בנק ישראל
הפיקוח על הבנקים
אגף מדיניות והסדרה

טיוטה

תל-אביב, כ״ו בסיוון תשע״ז
20 ביוני 2017
חוזר מס׳ – 06 - טיוטה

לכבוד
התאגידים הבנקאיים וחברות כרטיסי אשראי

הנדון: מחשוב ענן
(ניהול בנקאי תקין הוראה מס׳ XXX)

כללי

1. בשנים האחרונות גובר השימוש בארגונים בישראל ובחו״ל בטכנולוגיות מחשוב ענן (Cloud Computing). טכנולוגיות אלו מאפשרות הקטנת הוצאות מחשוב- ציוד, תשתיות, תוכנה, שטחי ה- Data Center וחיסכון באנרגיה נוכח ניצול יעיל ונוח של משאבי מחשוב ואפשרות לשיתוף משאבים ולשימוש בהם לפי הצורך. קיימים 3 מודלים עיקריים של מחשוב ענן: Infrastructure as a Service -IaaS, Platform as a Service – PaaS ו-Software as a -SaaS Service. בשימוש בטכנולוגיות מחשוב ענן יש כדי לסייע לתאגיד בנקאי לעמוד בעקרון TTM- Time to Market. כך למשל, תאגיד בנקאי יכול להאיץ באופן משמעותי תהליכי פיתוח מערכות ע״י שימוש במודל PaaS או לוותר על פיתוח עצמי ולעשות שימוש באמצעות מודל SaaS בתוכנה שפותחה, מתוחזקת ופועלת בענן.

2. מחשוב ענן מהווה סוג של מיקור חוץ. למרות האמור לעיל, שימוש בטכנולוגיות ענן עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מהותיים וסיכוני סייבר ואבטחת מידע כגון: דלף מידע רגיש, המשכיות עסקית, שליטה ובקרה על נכסי ה- IT, וכד׳. סיכונים אלו

נגזרים, בין היתר, מתלות בספקים או בטכנולוגיות ספציפיים; החלשת השליטה והבקרה על השימוש בטכנולוגיות ענן; 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. נוכח המאפיינים הספציפיים של טכנולוגיות מחשוב ענן בהשוואה למיקור חוץ מסורתי, והעובדה שכלי הבקרה והאבטחה אינם בהכרח בשלים, גלומים בהן סיכונים ייחודיים וסיכונים מוכרים שבהתממשותם הנזק לתאגיד הבנקאי עלול להיות משמעותי.

3. הוראה זו מבטלת את מכתב המפקח על הבנקים בנושא "ניהול סיכונים בסביבת מחשוב ענן" מיום 29.06.2015 שבו הוגדרו לראשונה התנאים לשימוש של תאגיד בנקאי בטכנולוגיות מחשוב ענן. במכתב המפקח נדרש התאגיד הבנקאי לפנות לפיקוח על הבנקים בבקשת היתר לפני כל שימוש בטכנולוגיות מחשוב ענן. נוכח הניסיון שנצבר בנושא הן בפיקוח על הבנקים והן בקרב תאגידים בנקאיים, הוחלט לצאת עם הוראה שתמנע את הצורך מתאגיד בנקאי לפנות לפיקוח בבקשת היתר לפני כל שימוש בטכנולוגיות מחשוב ענן, אלא רק במקרים שמוגדרים בהוראה.

4. ההוראה קובעת הנחיות ותנאים הנדרשים לשימוש של תאגיד בנקאי בטכנולוגיות מחשוב ענן, תוך הגדרת המקרים בהם נדרש מראש היתר מהפיקוח על הבנקים והמקרים בהם התאגיד הבנקאי רשאי לעשות שימוש בטכנולוגיות מחשוב ענן ללא קבלת היתר כאמור. בכל מקרה, ההוראה אינה מאפשרת לתאגיד בנקאי לעשות שימוש בטכנולוגיות ענן עבור פעילויות ליבה ו/או מערכות ליבה.

5. פרסום הוראה מיוחדת לנושא מחשוב ענן נועד להדגיש את הצורך לנהל את הסיכונים לכל שימוש בטכנולוגיות מחשוב ענן, תוך מעורבות דרגי הניהול הבכירים בתאגיד הבנקאי. הוראה זו הינה כללית לכל סוגי המודלים של מחשוב ענן, לרבות אלו המפורטים בסעף 1 לעיל.

6. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגידה, קבעתי את הוראת הניהול התקין הבאה, כמפורט להלן.

מבנה ההוראה

7. ההוראה כוללת שבעה פרקים:

(א) **פרק א': רקע** – כולל מבוא להוראה ותחולה.

(ב) **פרק ב': כללי** - מפרט הנחיות כלליות.

(ג) **פרק ג': ממשל תאגידי** – עוסק בציפיות ממעורבות הדירקטוריון וההנהלה הבכירה.

(ד) **פרק ד': יישומי מחשוב ענן המחייבים קבלת היתר** - מפרט את המקרים בהם נדרש תאגיד בנקאי לקבל היתר מהפיקוח על הבנקים לפני שימוש בטכנולוגיות מחשוב ענן.

(ה) **פרק ה' : ניהול סיכונים** – מפרט הנחיות הנוגעות לניהול סיכונים ויישום אמצעי הגנת סייבר ואבטחת מידע עבור תאגיד בנקאי שנדרש להיתר לשימוש בטכנולוגיות מחשוב ענן.

(ו) **פרק ו' : הסכם התקשרות עם ספק שירותי ענן** – כולל הנחיות הנוגעות להסכם ההתקשרות של התאגיד הבנקאי עם ספק שירותי ענן.

(ז) **פרק ז' : מכתב ההיתר** – כולל נושאים שעשויים להיכלל במכתב ההיתר לתאגיד הבנקאי.

(ח) **נספח א' : הערכת סיכונים – דוגמאות של היבטי מחשוב ענן** – כולל דוגמאות לסיכונים שיש לקחת בחשבון בעת ביצוע הערכת סיכונים.

מבוא, תחולה (סעיפים 1 – 4 להוראה)

8. ההוראה מציגה יתרונות של שימוש בטכנולוגיות מחשוב ענן, בד בבד עם הסיכונים הכרוכים בשימוש בטכנולוגיות אלו. אחד הסיכונים המרכזיים נגזר מהקושי של התאגיד הבנקאי לקיים שליטה ובקרה נאותים על היישום בענן ועל אמצעי הגנת הסייבר ואבטחת מידע. ההוראה מדגישה כי בצד הסיכונים המסורתיים, המתעצמים בשימוש בטכנולוגיות מחשוב ענן, קיימים סיכונים ייחודיים.

9. ההוראה מאפשרת למפקח על הבנקים לקבוע הוראות מסוימות שונות מההוראות המפורטות בהוראה, ובמקרים חריגים בלבד אף להתיר שימוש בטכנולוגיות מחשוב ענן שלא ע"פ האמור בהוראה; זאת, נוכח התפתחויות שונות שעשויות להתרחש במערכת הבנקאית ו/או ההתפתחויות המתמשכות הן של טכנולוגיות מחשוב ענן והן של כלי הגנת הסייבר ואבטחת המידע, שיתכן וישליכו על עמידה בהנחיות מסוימות.

כללי (סעיפים 5 – 9 להוראה)

10. ההוראה אינה מאפשרת לתאגידים הבנקאיים לעשות שימוש בשירותי ענן עבור פעילויות ליבה ו/או מערכות ליבה, כהגדרתן ע"י התאגיד הבנקאי.

11. במקרה שתאגיד בנקאי מאחסן, מעביר או מידע שהוא הגדיר כ"רגיש", עליו לוודא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לדירקטיבה על הגנת המידע במדינות האיחוד האירופי. התאגיד הבנקאי מתבקש לעקוב באופן שוטף אחרי העדכונים בדירקטיבה זו ולוודא שהספק עומד בהסדרים המשתנים.

12. ההוראה מציינת באופן מפורש מספר הוראות ניהול בנקאי תקין הרלבנטיות למחשוב ענן בהיבטי ניהול סיכונים והטמעת אמצעי הגנה ובקרה להפחתתם. במיוחד מדגישה ההוראה את הוראת ניהול בנקאי תקין מס' 357, מאחר ומחשוב ענן מהווה מקרה פרטי של מיקור חוץ. לפיכך, יש לתת דגש על סעיפים 17, 18, 30 להוראה 357.

13. ההוראה מפנה את התאגידים הבנקאיים לחוקים, לתקנות ולהנחיות הרלבנטיים להוראה זו כדוגמת חוק ותקנות הגנת הפרטיות.

