות (להלן: "**הרשות**"), מספר מסמכים ובהם גילוי דעת בנושא פרשנות תקנה 3 לתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001 (להלן: "**תקנות העברת מידע**") ומסמכים בעלי אופי טכנולוגי, שיש בהם כדי ללמד על עמדתה ביחס לאופן בו יש לבצע פעולות שונות הנדרשות בדין. מצאנו לנכון לרכז מסמכים אלה עבורכם במזכר זה.

נשמח לסייע לכם לבחון את עמידת ארגונכם בהוראות דיני הגנת הפרטיות בכלל, והוראות המסמכים השונים בפרט. לצורך כך אתם מוזמנים ליצור איתנו קשר, על מנת לתאם שיחת ייעוץ אישית, במסגרתה נוכל גם לסקור את הוראות המסמכים ביתר פירוט.

<u>גילוי דעת בנושא פרשנות תקנה 3 תקנות העברת מידע</u>[1]

1. תקנות העברת מידע קובעות איסור העברת מידע ממאגר מידע בישראל אל מחוץ לגבולותיה, אלא אם כן (1) דין המדינה שאליה מועבר המידע, מבטיח רמת הגנה על מידע שאינה פחותה, בשינויים המחויבים, מרמת ההגנה על מידע הקבועה בדין הישראלי, כמפורט בתקנה 1 לתקנות העברת מידע; או (2) מתקיימות נסיבות אחרות המנויות בתקנה 2 לתקנות העברת מידע.

2. בנוסף, תקנה 3 לתקנות העברת מידע קובעת כי בהעברת מידע לפי תקנה 1 או 2 יבטיח בעל מאגר המידע, **בהתחייבות בכתב של מקבל המידע**, כי מקבל המידע **נוקט אמצעים מספיקים להבטחת**

[1] תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

www.agmon-law.co.il | אגמון עם טולצ'ינסקי, משרד עורכי דין

פרטיותם של מי שהמידע עליהם, וכי הוא מבטיח שהמידע לא יועבר לכל אדם זולתו, בין באותה מדינה ובין במדינה אחרת.

3. לפי גילוי הדעת שפרסמה הרשות ביום 13.10.2024 (להלן: "**גילוי הדעת**") (א) התקנות מטילות איסור גורף על גורם במדינה זרה שקיבל מידע מישראל, להעביר את המידע (transfer) או לגלות אותו (disclose) לכל אדם זולתו; (ב) איסור גורף זה הוא בבחינת גזירה שהציבור אינו יכול לעמוד בה.

4. הרשות מבהירה לפיכך בגילוי הדעת כי –

א. מקבל המידע במדינה הזרה יהיה רשאי להעביר את המידע לצד שלישי בהתקיים התנאים הבאים: (1) ניתנה לו הסכמה לכך בכתב מאת בעל המאגר (שממנו הועבר המידע מישראל); (2) בכפוף לכך שעצם העברת המידע לצד שלישי הייתה עומדת בדרישות הדין גם אילו הייתה זו העברה המתבצעת בתחומי ישראל; ו-(3) אילו היה המידע מועבר ישירות מישראל לצד השלישי, היו מתקיימים בהעברה זו תנאי תקנה 1 או תקנה 2 לתקנות העברת מידע.

ב. תקנה 3 לתקנות העברת מידע קובעת כי "בהעברת מידע לפי תקנה 1 או 2 **יבטיח בעל מאגר המידע, בהתחייבות בכתב של מקבל המידע**, כי מקבל המידע נוקט אמצעים מספיקים להבטחת פרטיותם של מי שהמידע עליהם, **וכי הוא מבטיח שהמידע לא יועבר לכל אדם זולתו, בין באותה מדינה ובין במדינה אחרת**.

