טיוטת תיקון להוראה בנושא מחשוב ענן – נב"ת 362

עדכון לקוחות - מחלקת הייטק וטכנולוגיה – מאי 2022

לקוחות יקרים,

בתחילת החודש פרסם המפקח על הבנקים ("**המפקח**") טיוטת תיקון להוראה בנושא מחשוב ענן ניהול בנקאי תקין - הוראה מס' 362 ("**המסמך**").

במסגרת המסמך עתיד להתבטל האיסור לעשות שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ו/או מערכות ליבה של תאגידים בנקאיים, וכן נקבע כי תאגידים בנקאיים יחויבו בקביעת מדיניות לשימוש בשירותי מחשוב ענן, במסגרתה, בין השאר, ייקבעו מאפייני השירותים המוגדרים כ"מחשוב ענן מהותי".

ראינו לנכון לסקור בתמצית את עיקרי המסמך, בעיקר משום שלדעתנו כבר במתכונתו הנוכחית (כטיוטה), המסמך מצביע על האופן העדכני בו המפקח רואה את נושא שירותי מחשוב הענן בסקטור עליו הוא אמון.

נשמח לעמוד לרשותכם על מנת לסייע לארגונכם לעמוד בהוראות דיני הגנת הפרטיות ואבטחת המידע החלים עליו.

להלן נפרט את עיקרי המסמך.

במסגרת המסמך המפקח מציין כי הפיקוח על הבנקים רואה את השימוש בשירותי מחשוב ענן כמקרה פרטי של מיקור חוץ. על כן על תאגיד בנקאי העושה שימוש בשירותי מחשוב ענן יחולו לבד מהנחיות המסמך גם הוראות ניהול בנקאי תקין מס' 359A בנושא "מיקור חוץ" ("**נב"ת 359A**").

המסמך מגדיר "מחשוב ענן" כמודל המאפשר גישה נוחה מכל מקום, לפי דרישה, למאגר משותף של משאבי מחשוב הניתנים להגדרה (למשל: רשתות, שרתים, אחסון, יישומים ושירותים), שניתן לספק ולשחרר במהירות. זאת, למעט ענן פרטי.

"ענן פרטי" מוגדר במסמך כתשתית הענן המוקצית לשימושו הבלעדי של תאגיד בנקאי יחיד. הענן יכול להיות בבעלותו, בניהולו ובתפעולו של התאגיד הבנקאי או צד שלישי או בכל שילוב ביניהם והוא יכול להתקיים בחצרי התאגיד הבנקאי או מחוצה להם. המסמך אינו חל על ענן פרטי.

1. יש לשים לב שבמסגרת נב"ת 359A ישנה הפנייה למקורות דין אחרים.

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

מחשוב ענן מהותי. ביחס להגדרת מחשוב ענן מהותי המסמך מאמץ את הגדרת מיקור חוץ בנב"ת 359A ולעניין המהות מפנה לסעיף 27 בנב"ת 359A ולשיקולים הבאים – (א) סוג הענן, (ב) סוג שירות מחשוב הענן, (ג) קיומו של מידע המוגדר על ידי התאגיד הבנקאי כ-"רגיש" במסגרת שירות מחשוב הענן, (ד) קיומו של מידע שאינו מוגדר כ-"רגיש", אך שממנו ניתן להסיק פרטים שיאפשרו לתקוף או לפגוע בתאגיד הבנקאי ו/או בלקוחותיו, (ה) אם שירות מחשוב הענן מספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד, ואם קיימים אמצעים דומים מסוגיהם גם בחצרי התאגיד הבנקאי.

ממשל תאגידי. לפי התיקונים במסמך, פרק ב' בנב"ת 359A בנושא ממשל תאגידי (הגדרת תיאבון סיכון, אחריות כוללת לפעילות המוצאת למיקור חוץ, אישור התקשרויות ודיון על בסיס תקופתי וכו') יחול גם על מחשוב ענן שאינו מחשוב ענן מהותי. זאת, למעט סעיף 16 (המתייחס למעורבות הביקורת הפנימית כבר מהשלבים הראשונים בבחינת נאותות תהליכי העברת פעילות למיקור חוץ באופן ובהיקף שייקבע על ידה).

