

מחשוב ענן

פרק א': רקע

מבוא

1. בשנים האחרונות מתפתחת מגמה של מעבר הולך וגובר לתצורות שונות של מחשוב ענן (Cloud Computing). טכנולוגיות אלו מאפשרות ניצול יעיל ונוח של משאבי מחשוב תוך אפשרות לשיתוף משאבים ולשימוש בהם לפי הצורך; זאת, בד בבד עם חיסכון בעלויות ציוד, שטחי ה-Data Center, חשמל וכד', התורמים למחשוב ידידותי יותר לסביבה (Green Computing).
2. בצד היתרונות הגלומים בשימוש בטכנולוגיות ענן, שימוש בטכנולוגיות אלו עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מהותיים הקשורים לאבטחת מידע וסייבר, המשכיות עסקית, שליטה ובקרה על נכסי ה-IT, וכד'. סיכונים אלו נגזרים, בין היתר, מתלות בספקים או טכנולוגיות ספציפיים; כלי ניהול, אבטחה, שליטה ובקרה שטרם הבשילו; קשיים בהגנה על המידע וביישום בקרות נאותות; העצמת הנזק הפוטנציאלי במקרה של כשל, במיוחד כאשר נוצרות נקודות כשל יחידות (Single Points of Failure); רגישות הרכיבים הייעודיים של הטכנולוגיה; קושי בהפרדת תפקידים ועוד. נציין כי סיכונים אלו בחלקם אמנם מוכרים, אך נוכח המאפיינים הספציפיים של טכנולוגיות אלו והעובדה שמדובר בטכנולוגיות מתפתחות וכלי אבטחת מידע שאינם בהכרח בשלים, גלומים בהן סיכונים ייחודיים.
3. בוטל.

תחולה

4. (א) הוראה זו תחול על התאגידים הבאים כהגדרתם בחוק הבנקאות (רישוי), התשמ"א-1981 (להלן בהוראה זו – "תאגיד בנקאי"):

(1) תאגיד בנקאי;

(2) תאגיד בנקאי כאמור בסעיפים 11(א) (א3) ו-1(ב3);

(3) תאגיד בנקאי כאמור בסעיף 11(ב);

(4) סולק כהגדרתו בסעיף 36ט.

(ב) המפקח רשאי לקבוע הוראות מסוימות שונות מאלו המפורטות להלן שיחולו על תאגיד בנקאי מסוים או לפטור במקרים חריגים תאגיד בנקאי מסוים מהוראה מסוימת.

פרק ב': כללי

5. תאגיד בנקאי לא יעשה שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ו/או מערכות ליבה.
6. תאגיד בנקאי לא יאחסן, יעביר או יעבד מידע, שמוגדר על ידו כ"רגיש" (כגון: נתוני לקוחות, מידע עסקי חסוי וכד'), בענן מחוץ לגבולות מדינת ישראל, אלא אם כן, וידא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לדירקטיבה על הגנת המידע במדינות האיחוד האירופי.
7. מחשוב ענן מהווה מקרה פרטי של מיקור חוץ כהגדרתו בפרק ו' להוראת ניהול בנקאי תקין מס' 357. לפיכך, יש לפעול גם בהתאם להוראה כאמור, בנוסף להוראות ניהול בנקאי תקין מס' 361, 363, 367, 359A.
8. אין בהוראה זו כדי לגרוע מהחובות החלות על התאגיד הבנקאי לפי כל החוקים והתקנות הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, ובכלל זאת, חוק הגנת הפרטיות ותקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001, וכן, הנחיית רשם מאגרי מידע מס' 2/2011 – "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי".
9. התאגיד הבנקאי ייבחן את הצורך בהסתייעות, לפי העניין, ביועצים חיצוניים מומחים בהפחתת הסיכונים הגלומים בשימוש בטכנולוגיות ענן.

פרק ג': ממשל תאגידי**דירקטוריון**

10. על תאגיד בנקאי אשר בוחן שימוש בטכנולוגיות מחשוב הענן להביא את הנושא לדיון מקדמי בדירקטוריון, לפני הפעלת טכנולוגיות מחשוב ענן. בדיון זה יוצגו הסיכונים הגלומים בטכנולוגיות מחשוב ענן והבקורות המיושמות או המתוכננות להפחתתם. על הדירקטוריון:

(א) לדון בסיכונים אלו, להחליט האם לתת אישור מקדמי למהלך ולהנחות את הנהלת התאגיד הבנקאי בדבר הפעולות שעליה לנקוט – בין היתר ע"פ המפורט בהוראה זו.
(ב) להנחות את ההנהלה לגבש ולאשר מסמך מדיניות לשימוש בטכנולוגיות מחשוב ענן.

11. בהמשך לאמור בסעיף 10 לעיל, הדירקטוריון ידון ויאשר מדיניות לשימוש בטכנולוגיות מחשוב ענן.