ג. לפי גילוי הדעת, היקף ותוכן ההתחייבות הנזכרת בתקנה 3 לתקנות העברת מידע, אינם חייבים להגיע כדי הסכם "לקיים את התנאים לאחזקת מידע ולשימוש בו החלים על מאגר מידע בישראל", כאמור בתקנה 2(4) לתקנות העברת מידע. ההתחייבות אליה מתייחסת תקנה 3 יכולה לכלול ערובות מקובלות אחרות להבטחת פרטיותם של נושאי המידע, בשים לב להיקף המידע, רגישותו ושאר הנסיבות הצריכות לעניין, גם אם אינן זהות במדויק לדיני הגנת הפרטיות בישראל.[2]

ד. יובהר כי ההתחייבות האמורה חייבת לעמוד ביתר הוראות הדין לגבי מיקור חוץ או במתן גישה לגורם חיצוני אל מאגר המידע המצוי בישראל (במיוחד בקשר לתקנה 15 לתקנות אבטחת מידע).[3]

גילוי הדעת המלא זמין כאן

[2] למשל, עמידה ברגולציית הגנת המידע של האיחוד האירופי(GDPR) או בחקיקה של מדינות אשר הוכרו על ידי האיחוד האירופי כבעלות מעמד תאימות (Adequacy) בתחום הגנת המידע.

[3] לתקנות הפרטיות אבטחת מידע ה'תשע"ז-2017 (להלן: "**תקנות אבטחת מידע**").

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

אגמון עם טולצ'ינסקי, משרד עורכי דין | www.agmon-law.co.il

<u>האתגרים במעבר של מאגרי מידע ומערכות המאגר לענן</u>

1. במסמך שפרסמה הרשות מיום 5.9.2024 ("**מסמך אתגרי המעבר לענן**"), הרשות מצביעה על התקדמות בטכנולוגיות להעברת מידע בצורה מהירה, המאפשרת קישוריות גבוהה בין רכיבים (לרבות רכיבי אחסון) באמצעות רשתות האינטרנט והסלולר. כן היא מצביעה על התקדמות בטכנולוגיות הדורשות משאבי מחשב מרובים, כגון טכנולוגיות המאפשרות עיבוד בסיסי נתוני עתק (Data Big) וקבלת החלטות לפיהם, דוגמת טכנולוגיות בינה מלאכותית (AI). התקדמות של טכנולוגיות אלה, לצד התקדמות בטכנולוגיות מחשוב ענן (Cloud Computing) המאפשרות שימוש קל ונוח במשאבי אחסון ועיבוד מידע בהיקף כמעט בלתי מוגבל, הביאו לפי הרשות לעלייה משמעותית במספר מאגרי המידע המועברים לאחסון ענן.

2. לפי הרשות הליך העברת תשתיות ויישומים שונים לשרותי ענן (מיגרציה), הינו הליך מורכב בו מעורבות רוב המחלקות בארגון. לפי הרשות נדרשים ארגונים לתעד את השלבים השונים של המיגרציה וההחלטות הנלוות אליה ובתוך כך להתייחס לאתגרים שונים שפורטו במסמך אתגרי המעבר לענן. בחינת אתגרים אלה אינה גורעת מהחובה כללית הקיימת לפי תקנה 15(א)(1) לתקנות אבטחת מידע, ביחס לבחינת הסיכונים הכרוכים בהתקשרות עם כל ספק המקבל גישה למידע אישי של הארגון.

3. **אתגרים לפי מסמך אתגרי ענן**

א. <u>חוסר ההתאמה של הארכיטקטורה הנוכחית</u> - לפי הרשות אחד האתגרים הראשונים הוא התאמת הארכיטקטורה בסביבה החדשה שאליה מועבר המידע. חוסר תאימות עלול להביא להעברה איטית של נתונים או אף לשגיאה בהעברת הנתונים. לדעת גורמים מסוימים עמם אנו עובדים, ארכיטקטורה שגויה עלול לגרום גם לאחסון נתונים באופן החשוף לגישה מרשת ציבורית (האינטרנט). הרשות ממליצה לבצע סקר מקדים של הארכיטקטורה המקומית ולייצר תיעוד מקיף שלה. כך, במיוחד כאשר יהיה צורך לשלב נכסים מקומיים בסביבת ענן (או להעביר את קצתם לענן פרטים וקצתם לענן ציבורי), יהיה אפשר לבחון את הארכיטקטורה אל מול הסביבות החדשות, ולבצע את השינויים הנדרשים לשם הפחתת סיכונים וחשיפת נתונים מהסביבה המקומית.