מדיניות ותוכנית עבודה. המסמך קובע כי על ההנהלה הבכירה (א) להכין תכנית עבודה רב שנתית למחשוב ענן ("**תכנית רב שנתית**"), אשר תיתן מענה, בין היתר, לסיכונים הגלומים בטכנולוגיות מחשוב הענן והבקרות המיושמות או המתוכננות להפחתתם; (ב) לעקוב באופן שוטף אחר יישום מדיניות מסמך "מדיניות השימוש בטכנולוגיית מחשוב ענן" (אותה היא אמורה לגבש כאמור במסמך).[2]

דירקטוריון התאגיד הבנקאי אמור (א) לדון ולאשר את מסמך "מדיניות השימוש בטכנולוגיית מחשוב ענן"; (ב) לאשר את התוכנית הרב שנתית; (ג) לוודא שהשימוש בטכנולוגיות מחשוב ענן יהיה לפי המדיניות האמורה.

מומחי תכן וגורמים מלווים. המסמך קובע כי התאגיד הבנקאי (א) יגדיר גורם הכפוף למנהל חטיבת טכנולוגיות המידע שיכיר את הארכיטקטורות והקונפיגורציות של שירותי מחשוב הענן; (ב) יבחן הגדרת גורם אחראי לכל נותן שירותי מחשוב ענן שבשימוש; (ג) יגדיר גורם הכפוף למנהל הסיכונים, שיכיר באופן מעמיק את סיכוני כלל הפעילות במחשוב ענן.[3]

---

2. לפי המסמך, המדיניות שתגובש על ידי ההנהלה הבכירה ותאושר על ידי הדירקטוריון תבחין בין מחשוב ענן מהותי הדורש את אישור הדירקטוריון לבין מחשוב ענן הדורש את אישור ההנהלה הבכירה. המדיניות תתאם לדרישות הרגולטוריות השונות הרלבנטיות לרבות אלו העוסקות בטכנולוגיית מידע ותקשורת, אבטחת מידע והגנת הסייבר, המשביות עסקית וניהול סיכונים תפעוליים.
3. לפי המסמך מחשוב ענן עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מוגברים. בהתאם לכך נדרש התאגיד הבנקאי בהיערכות מתאימה במסגרת הקו הראשון ובמסגרת הקו השני עם תחילת השימוש בשירותי מחשוב ענן. ראו בפירוט בגוף המסמך בקשר עם האמור.

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

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

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

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

WWW.AGMON-LAW.CO.IL

התאמות לנב"ת 359A. היות ולפי המסמך שירות מחשוב ענן הוא מקרה פרטי של מיקור חוץ, יחולו עליו גם הוראות נב"ת 359A (ללא קשר למהותיות שלו), בכפוף לשני חריגים: (א) חובת דיווח למפקח על הבנקים לא תחול על מחשוב ענן בין אם מהותי ובין אם שאינו מהותי; (ב) הוראות בדבר המשכיות עסקית (המפורטות בסעיף 29 בנב"ת 359A) ו-התקשרות עם נותן שירות (בסעיפים 18-23 לנב"ת 359A) לא יחולו על מחשוב ענן **שאינו** מהותי.

הוראות חיצוניות. בסעיף 7 למסמך נמחקה התייחסות לנב"ת שונים, אך המפקח מבהיר כי אין במחיקה זו כדי לגרוע מחובת התאגיד הבנקאי לעמוד בהם. זהו גם המצב ביחס למחיקת ההתייחסות (בסעיף 8) להנחיית רשם מאגרי מידע מס' 2/2011 – "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" ("**הנחיית מיקור חוץ**"), הקובעת בנספח ג' את תחולת ההנחיה על גופים הנתונים לפיקוח של המפקח או של הממונה על שוק ההון (כך שדומה שאין ללמוד גם ממחיקה זו שההנחיה אינה חלה בכללותה).

