ממצאי פיקוח רוחב של הרשות להגנת הפרטיות בקרב ספקיות שירותי אחסון ועיבוד מידע

מזכר לקוחות – נובמבר 2020

לקוחות יקרים,

ביום 2.11.2020, פרסמה הרשות להגנת הפרטיות ("**הרשות**") את ממצאי הליך פיקוח הרוחב שערכה בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל ("**הדו"ח**"). הדו"ח עסק בחברות המעניקות שירותי אחסון ועיבוד מידע עבור בעלי מאגרי מידע שונים, דוגמת שירותי תוכנה as a Service - SaaS) (Software או פלטפורמה (Platform as a Service - PaaS), הכוללים בין היתר אפליקציות, ממשקים ופיתוחים שונים עבור בעלי מאגרי מידע (לרבות אירוח אתרי אינטרנט הכוללים מידע אישי).
חברות נוספות שנבחנו במסגרת הפיקוח, היו כאלה המעניקות שירותי תשתית (IaaS Infrastructure as a Service), הכוללים בעיקר מתן שירותי אחסון עבור בעלי המידע.

חוק הגנת הפרטיות התשמ"א- 1981 ("**החוק**") מגדיר "מחזיק, לענין מאגר מידע", כ- "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". עמדת הרשות, כפי שהיא מובאת בדו"ח, היא שחברה המספקת לאחר שירותי אחסון או גיבוי של מידע, לרבות בדרך של העמדת שרתים, נחשבת כ"מחזיק" של המידע, **גם אם תוכן המידע מוצפן והמפתח אינו מצוי בידיה אלא בידי בעל המאגר**. לפי עמדת הרשות, הצפנת המידע המאוחסן והצפנת אופן העברתו, אינה משחררת את המחזיק מאחריותו על פי הוראות החוק והתקנות שהותקנו מכוחו ("**התקנות**").

במסגרת הדו"ח ציינה הרשות, כי ניכר שקיימת אי בהירות באשר להיקף תחולת החוק והתקנות על כלל הגופים המשתייכים למגזר שפוקח במסגרת הדו"ח (מתוקף היותם מחזיקים במאגר מידע) וכן כי נמצא שבתחומים מסוימים אין עמידה מספקת בהוראות החוק והתקנות בקרב מגזר זה.

בנוסף ציינה הרשות שבכוונתה להמשיך לפעול לאכיפת מדיניותה בקרב בעלי ומחזיקי מאגרי מידע באמצעות פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות בגופים שהונחו לתקן ליקויים. **משכך, אנו ממליצים ללקוחותינו העוסקים בתחומים האמורים להקדים ולוודא את עמידתם בהוראות החוק והתקנות.**

להלן הרחבה אודות האמור בדו"ח וממצאיו:

שאלוני הביקורת שנשלחו לחברות בחנו ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות ובהם (1) בקרה ארגונית וממשל תאגידי - קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות, ומינויים של גורמים אחראיים בתחום; (2) ניהול מאגרי מידע - אופן קבלת ההסכמה לשימוש במידע, מידת התאמת השימוש במידע למטרה לשמה נאסף, מתן זכות עיון במידע, ועמידה בהוראות החוק בעניין דיוור ישיר; (3) אבטחת מידע - נבחנה עמידת הגופים בהוראות תקנות אבטחת מידע, בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם; ו-(4) שימוש בשירותי מיקור חוץ - נבחנו ההתקשרויות של בעלי מאגרי המידע עם גורמים חיצוניים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע.

WWW.AGMON-LAW.CO.IL

ירושלים הגן הטכנולוגי מלחה, בניין 1
טלפון: 02-5607607 | פקס: 02-5639948

תל אביב מגדל אלקטרה, יגאל אלון 98
טלפון: 03-6078607 | פקס: 03-6078666

Sydney Australia 50 Carrington Street,
Sydney NSW 2000 | 61-2-90606206

באר שבע נב ים, רחוב האנרגיה 77
טלפון: 03-6071450

בין הממצאים בתחומים השונים שנבדקו, מצאנו לנכון לציין את הליקויים הבאים:

1) אצל גופים רבים נמצאו פערים משמעותיים ביישום ההנחיות הנוגעות לחובה לבצע סקרי סיכונים ומבדקי חדירות ביחס למאגרי מידע ברמת אבטחה גבוהה.

2) ליקוי מרכזי נוסף במגזר שנבדק מתייחס לעיבוד מידע אישי במיקור חוץ. הדו"ח מציג תמונת מצב לפיה גופים רבים מאלה שנבדקו אינם עומדים בהוראות החוק והתקנות ביחס למיקור חוץ הן כספקי שירותי מיקור חוץ (עבור בעלי המאגרים) והן כמי שמקבלים שירותים מספקי מיקור חוץ בעצמם.

3) ממצא נוסף העולה מהדו"ח הוא שבקרב כשליש מהגופים שנבדקו נמצאה רמת עמידה בינונית ומטה באופן ניהול הבקרה הארגונית והממשל התאגידי. בין היתר נמצאו גופים מפוקחים אשר מינו בעלי תפקידים ללא כתב מינוי ועדכון בפנקס מאגרי המידע כנדרש בחוק.