ב. <u>הגדרות שגויות</u> - יצירת הגדרות שגויות עלולות להוביל לחשיפת מידע ארגונים בידי גורמים שאינם מורשים להיחשף למידע זה. לרוב לצוותי המחשוב (IT) בארגונים ניסיון רב בתחזוקת מערכות

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

אגמון עם טולצ'ינסקי, משרד עורכי דין | www.agmon-law.co.il

פנימיות של הארגונים ובהגדרות השונות שלהן, אך השוני בין מערכות אלו למערכות בענן או בסביבה העננית משמעותי ולכן הידע של צוותים אלו לעיתים לא רלוונטי. הרשות מציעה לוודא כי קיים כוח אדם מיומן, בהיקף הנדרש, שיהיה אחראי על המעבר לענן וביצוע הגדרות המערכות במסגרתו.

ג. ממשקי AP שאינם מאובטחים כראוי - Application Programming Interface המקשרים בין רכיבים שונים בשירותי הענן השונים, בין שירותי הענן לאחסון מקומי, או בין שרתי האחסון לבין שרתים החשופים לרשת ציבורית (אינטרנט), קיימים כמעט בכל שירות ענן. כשל בהגנה על ממשקים אלו עלול לאפשר שליפת נתונים ומידע על ידי גורמים שאינם מורשים לכך. לכן הרשות ממליצה להקפיד לשלב מנגנוני אבטחה על ממשקי המערכות, ומגנוני בקרה ותיעוד שישמשו את הליך המיגרציה, העבודה והתחזוקה של תשתית הענן / שירות הענן. המלצה נוספת היא הצפנת המידע במנוחה ובתנועה, תוך הקפדה שעל שמירת מפתחות ההצפנה בסביבה מוגנת, שאיננה הסביבה שבה מאוחסן המידע.

ד. אובדן נתונים (Data Loss) - הרשות ממליצה לגבות את כל הנתונים השמורים במערכת הארגון לפני ביצוע מיגרציה, כדי לצמצם את החשיפות השונות הקשורות לאובדן נתונים במהלך המיגרציה.

ה. סיכוני אבטחה – מעבר לענן מקים סיכונים חדשים הנוגעים לאבטחת מידע הארגון וכן דורש חלוקה חדשה של הגורמים האחראים לנקיטת אמצעים שונים כנגד סיכונים שקודם למיגרציה היו בשליטתו הבלעדית של הארגון. חשוב לציין כי חובות אבטחת המידע הקבועות בתקנות אבטחת מידע חלות על ארגון בהתאם לרמת האבטחה החלה על מאגרי המידע שלו, גם בעת המעבר לענן (לרבות החובה לקבוע מנגנוני אימות, הגבלת הרשאות, שימוש במנגנוני הצפנה, הדרכות עובדים, תיעוד ובקרה ועוד). כפועל יוצא הרשות מחדדת את החשיבות להביא לביטוי מול ספק שירותי הענן מודל חלוקת אחריות מתאים.[4] הרשות רואה לנכון לציין כי חובת ארגונים לבחון אחת לשנה אם המידע שהם שומרים במאגר מידע רב מן הנדרש (תקנה 2(ג) לתקנות אבטחת מידע) מקבלת משנה תוקף בעת המעבר לענן (שעה שהארגון מוציא מחזקתו את המידע האמור).

[4] לפי הרשות לצורך ניהול סיכוני האבטחה והתמודדות עימם, יש לפעול במסגרת מודל חלוקת האחריות להגנה על המידע העסקי לפיו "ההגנה על המידע בתוך הענן חלה על הלקוח", אשר משמעותו היא שהאחריות להגנת המידע המצוי במערכות הארגון, חלה על הארגון עצמו, ולא על ספק הענן.

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

אגמון עם טולצ'ינסקי, משרד עורכי דין | www.agmon-law.co.il

ו. <u>היעדר אסטרטגית במעבר לענן</u> - לאור המורכבות של הליך המעבר לענן, הרשות ממליצה כבר בשלבים הראשונים של המעבר לענן, לבצע הליך מיפוי של מאגרי המידע של הארגון, תוך תיעוד והבנה מעמיקה של מבנה התשתיות המחשוב הארגוני ואופן זרימת המידע בהן. מיפוי זה יאפשר הבנה של המאגרים שנכון לשלב בהם שירותי ענן (מבחינת מטרות השימוש בהם, רגישות המידע בהם ועוד). לפי מיפוי זה ניתן יהיה לשקול אם להתקשר עם ספקי שירותי ענן מרובים או בודד וביחס לאילו מאגרים. הרשות ממליצה לבחון גם את מספר ספקי הענן בהם מתכוון הארגון להיעזר, כיוון שריבוי ספקי ענן עלול להעלות את רמת הסיכון למידע המצוי אצל ספקים רבים יותר. כן רצוי לשים לב ששימוש בריבוי ספקי ענן ידרוש גם תשומות הכשרה רבות לאור הצורך בכוח אדם מיומן כאמור לעיל.