אחריות על ספקי משנה. בסעיף 9 נקבעה חובה לוודא כי נותן שירות מחשוב הענן יישא באחריות כלפי התאגיד הבנקאי, גם במקרה בו נותן שירות מחשוב הענן עושה שימוש בנותן שירות משני.[4]

ניהול סיכונים. סעיף 19 למסמך קובע את האופן בו יבוצעו הערכת הסיכונים וסקר הסיכונים. לפי הסעיף (א) הערכת הסיכונים תיעשה קודם להתקשרות עם נותן שירותי מחשוב הענן ותעודכן באופן שוטף במהלך תקופת ההתקשרות (למשל בהתאם לשינויים טכנולוגיים, משפטיים ,רגולטוריים, עסקיים וארגוניים אצלו ואצל נותן שירותי מחשוב הענן). הערכת הסיכונים צריכה לכלול גם סיכונים ייחודיים (טכנולוגיים ואחרים) הקשורים לשימוש במחשוב ענן, ובמיוחד את אלה המנויים בנספח ב' למסמך ("היבטים עיקריים להערכת סיכונים במחשוב ענן"); (ב) ביחס למחשוב ענן מהותי יבוצע סקר סיכונים כאמור בהוראות נב"ת 350 ("ניהול סיכונים תפעוליים") לפחות אחת לשנתיים[5], ויש לוודא קיומן של בקרות מפצות לפי הערכת הסיכון.

במחשוב ענן מהותי, התאגיד הבנקאי יבצע בדיקת נאותות (Due Diligence) לנותן שירותי מחשוב הענן כאמור בפרק ו', לרבות זיהוי והערכת הסיכונים הפוטנציאליים בהתקשרות עמו והשימוש בשירותיו, ולכל הפחות יבחן (א) את העמידה של נותן שירותי מחשוב הענן בכל דין ורגולציה הרלבנטיים (לרבות במדינה בה הוא פועל);

---

4. ראו והשווה לתקנה 15.(א)(2)(ז) לתקנות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("תקנות אבטחת מידע").
5. לפי המסמך הדוחות הסדירים המוגשים להנהלה הבכירה ולדירקטוריון בנושאי סיכונים תפעוליים, כאמור בהוראת ניהול בנקאי תקין מס' 350 בנושא "ניהול סיכונים תפעוליים", יכללו התייחסות פרטנית לסיכוני מחשוב ענן.

WWW.AGMON-LAW.CO.IL

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

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

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

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

(ב) את העמידה של נותן שירותי מחשוב הענן ברמת הגנת סייבר נאותה לפי "מדיניות השימוש בטכנולוגיות מחשוב ענן";[6] (ג) את הסיכונים המפורטים בנספח ב' להוראה זו – "היבטים עיקריים להערכת סיכונים במחשוב ענן".

במסגרת המסמך, התאגיד הבנקאי נדרש להגדיר (א) תחומי אחריות לניהול, שליטה, אישור ותיעוד של שירותי מחשוב הענן בתאגיד הבנקאי; (ב) מודל חלוקת אחריות (Shared Responsibility Model) ("**מודל ה-SRM**") בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן (ובכלל זה בהיבטי אבטחת מידע והגנת הסייבר).

כן נדרש התאגיד הבנקאי לתעד ולעדכן אחת לתקופה (א) ההחלטות והשיקולים במימוש שירותי מחשוב הענן, כגון: רמת מהותיות, שיקולים לשימוש בשירותי ענן, סיכונים, אישורים וכו'; (ב) מאפייני נותן שירותי מחשוב הענן והחוזה עימו, כגון: תאריכי חתימת החוזה ,חידושו, ואופציות להארכתו, מיקום מתקני הענן ואחסון הנתונים, סוג ועלות השירות, סמכויות שיפוט וכו'; (ג) מאפייני שירותי מחשוב הענן, כגון: מיפוי ותיאור הארכיטקטורה, הממשקים ודרישות אבטחת המידע והגנת הסייבר וכו'.[7]

<u>ההתקשרות עם נותן שירותי מחשוב הענן.</u> לפי המסמך יש להתייחס בחוזה מול נותן שירותי מחשוב הענן, בין היתר, לנושאים הבאים[8]: (א) מחיקה או פעולה דומה של המידע של התאגיד הבנקאי ממערכות נותן שירותי מחשוב הענן והתחייבותו כי לא ניתן יהיה לאחזר מידע זה במערכותיו; (ב) יכולתו של התאגיד הבנקאי לקבל מידע הרלוונטי לפעילויות שהועברו למיקור חוץ המוחזק אצל נותן השירות, לרבות ביקורות שבוצעו אצל נותן השירות, ולבחון אותו או להעביר אותו למפקח על הבנקים על פי בקשתו (יש לשים לב לסעיף 22 בנב"ת 359A לפיה במקרה של מחשוב ענן מהותי יש לאפשר למפקח לקיים ביקורות אצל נותן השירות); (ג) יישום הנחיות המודל שנקבע לעניין חלוקת אחריות לפי מודל ה-SRM באותו עניין; (ד) הגדרת מיקום מתקן הענן ממנו יינתן השירות ומיקום אחסון הנתונים וחובת מתן הודעה על שינוי כאמור; (ה) הגדרת יכולת התאגיד הבנקאי בהפעלתם ובהפסקתם של שירותי מחשוב ענן מהותיים או רכיבים מתוך שירותים;[9]