12. כאמור בסעיף 13 (א) להלן, על הדירקטוריון לאשר יישום של כל מחשוב ענן מהותי.
13. על דירקטוריון התאגיד הבנקאי לוודא שהשימוש בטכנולוגיות מחשוב ענן יהיה ע"פ המדיניות שנקבעה כאמור.

הנהלה בכירה

13. (א) על ההנהלה הבכירה לגבש מדיניות לשימוש בטכנולוגיות מחשוב ענן אשר תקבע בין היתר את סוגי היישומים בטכנולוגיית מחשוב ענן בהם נדרש אישור של הדירקטוריון (להלן: "מחשוב ענן מהותי" - דוגמאות למחשוב ענן מהותי בנספח א') וסוגי היישומים בהם נדרש אישור הנהלה.

(ב) מסמך המדיניות יתייחס לסמכויות, אחריות ופעולות גופי ניהול שירותי ענן, גופי הבקרה והבקורות; סוגי השירותים והיקפם; תהליכי אישור ודרגי אישור; אחריות הגורמים השונים בתאגיד הבנקאי לטיפול בהיבטים משפטיים, תחזוקה, ניטור, הגנת הסייבר ואבטחת מידע וכד'. המדיניות תיתן מענה, בין היתר, גם לנדרש בהוראה זו.

פרק ד': יישומי מחשוב ענן המחייבים קבלת היתר - בוטל

פרק ה': ניהול סיכונים

17. (א) לפני יישום מחשוב ענן נדרש התאגיד הבנקאי לבצע תהליכי מיפוי והערכת סיכונים נאותים, במעורבות כלל הגורמים הרלוונטיים בתאגיד הבנקאי, ובהתייחס לכלל ההיבטים הרלוונטיים, כמפורט בסעיף 19 להלן.
18. במחשוב ענן מהותי, לפני התקשרות עם ספק שירותי הענן, על התאגיד הבנקאי לבצע בדיקת Due Diligence לרבות בנוגע לחוסנו הכלכלי, יכולתו המקצועית וניסיונו לספק שירותים דומים. ראוי לבצע מעת לעת בדיקה כאמור, גם במהלך תקופת ההתקשרות.
19. תאגיד בנקאי יבצע מיפוי והערכת סיכונים לכל יישום של מחשוב ענן מהותי. הערכת הסיכונים תעשה קודם להתקשרות עם הספק ותעודכן באופן שוטף במהלך תקופת ההתקשרות בין היתר, בהתאם לשינויים כגון: טכנולוגיים, משפטיים, רגולטוריים, עסקיים וארגוניים אצלו ואצל ספק שירותי הענן. על התאגיד הבנקאי לוודא קיום בקרות מפצות מתאימות. על אף שמחשוב ענן מהווה מקרה פרטי של מיקור חוץ, הערכת הסיכונים צריכה לכלול גם סיכונים ייחודיים (טכנולוגיים ואחרים) הקשורים לשימוש במחשוב ענן. דוגמאות של היבטים שיש לקחת בחשבון מובאות בנספח ב'.
20. על התאגיד הבנקאי לוודא שביכולתו לבצע ניטור אירועי סייבר ואבטחת מידע הקשורים ליישום מחשוב ענן מהותי ולשימוש במערכות מחשוב ענן. אם ניטור זה מבוצע באמצעות כלים המסופקים ע"י הספק, יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של התאגיד הבנקאי.
21. במחשוב ענן מהותי, על התאגיד הבנקאי לוודא כי עבור כלל ערוצי הגישה מ/אל ספק מחשוב הענן, קיימים אמצעים להגנת הסייבר ואבטחת המידע, שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפת התאגיד הבנקאי.
22. על המידע של התאגיד הבנקאי להיות מוצפן בעת העברתו בתקשורת וכן כאשר הוא מאוחסן במערכת שאינה לשימוש הבלעדי (Multi-tenancy). במקרים בהם יש קושי לתאגיד הבנקאי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידו כרגישים ושיש בחשיפתם כדי לפגוע בתאגיד הבנקאי ובלקוחותיו. יש לבחון יישום המאפשר, ככל שניתן, לאחסן את מפתחות ההצפנה אצל התאגיד הבנקאי.

פרק ו': הסכם התקשרות עם ספק שירותי הענן

23. מבלי לגרוע מהחובות החלות על התאגיד הבנקאי לפי סעיף 18 להוראת ניהול בנקאי תקין מס' 357 והוראת ניהול בנקאי מס' 363, במחשוב ענן מהותי, הסכם ההתקשרות עם הספק יכלול, בין היתר:

(א) קיום אפשרות חד-צדדית של התאגיד הבנקאי להפסיק את השימוש בשירותי הספק או לעבור לספק אחר תוך העברת נתוניו הרלבנטיים ממערכות הספק תוך זמן קצר, מחיקתם במערכות הספק והתחייבות הספק שלא ניתן לאחזר נתונים אלו במערכותיו.

(ב) התייחסות לקבלת מידע הנוגע למבדקים וביקורות על הספק שירותי הענן.

(ג) מתן אפשרות לתאגיד הבנקאי על בסיס הערכת הסיכונים, לבצע ביקורות אצל ספק שירות הענן.