תהליך המעבר לענן יכול להביא לפתרונות רבים עבור ארגונים שונים, אך לצד זאת, קיימים אתגרים וסיכונים רבים הנלווים לשימוש בפלטפורמת הענן. לכן חשוב להקפיד על המלצות הרשות בעניין האתגרים שצוינו כדי להבטיח כי הארגונים העושים שימוש במערכות ענן עומדים בדרישות החוק. בהקשר זה נעיר שיישומים שונים (דוגמת AI) דורשים מענה משפטי מותאם,[5] כך גם יתכן שבסקטורים שונים יש הנחיות נוספות לגבי מעבר למחשוב ענן.[6] מסמך אתגרי ענן המלא זמין כאן. נציין כי ביום 3.10.2024 פרסם מערך הסייבר הלאומי מסמך שכותרתו "אבטחת שירותי ענן ציבוריים בראי איום הכופרה (Ransomware)", שראוי לדעתנו שארגונים המנהלים פעילות בענן יכירו אף אותו.

<u>מדריך פעולה ליישום תקנה 10(ד) לתקנות אבטחת מידע לשמירת קבצי תיעוד ולוגים</u>

4. תקנה 10 לתקנות אבטחת מידע, הרלוונטית למאגרי מידע שחלה עליהם רמת אבטחה בינונית או גבוהה, מכילה הוראות בדבר מנגנון בקרה ותיעוד של הגישה למערכות המאגרים,[7] של מאגרים מסוג זה. התקנה קובעת כי יש צורך לקיים מנגנון תיעוד אוטומטי אשר יתעד את (א) זהות המשתמש, (ב) התאריך והשעה של ניסיון הגישה, (ג) רכיב המערכת שאליו בוצע ניסיון הגישה, (ד) סוג הגישה, היקפה, ו-(ה) אם הגישה אושרה או נדחתה (להלן: "**מנגנון הבקרה**"). את נתוני מנגנון הבקרה נכנה "**נתוני התיעוד**" (log).

[5] ראו למשל מזכרנו בדבר חובת יידוע במסגרת איסוף ושימוש במידע אישי.
[6] ראו למשל מזכרנו בנושא נוהל בנקאי תקין 362.
[7] ""מערכות המאגר" – מערכות המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע" לפי תקנות אבטחת מידע.

ירושלים
הגן הטכנולוגי מלחה, בניין 1
ט. 02-5607607
פ. 02-5639948

תל אביב
מגדל אלקטרה, יגאל אלון 98
ט. 03-6078607
פ. 03-6078666

באר שבע
גב ים, רחוב האנרגיה 77
ט. 03-6071450
פ. 08-6155780

סידני, אוסטרליה
50 Carrington St, NWS 2000
T. +61-2-90606206

אגמון עם טולצ'ינסקי, משרד עורכי דין | www.agmon-law.co.il

5. לפי תקנות אבטחת מידע מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים בארגון. נתוני התיעוד צריכים להישמר למשך 24 חודשים, וארגונים צריכים לקיים נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ולערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

6. ביום 29.9.2024 הרשות פרסמה מסמך ("**מסמך קבצי תיעוד**"), שמטרתו להבהיר את האופן בו יש ליישם את החובות בתקנה. זאת מתוך רצון ליישם את התכלית של בדיקה בדיעבד של אירועי אבטחה או ליקויים אחרים, תוך הבטחת זמינותם של נתוני התיעוד, ומניעת זליגתם מחד; ומאידך מתוך רצון לסייע לארגונים לנהל את תיעוד ושמירת הלוגים בצורה יעילה, נגישה וזמינה.