---

6. דוגמא הניתנת במסמך היא דיווחים ביחס לאירועי סייבר ואירועי אבטחת מידע.
7. ראו והשוו להנחיית מיקור חוץ, ותקנה 15(א)(3) לתקנות אבטחת מידע.
8. זאת מבלי לגרוע מהוראות נב"ת 359A ונב"ת 363 ("ניהול סיכוני סייבר בשרשרת אספקה").
9. לפי המסמך - לרבות חסימות גישה, ככל שרלוונטי ובעת חירום בדוגמת אירוע סייבר, בין אם באופן עצמאי ובין אם על ידי נותן שירות מחשוב הענן בהתאם לבקשת התאגיד הבנקאי ומתוך הצורך לצמצם סיכונים בעת חירום. הגדרת התהליכים התומכים ביכולות אלה יוגדרו תוך התייחסות למשאבים של נותן שירותי הענן בהם נעשה שימוש משותף על ידי התאגיד הבנקאי וגורמים אחרים המקבלים שירות מאותו נותן שירות מחשוב ענן.

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

(ו) סוגיות המובאות בסעיף 23(ח) לנב"ת 359A; (ז) סוגיות המובאות בסעיף 23(ו) לנב"ת 359A; (ח) בחינת שילוב התחייבות נותן שירות מחשוב הענן להשתתפות בתרגילי סייבר שיקיים מולו התאגיד הבנקאי אחת לתקופה, בהתאם לאופי היישום; (ט) יישום בקרות מפצות הנדרשות מנותן שירות מחשוב הענן בהתאם להערכת סיכונים כמפורט בסעיף 19 למסמך.

<u>ההתקשרות עם נותן שירותי מחשוב ענן מהותי</u>. לפי המסמך, התאגיד הבנקאי ינהל את ההתקשרות עם נותן שירותי מחשוב ענן מהותי, לכל הפחות, על פי העקרונות הבאים:

א- מעקב אחר ביצועי השירות, בטחון ואבטחת המידע, ועמידה ביעדי השירות המוסכמים עם נותן שירותי מחשוב הענן, כל זאת באמצעי ניטור התואמים את תיאבון הסיכון של התאגיד הבנקאי.

ב- הערכה של ההסדרים עם נותן שירותי מחשוב הענן, בהתייחס למצבי סיכון, אירועים ושינויים שהתחוללו במהלך התקופה ולתפעול קריטי של מערכות המחשוב של התאגיד הבנקאי בענן. הערכה זו תכלול גם הערכת סיכונים ותביא בחשבון את יכולותיו של נותן שירותי מחשוב הענן, תוך עמידה בדרישות בהיבטי טכנולוגיה, המשכיות עסקית, אבטחת מידע והגנת הסייבר.

ג- מעקב אחר יישום מודל ה-SRM מול נותן שירותי מחשוב הענן.

ד- ניהול ממשקים קבועים ושוטפים של מנהל ההמשכיות העסקית ומנהל הגנת הסייבר של התאגיד הבנקאי עם הגורמים בתאגיד הבנקאי אשר ממונים על הקשר השוטף עם נותן שירותי מחשוב הענן, לרבות הגדרה ברורה של סמכויותיהם ותפקידיהם במסגרת ממשקים אלה.

ה- קיום תכנית יציאה/סיום התקשרות. התכנית תיבדק ותתעדכן אחת לשלוש שנים.

ו- חובה לבחון את הצורך בעדכון החוזה עם נותן שירותי מחשוב הענן לכל הפחות אחת לשלוש שנים או בעת התרחשות אירוע או שינוי מהותי בשירותי מחשוב הענן או שינוי בכל דין ורגולציה הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן.

