בנק ישראל
המפקח על הבנקים

ירושלים, י״ב תמוז תשע״ה
29 יוני 2015
15LM2087

לכבוד
התאגידים הבנקאיים – לידי המנהל הכללי

הנדון: **ניהול סיכונים בסביבת מחשוב ענן**

1. רקע

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).

בצד היתרונות, שימוש בטכנולוגיות אלו עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מהותיים הקשורים לאבטחת מידע, 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.

2. תחולה

הוראות מכתב זה יחולו בהתאם להוראות התחולה הקבועות בסעיף 2 להוראת ניהול בנקאי תקין מספר 357 (להלן: ״ההוראה״).

3. כללי

3.1. תאגיד בנקאי לא יעשה שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ו/או מערכות ליבה.

3.2. תאגיד בנקאי לא יאחסן מידע או נתוני לקוחות בענן מחוץ לגבולות מדינת ישראל, אלא אם כן, וידא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

3.3. מחשוב ענן מהווה מקרה פרטי של מיקור חוץ כהגדרתו בפרק ו׳ להוראה. לפיכך, יש לפעול בהתאם להוראת ניהול בנקאי תקין מס׳ 357, בפרט בהתייחס לאמור בסעיפים 17, 18 ו- 30 להוראה.

3.4. הננו מפנים את התאגידים הבנקאיים לחוקים ולתקנות הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, ובכלל זאת, לחוק הגנת הפרטיות ולתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001. בנוסף, אנו מפנים להנחיית רשם מאגרי מידע מס' 2/2011 – "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי".

3.5. מומלץ כי התאגיד הבנקאי יסתייע, לפי העניין, ביועצים חיצוניים מומחים בהפחתת הסיכונים הגלומים בשימוש בטכנולוגיות ענן.

4. ממשל תאגידי

4.1. 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 והבקרות המיושמות או המתוכננות להפחתתן. על הדירקטוריון לדון בסיכונים אלו, להחליט האם לתת אישור מקדמי למהלך, ולהנחות את הנהלת הבנק בדבר הפעולות שעליה לנקוט – בין היתר ע"פ המפורט במכתב זה. לפי העניין, ינחה הדירקטוריון את ההנהלה לגבש ולהגיש לאישורו מסמך מדיניות לשימוש בטכנולוגיות מחשוב ענן.

4.2. בהמשך לאמור בסעיף 4.1 לעיל, הדירקטוריון ידון ויאשר מדיניות לשימוש בטכנולוגיות מחשוב ענן. מסמך המדיניות יתייחס לסמכויות, אחריות ופעולות גופי ניהול שירותי ענן, גופי הבקרה והבקרות; סוגי השירותים והיקפם; תהליכי אישור ודרגי אישור; אחריות הגורמים השונים בבנק לטיפול בהיבטים משפטיים, תחזוקה, ניטור, אבטחת מידע וכד'. המדיניות תיתן מענה, בין היתר, גם לנדרש במכתב זה.

4.3. לפני כל התקשרות עם ספק שירותי מחשוב ענן (להלן: "ספק שירותי הענן" או "הספק") יערך דיון בהנהלה, ולפי העניין, גם בדירקטוריון.

4.4. על הנהלת התאגיד הבנקאי לוודא שכל שימוש בטכנולוגיות מחשוב ענן יהיה ע"פ המדיניות שנקבעה כאמור.

5. ניהול סיכונים

5.1. 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.

5.2. תאגיד בנקאי יבצע מיפוי והערכת סיכונים לכל התקשרות עם ספק שרותי ענן, הערכת הסיכונים תעשה קודם להתקשרות ותעודכן באופן שוטף במהלך תקופת ההתקשרות בין היתר, בהתאם לשינויים כגון: טכנולוגיים, עסקיים וארגוניים אצלו ואצל ספק שירותי הענן, רגולטוריים. 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. בהתאם לכך, על התאגיד הבנקאי לוודא שיקבל מספק שירותי הענן את המידע הנדרש לצורך ביצוע הערכת הסיכונים, לרבות הנדרש בסעיף 6.1.1 להלן.

5.3. על תאגיד בנקאי לוודא שביכולתו לבצע ניטור אירועי אבטחת מידע הקשורים לשימושו 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 הבנק.

5.4. על המידע של התאגיד הבנקאי להיות מוצפן בעת העברתו בתקשורת וכן כאשר הוא מאוחסן במערכת שאינו לשימושו 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. מפתחות ההצפנה יאוחסנו אצל התאגיד הבנקאי ולא אצל הספק.

6. הסכם התקשרות עם הספק

6.1. הסכם ההתקשרות עם הספק יכלול, בין היתר את הדרישות הבאות:

6.1.1. קבלת דוחות ביקורת פנימיים של הספק ודוחות ביקורת חיצוניים שנערכו על פעילותו, לרבות דוחות ביקורת שבוצעו ע"י גופים רגולטוריים. בנוסף, ההסכם יכלול אפשרות לתאגיד הבנקאי לדרוש במקרים מיוחדים מהספק לערוך עבורו ביקורת בנושא מסוים.

6.1.2. 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.

6.1.3. מתן אפשרות לפיקוח על הבנקים לבצע ביקורות אצל ספק שירותי ענן.

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

7. קבלת היתר מהמפקח על הבנקים

על אף האמור בסעיף 3.3 לעיל, התאגיד הבנקאי נדרש לקבל היתר מראש ובכתב מהמפקח על הבנקים לפני כל התקשרות עם ספק מחשוב ענן שבמסגרתו מאוחסן מידע אצל ספק גם אם לא מדובר במידע של לקוחות. לצורך קבלת היתר זה, על הבנק לפנות לפיקוח על הבנקים לפחות 60 ימים לפני הפעלת השירות.

8. תחילה

הנחיות מכתב זה ייכנסו לתוקף עם פרסומו.

בכבוד רב,

דוד זקן

המפקח על הבנקים

<u>נספח - הערכת סיכונים - דוגמאות של היבטי מחשוב ענן</u>

- 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.
- ניידות 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.
- אבטחת מידע, לרבות שינויים בתפיסה המסורתית והשימוש בכלי אבטחה ייעודיים.
- 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. סביבות 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.