(ד) מתן אפשרות לפיקוח על הבנקים לבצע ביקורות אצל ספק שירות הענן ביישום מחשוב ענן מהותי.

24. בכל שינוי בבעלות על ספק שירותי הענן, על התאגיד הבנקאי לבחון מחדש את ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם ע"י הבעלים החדשים.

פרק ז': מכתב ההיתר - בוטל

פרק ח': דיווח לפיקוח

27. אחת לשנה (בסיום שנה קלנדרית), על תאגיד בנקאי להעביר בכתב לידי הפיקוח על הבנקים :

(א) רשימה מעודכנת של יישומי מחשוב הענן, לרבות תיאור היישום, מועד היישום, הגורם המאשר ושם ספק שירותי הענן. במחשוב "ענן מהותי" יש לציין את מיקום שרתי הענן.

(ב) דיווח על יישומי מחשוב ענן עתידיים.

תאריך	פרטים	גרסה	עדכונים חוזר מס'
05/07/2017	מכתב מפקח מקורי	1	2536
13/11/2018	עדכון	2	2579

נספח א' – דוגמאות למחשוב ענן מהותי

- יישום מחשוב הענן כולל מידע המוגדר על ידי התאגיד הבנקאי כמידע רגיש.
- המידע אינו מוגדר ע"י התאגיד הבנקאי כמידע רגיש, אך כתוצאה מחשיפתו, ניתן להסיק פרטים שיאפשרו לתקוף או לפגוע בתאגיד הבנקאי ו/או בלקוחותיו.
- שיבוש או הפסקת הפעילות של יישום מחשוב הענן, עלולים לפגוע באופן משמעותי בהתנהלות התאגיד הבנקאי ו/או ביכולתו לתת שירות ומענה ללקוחותיו.
- יישום מחשוב הענן מספק אמצעי הגנת הסייבר ואבטחת מידע כרובד הגנה יחיד, ושלא קיימים אמצעים דומים מסוגיהם גם בחצרי התאגיד הבנקאי.

נספח ב' – הערכת סיכונים - דוגמאות של היבטי מחשוב ענן

- ממשל תאגידי, מדיניות ונהלים, ביקורת פנימית וחיצונית – האם מסמכי המדיניות מתייחסים כראוי לשימוש במחשוב ענן?
- סיכון רגולטורי - קושי בעמידה בחוקים, תקנות ורגולציות של מדינת ישראל ושל המדינה שבה פועלת או מאוחסנת המערכת ו/או הנתונים. יש חשיבות, בין היתר, להתייחס לסוגיות כגון חובת הספק למסור מידע לגורמי חוק ואכיפה גם ללא ידיעת התאגיד הבנקאי. יש היבטים חוקיים רבים הקשורים לאי-אחידות ההגדרות והדרישות במדינות שונות.
- סיכון סיסטמי הנגזר מספק שירותי הענן הנותן שירותים למספר תאגידים בנקאיים.
- מחזור חיי הנתונים, לרבות מיקום, ריבוי העתקים וחשיפת נתונים.
- נידודת נתונים, רכיבים ומערכות - למשל, האם השימוש ברכיבי ענן של ספק מסוים מגביל את התאגיד הבנקאי ועלול למנוע ממנו את האפשרות לעבור לספק אחר או להעביר את המידע ו/או המערכות חזרה לחצרי הבנק.
- סיכוני סייבר ואבטחת מידע, לרבות דלף מידע, שינויים בתפיסה המסורתית, השימוש בכלי אבטחה ייעודיים, אופן ניהול מפתחות ההצפנה.
- הרשאות גישה, תוך הפעלת כלים המתאימים לסביבת מחשוב ענן.
- ניהול שינויים וניהול נכסי טכנולוגית המידע - למשל, האם לתאגיד הבנקאי יש שליטה על שינויים במערכות והאם תהליכי השינויים תואמים את מדיניות ונהלי התאגיד הבנקאי.
- סיכונים הקשורים להמשכיות עסקית ו-BCP/DRP, לרבות שינויים בתצורת רשת התאגיד הבנקאי, ומיקומם הגאוגרפי של שרתי הענן ובכללם שרתי הגיבוי.
- סיכונים הקשורים לסביבות העבודה וכלי הניהול העלולים להוסיף רמת תחכום ומורכבות למערכות.
- סיכונים משפטיים וביניהם היבטי סודיות, שמירת נתונים, הבעלות על המידע ורישוי תוכנות.
- טיפול באירועים חריגים, לרבות הסדרי הדיווח והטיפול, והסדרת תחומי האחריות.
- סיכונים הנוגעים למעטפת התקיפה כגון: שילוב מכשירים ניידים (טלפונים ניידים, טאבלטים וכל אמצעי נייד אחר) ביישום מחשוב הענן.
- סיכונים הכרוכים בשרשרת אספקה של יישום מחשוב ענן, ע"פ האמור בהוראת ניהול בנקאי תקין מס' 363.