ז- בכל שינוי בבעלות שליטה על נותן שירותי מחשוב הענן, על התאגיד הבנקאי לבחון מחדש את ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם ע"י הבעלים על ידי בעלי השליטה החדשים.

<u>אבטחת מידע, הגנת הסייבר והמשכיות עסקית</u>. פרק ז' למסמך קובע, בין היתר, כדלקמן:

1. על התאגיד הבנקאי לנהל את סיכוני אבטחת המידע והגנת הסייבר במחשוב ענן,[10] תוך התייחסות בין היתר להיבטים של סיווג המידע, מיקום מפתחות ההצפנה, מעורבות התאגיד הבנקאי בניהול מפתחות ההצפנה ורמת ההצפנה, שיטת ההצפנה ועוד.[11]

10. מהותי ושאינו מהותי
11. בהקשר זה ניתן להשוות למודלים ודרישות של רגולטורים אחרים המאסדרים טיפול במידע אישי.

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

2. על המידע של התאגיד הבנקאי להיות מוצפן בעת העברתו בתקשורת וכן בעת אחסונו (in transit and at rest). במקרים בהם יש קושי לתאגיד הבנקאי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידו כמידע רגיש או שיש בחשיפתם כדי לפגוע בתאגיד הבנקאי ובלקוחותיו.
3. על התאגיד הבנקאי לוודא שביכולתו לבצע ניטור רציף, מלא ובזמן אמת באופן שיאפשר לזהות אירוע סייבר מוקדם ככל הניתן ובאופן הרלוונטי לסוג שירות מחשוב הענן, וזאת לגבי אירועי סייבר[12] הקשורים לשירותי מחשוב ענן בין היתר כמפורט בנספח ג' למסמך ("ניטור אירועי סייבר").
4. על התאגיד הבנקאי להיערך להתמודדות עם אירועי סייבר בשירותי מחשוב ענן. היערכות זו תבוצע, בין היתר, בכלים הבאים: (א) קיום תרגילי סייבר ;(ב) ביצוע תרחישים של אירועי סייבר;[13] (ג) ביצוע, לכל הפחות, של תרחיש קיצון אחד מייצג בפעילות אחת או יותר משירותי מחשוב הענן המהותיים שלו.
5. על התאגיד הבנקאי לוודא כי עבור כלל ערוצי הגישה אל שירות מחשוב הענן וממנו, קיימים אמצעים לאבטחת מידע ולהגנת הסייבר שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפת התאגיד הבנקאי. בסעיף זה אין שינוי מנוסח המסמך הקיים.
6. ככל שמחשוב הענן מהווה שירות חיוני לתאגיד הבנקאי יחולו הוראות נב"ת 355 ("ניהול המשכיות עסקית").
7. ככל שמחשוב הענן הינו מחוץ לישראל, על התאגיד הבנקאי לבחון תכניות מענה לתרחיש של אי זמינות השירות.[14]
8. התאגיד יעריך את יכולת ההמשכיות העסקית של נותן השירות אל מול איומי הייחוס המקומיים של המדינה המארחת.
9. באתר מחשוב בענן ראשי או חלופי - התאגיד הבנקאי נדרש לוודא עמידתו של האתר בדרישות Tier III לפי תקן ה-UpTime Institute (UTI).

<u>דיווח</u>. פרק ח' קובע כי על תאגיד בנקאי להעביר אחת לשנה (בסוף השנה) דיווח לידי המפקח לפי הוראת דיווח לפיקוח מס' 881 ("דיווח על מחשוב ענן (שנתי)"). כאשר כאמור לעיל התאגיד הבנקאי אינו נדרש להודיע מראש למפקח על יישום של מחשוב ענן מהותי.

---

12. "אירוע סייבר" כהגדרתו בנב"ת 361 ("הגנת הסייבר").
13. תרחישים אלו צריכים לכלול לכל הפחות: (1) מצב בו שירות המחשוב בענן עשוי להישאר פעיל ונגיש אך בפועל לא ניתן להסתמך על אמינות הנתונים המוצגים בו; (2) תקיפות מערך הגיבויים של שירות המחשוב בענן; (3) תקיפות שכחלק מהטיפול בהן יידרש ניתוק גישה מיעדים ספציפיים.
14. למשל כתוצאה מנתק תקשורתי לחו"ל ו/או מאירועים גיאופוליטיים מול המדינה הזרה.