7. **סוגי גישה למערכות המאגר**. במסמך קבצי התיעוד הרשות מתייחסת לשני סוגי גישה למערכות המאגרים - (א) <u>גישה המתבצעת בידי משתמש</u> - בגישה המתבצעת בידי משתמש אנושי, לשרת המכיל מאגר מידע או לשרת אשר מספק שירותים המבוססים על מאגר מידע, כוונת הרשות היא לתחנת קצה (endpoint) מרוחקת של לקוח (client) שבאמצעותה המשתמש ניגש לצד השרת (server)עליו רץ היישום (האפליקציה), במטרה לאחזר מידע מן המאגר; (ב) <u>גישה המתבצעת באמצעות רכיב קוד</u> - בגישה שמתבצעת בידי רכיב קוד כלשהו, כוונת הרשות היא לממשק פנימי שמקשר בין צד השרת שעליו היישום רץ, לבין מאגר המידע שהיישום ניגש אליו. במצב זה ייתכן שמדובר גם בממשק חיצוני שמקשר בין יישום החיצוני לבין שרת, במטרה לאחזר מידע מן המאגר או ביישום החיצוני ייגש ישירות למאגר.

8. **מערכות קריטיות**. במסמך קבצי התיעוד מבארת הרשות שהחובה הקבועה בהוראות תקנה 10 לתקנות אבטחת מידע היא לשמור לוגים של כל מערכות המאגר, משמעה, אחסון כל קובץ שמתעד את הפעולה ונתוני הפעולה, של כל אחת ממערכות האבטחה של המאגר והמערכות המשמשות את המאגר. זאת, תוך הקפדה על זמינותם ונגישותם של הלוגים השמורים לפרק זמן של שנתיים לפחות. יחד עם זאת -

א. **לפי הרשות יש מערכות קריטיות לתפעול מאגר המידע ואבטחתו, שחובה לנטרן ולתעד את פעילותן באופן רציף. את נתוני התיעוד של המערכות האלה, יש לשמור נגישים, זמינים ומאובטחים במערכות אחסון מקומיות למשך כל התקופה הקבועה (שנתיים).**

ב. **ביחס ליתר מערכות המאגר, סבורה הרשות שניתן לשמור אותם במערכות אחסון מקומיות, למשך שישה חודשים לפחות, ובתום שישה חודשים ניתן להעבירם למשך הזמן שנותר(שנה**

וחצי) לאחסון במנגנון שימור ארוך טווח (דוגמת התקן אחסון המצוי מחוץ לחצרי הארגון (Off Site).

9. במסמך קבצי התיעוד, הרשות נותנת דוגמאות למערכות קריטיות עליהן תחול החובה האמורה בסעיף 8א לעיל, והנחיות ספציפיות לגבי קבצי התיעוד מהן. מערכות אלה כוללות את מערכות ההפעלה, בסיסי הנתונים, מערכות ניהול הקבצים, ה-Active Directory , EDR, NAC, Firewall, WAF ו-DBFW.

10. נציין שביחס למשך שמירת נתוני התיעוד, ניתן מקום מיוחד בטבלת הקנסות במצויה בתוספת השלישית של תיקון 13 לחוק הגנת הפרטיות, התשמ"א-1981.[8]

מסמך קבצי התיעוד המלא זמין כאן.

מידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו.

נשמח לסייע לכם לבחון את עמידת ארגונכם בהוראות דיני הגנת הפרטיות בכלל, והוראות המסמכים השונים בפרט. לצורך כך אתם מוזמנים ליצור איתנו קשר, על מנת לתאם שיחת ייעוץ אישית, במסגרתה נוכל גם לסקור את הוראות המסמכים ביתר פירוט.

[8] חוק הגנת הפרטיות (תיקון מס' 13), התשפ"ד-2024.

עו"ד סער רוסמן, שותף
מחלקת הייטק, טכנולוגיה והון סיכון
וראש תחום סייבר ופרטיות
Saar@agmon-law.co.il

מתן אברמוביץ, עו"ד
מחלקת הייטק, טכנולוגיה והון סיכון
Matana@agmon-law.co.il

עדו רביד, עו"ד
מחלקת הייטק, טכנולוגיה והון סיכון
Ador@agmon-law.co.il