4) בנוסף, נמצא שגופים שנבדקו, שהינם בעלי תקן ISO27001, סברו שקיום התקן מספק את הדרישות החוק בתחום אבטחת המידע. זאת, בניגוד להנחיית רשם מאגרי המידע מס' 2018/03 הקובעת כי עמידה בתקן מהווה ראיה לעמידה בחלק מהוראות התקנות בלבד, וגם זאת בתנאים מסוימים.

בהמשך הדו"ח, הרשות מספקת הבהרות והמלצות לגופים המשתייכים למגזר המפוקח. **הבהרות והמלצות אלה מתייחסות בין היתר ביחס לנושאים הבאים**:

1. **בתחום הבקרה הארגונית וממשל תאגידי**

(א) מוצע לגופים לוודא רישום כלל המאגרים שבבעלותם/החזקתם בהתאם להוראות החוק ולוודא שקיימת התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום בפנקס מאגרי המידע (בכרטיס המאגר).

(ב) מוצע לגופים לפעול לביצוע ביקורות אבטחת מידע, סקר סיכונים ומבדקי חדירות כנדרש בתקנות.

2. **ניהול מאגרי מידע**

(א) הרשות מבהירה שיש לקבל הסכמות מנושאי המידע כנדרש בחוק לצורך שמירת פרטיהם במערכות הארגון.

(ב) הרשות מזכירה שגופים המחזיקים בחמישה מאגרים, נדרשים למסור לרשם מידי שנה רשימה של המאגרים, שמות בעלי המאגרים וממונה אבטחת המידע ופרטים נוספים כנדרש בחוק. ראוי לציין שלגופים כאלה ישנן דרישות נוספות בדין דוגמת מינוי ממונה אבטחת מידע.

3. **דיוור ישיר** - יש להקפיד לציין את הפרטים המנויים בסעיף 17ו לחוק (לרבות כי הפניה היא בדיוור ישיר, זהות ומען בעל מאגר מידע, מקור המידע, למי יימסר המידע, הזכות להימחק ממאגר המיועד לדיוור ישיר ועוד).

תל אביב מגדל אלקטרה, יגאל אלון 98
טלפון: 03-6078607 | פקס: 03-6078666

באר שבע גב ים, רחוב האנרגיה 77
טלפון: 03-6071450

ירושלים הגן הטכנולוגי מלחה, בניין 1
טלפון: 02-5607607 | פקס: 02-5639948

Sydney Australia 50 Carrington Street,
Sydney NSW 2000 | 61-2-90606206

WWW.AGMON-LAW.CO.IL

4. **אבטחת מידע** - הרשות ממליצה לוודא קיומם של נהלי אבטחת מידע הכוללים את הנושאים המפורטים בתקנות ובחינת תוקפם מעת לעת כנדרש בתקנות, ובכלל זאת קיום נהלים בתחום הרשאות הגישה, ביקורות, אבטחה פיזית, התמודדות עם אירועי אבטחה ועוד.

5. **עיבוד מידע אישי במיקור חוץ** - הרשות מזכירה שגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, נדרשים לוודא עמידה בתקנה 15 לתקנות ובהנחיות הרשם בנושא מיקור חוץ, לרבות בחינה מקדימה של הסיכונים הכרוכים בהתקשרות, עריכת הסכם מתאים ופיקוח ובקרה על הגורם החיצוני.

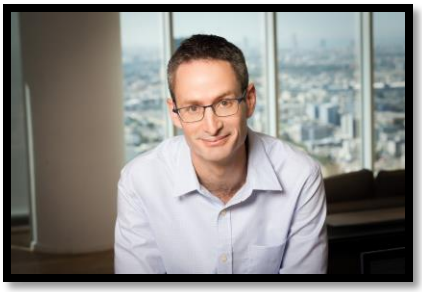
לקריאת הדו"ח המלא לחצו כאן.

נשמח לסייע לארגונכם לוודא עמידה בהוראות הגנת הפרטיות ואבטחת המידע החלות עליו.

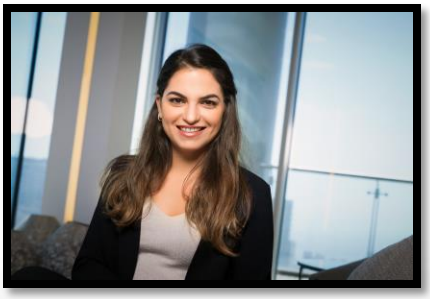
המידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו.

הצוות ישמח לעמוד לרשותכם בכל שאלה:

עו"ד אסנת סרוסי פירסטטר
ראש מחלקת הייטק וטכנולוגיה
osnat@agmon-law.co.il
03-6078607



עו"ד סער רוסמן
שותף, מחלקת הייטק וטכנולוגיה
saar@agmon-law.co.il
03-6078607



עו"ד אורן שטרית
מחלקת הייטק וטכנולוגיה
oransh@agmon-law.co.il
03-6078607