WWW.AGMON-LAW.CO.IL

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

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

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

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

<u>תחולת הוראות המסמך ונב"ת 359A על מחשוב ענן מהותי ושאינו מהותי</u>. במסגרת המסמך מובאת (בנספח א') טבלה המרכזת את התכולה של המסמך ונב"ת 259A על מחשוב ענן מהותי ומחשוב ענן שאינו מהותי.

<u>היבטים עיקריים להערכת סיכונים במחשוב ענן</u>. מצאנו לנכון לסקור את עיקרי הוראות נספח ב' בדבר הערכת סיכונים במחשוב ענן. במסגרת הנספח המתוקן –

א- נמחקו סיכונים המופיעים בנב"ת 359A ועובו סיכונים הנובעים (א) משימוש או מאי שימוש בתצורת ענן המבוססות על שילוב של מספר פתרונות שונים של מחשוב ענן; (ב) הכרוכים בקבלת שירות מחשוב ענן המספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד.

ב- כן נוספה התייחסות להיבטי סיכון הכרוכים בשינויים הנדרשים מנותן שירותי מחשוב הענן כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים והורחבו ההיבטים הקשורים לסיכוני התפעול השוטף (והקטנתם בין היתר באמצעות הסדרת תחומי אחריות בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן).

ג- בהקשר זה נציין כי לדעתנו ניתן ללמוד גם משיקולים שמונים רגולטורים אחרים ביחס לסיכונים במחשוב ענן לשם הערכת הסיכונים הכרוכים שבשירותים אלה ואופן ההתמודדות עימם.

<u>ניטור אירועי סייבר במחשוב ענן</u>. מצאנו לנכון לסקור את עיקרי הוראות נספח ג' בדבר ניטור אירועי סייבר. הנספח דורש בין היתר כי –

א- כי ניטור אירועי הסייבר ישתלב במערך הניטור השוטף של התאגיד הבנקאי. כאשר הניהול וההגדרה יהיו לכל הפחות בהתאמה לאופי השירות בו נעשה שימוש. כך למשל ההיבטים האבטחתיים והיכולות הנדרשות כאשר השירות בו עושה התאגיד שימוש הוא שירות SaaS שונה ממצב בו מדובר בשירותי IaaS.

ב- בהתאם לאמור לעיל, הניטור יכלול בין היתר חריגות מפעילות לגיטימית בתשתיות הבנק, כך לדוגמא שינויי ארכיטקטורת הרשת (סגמנטציה), הקמת שרתים חדשים, גישה לבסיסי נתונים, שינוי במנגנוני הצפנה, תעבורת רשת חריגה מסביבת הענן.

ג- במצבים בהם נעשה שימוש באמצעות כלים המסופקים ע"י נותן שירותי מחשוב הענן, יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של התאגיד הבנקאי.

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

ד- בנוסף, במצבים בהם נעשה שימוש במערכת ניטור המצויה בסביבות הענן, בסביבה תשתיתית בה מצוי שירות מחשוב ענן מהותי של התאגיד הבנקאי, התאגיד הבנקאי יגדיר פעולות בקרה להמשך רציפות ניטור שירות מחשוב הענן המהותי גם בעת ניתוק תקשורת בין התאגיד הבנקאי למערכת הניטור של סביבת הענן.

<u>תחולה</u>

א- מועד התחילה לאמור במסמך אמור להיות יום 1.1.2023 ("**מועד התחילה**").

ב- לעניין חוזים שנכרתו לפני המועד בו יפורסם המסמך – במועד החידוש הקרוב של החוזה ולא יאוחר מ-4 שנים ממועד התחילה. יש לשים לב כבל שנדרש לבצע התאמות בהתקשרויות קיימות יש לעשות עד אותה עת.

ג- לעניין חוזים שנכרתו לאחר מהמועד בו יפורסם המסמך ועד למועד התחילה – לא יאוחר משנה ממועד התחילה. גם במקרה זה יש לשים לב כבל שנדרש לבצע התאמות בהתקשרויות קיימות יש לעשות עד אותה עת.

ד- תאגידים בנקאיים רשאים ליישם את ההוראה בכללותה לפני מועד התחילה.

לקריאת המסמך המלא לחצו כאן.

**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.

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

צוות מחלקת הייטק וטכנולוגיה ישמח לעמוד לרשותכם:

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