בנק ישראל
הפיקוח על הבנקים
אגף מדיניות והסדרה

תל-אביב, ט״ו באלול תשע״ד
10 בספטמבר 2014
חוזר מס׳ XX

לכבוד
התאגידים הבנקאיים וחברות כרטיסי האשראי – לידי המנהל הכללי

הנדון: **<u>ניהול סיכונים בסביבת מחשוב ענן</u>**

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

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

3. הטיפול במחשוב ענן

3.1. מחשוב ענן מהווה מקרה פרטי של מיקור חוץ כהגדרתו בפרק ו׳ להוראה. לפיכך, יש לפעול בהתאם לאמור בסעיפים 17, 18 ו- 30 להוראה.

3.2. בנוסף ולנוכח המאפיינים הייחודיים של מחשוב ענן, אנו מציגים מספר הנחיות נוספות בקשר עם שימוש במחשוב ענן:

3.2.1. התאגיד הבנקאי לא יעשה שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ומערכות ליבה.

3.2.2. התאגיד הבנקאי לא יאחסן מידע או נתוני לקוחות בענן מחוץ לגבולות מדינת ישראל, אלא אם כן, בדק ווידא שספק שירותי מחשוב הענן (להלן: "ספק שירותי הענן" או "הספק") מקיים את רמת ההגנה בהתאם לדירקטיבה על הגנת המידע במדינות האיחוד האירופי.

3.2.3. לפני ההתקשרות 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.

3.2.4. התאגיד הבנקאי יוודא שתהיה לו אפשרות להפסיק את השימוש בשירותי הספק או לעבור לספק אחר תוך מחיקת הנתונים והתחייבות הספק שלא ניתן לאחזר את נתוניו במחשביו.

3.2.5. 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.

3.2.6. על התאגיד הבנקאי לוודא שבפועל יש לו אפשרות 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.

3.2.7. על התאגיד הבנקאי לעגן בהסכם כתוב מול ספק שירותי הענן אפשרות לביצוע ביקורת ע"י הביקורת הפנימית והביקורת החיצונית של התאגיד הבנקאי וכן ע"י הפיקוח על הבנקים.

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

3.4. לפני הפעלת טכנולוגיות מחשוב ענן, התאגיד הבנקאי מתבקש:

3.4.1. לקבוע מדיניות במסמך כתוב תוך התמקדות בסמכויות, 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 לאמור בסעיפים 3.2.1 עד 3.2.6 לעיל.

3.4.2. להביא את מסמך המדיניות לדיון ואישור ההנהלה והדירקטוריון.

3.4.3. לבצע הערכת סיכונים ולקבוע 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.

3.4.4. להביא את נושא השימוש בטכנולוגיות מחשוב הענן לדיון ואישור בדירקטוריון. בדיון זה יוצגו הסיכונים הגלומים בטכנולוגיות מחשוב ענן והבקרות המיושמות או המתוכננות להפחתתן. על הדירקטוריון לדון בסיכונים אלו, לתת אישור מקדמי למהלך, ולהנחות את הנהלת הבנק בדבר הפעולות שעליה לנקוט – בין היתר ע"פ המפורט במכתב זה.

3.4.5. למען הסר ספק, גם תאגיד בנקאי שהחל בשימוש בטכנולוגיות אלו לפני קבלת מכתבנו זה יפעל בהתאם ויקבל את אישור הדירקטוריון, תוך פרק זמן סביר, כתנאי להמשך הפעילות.

3.4.6. על ההנהלה לוודא שכל שימוש בטכנולוגיות מחשוב ענן יהיה ע"פ המדיניות שנקבעה כאמור.

3.5. 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".

4. קבלת היתר מהמפקח על הבנקים

על אף האמור בסעיף 3.1 לעיל, התאגיד הבנקאי נדרש לקבל היתר מהמפקח על הבנקים לפני שימוש במחשוב ענן שבמסגרתו מאוחסן מידע אצל ספק גם אם לא מדובר במידע של לקוחות. לצורך קבלת היתר זה, על הבנק לפנות לפיקוח על הבנקים לפחות 45 יום לפני הפעלת השירות.

5. תחילה

הנחיות מכתב זה ייכנסו לתוקף עם פרסומו.

בכבוד רב,

נספח - 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.
- 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.