ממשל תאגידי (סעיפים 10 – 13 להוראה)

14. תאגיד בנקאי שבוחן את האפשרות לעשות שימוש בטכנולוגיית שימוש ענן, נדרש להביא את הנושא לדיון בדירקטוריון עוד לפני הפעלת היישום. בדיון מתבקש הדירקטוריון לדון בסיכונים הגלומים בטכנולוגיה זו, כפי שהוצגו בפניו וגם בבקרות להפחתת סיכונים אלו. הדירקטוריון מצופה להבין את ההשלכות של התממשות הסיכונים על התאגיד הבנקאי ולקוחותיו ולהשתכנע שהבקרות נותנות מענה מספק לסיכונים אלו.

15. בנוסף לאמור לעיל, על הדירקטוריון להנחות את ההנהלה לגבש ולאשר מסמך מדיניות בנושא השימושים במחשוב ענן, וגם עליו לדון ולאשר מדיניות זו. מסמך המדיניות צריך לכלול התייחסות להיבטים שונים, לרבות אלו המפורטים בהוראה. ההנהלה מתבקשת לוודא שהתאגיד הבנקאי פועל ע"פ המדיניות שאושרה.

16. במקרה שהתאגיד הבנקאי מתכנן לעשות שימוש בטכנולוגיית שימוש ענן, המחייב היתר לפי הנאמר בהוראה, יש לקיים דיון בהנהלה או בוועדת הנהלה מתאימה ביישום לפני הפעלתו. במקרים מסויימים, כאשר למשל מדובר ביישום קריטי לבנק או שחושף את התאגיד הבנקאי לסיכונים מהותיים, ראוי שיתקיים דיון גם בדירקטוריון.

יישומי מחשוב ענן המחייבים קבלת היתר (סעיפים 14 – 17 להוראה)

17. ההוראה מפרטת את המקרים בהם התאגיד הבנקאי נדרש להיתר מהפיקוח על הבנקים, לפני שמיישם שימוש בטכנולוגיות ענן. המקרה הראשון: כאשר היישום כולל מידע רגיש. התאגיד הבנקאי מצופה להגדיר מהו מידע "רגיש" ולסווג את המידע בהתאם למדיניות ולכללים שקבע. מידע רגיש אינו בהכרח מידע שנוגע רק לפרטים חסויים של לקוחות התאגיד או עובדי הבנק, אלא לכל מידע אחר בהתאם למדיניות התאגיד, לדוגמא: מידע עסקי בהתאם לכללים שנקבעו כאמור. המקרה השני: כאשר חשיפת המידע, גם אם אינו רגיש, עלולה לאפשר לגורם עוין לתקוף את התאגיד הבנקאי או לפגוע בו. המקרה השלישי: אם השבתת פעילות היישום מכל סיבה שהיא, עלולה לפגוע בהתנהלות א התאגיד הבנקאי ו/או ביכולתו לספק שירותים ללקוחותיו. המקרה הרביעי שבו נדרש היתר: אם היישום כולל אמצעי הגנה השייכים לאותו סוג או משפחה של פתרונות, ואין בחצרי התאגיד אמצעי נוסף מלבדם. לדוגמא: התאגיד הבנקאי מתכנן שכל מערך הסינון של הדוא"ל יתנהל בענן.

18. התאגיד הבנקאי אינו נדרש להיתר במקרים שאינם מפורטים לעיל. מספר דוגמאות: נתונים סטטיסטיים שמאוחסנים בענן לצורך ביצוע ניתוחים שונים או לצרכי שיווק ואין כל נתונים שיש בהם כדי לחשוף את הבעלים של נתונים אלו. יישום אתר שיווקי בענן אינו מחייב היתר, רק אם אין בו מידע רגיש או מידע שיש בו כדי לפגוע בתאגיד הבנקאי או לתקוף אותו.

19. ההוראה מדגישה שגם במקרים בהם התאגיד הבנקאי אינו נדרש להיתר, עליו לבצע הערכת סיכונים בנוגע לכל ההיבטים הרלוונטיים (למשל, כל סוגי הסיכונים הרלוונטיים- סיכונים משפטיים, סיכוני ציות, סיכוני סייבר, סיכוני המשכיות עסקית וכד') ועל בסיס מתמשך. בהערכת הסיכונים כל הגורמים הרלוונטיים בתאגיד צריכים להיות מעורבים.

20. בהמשך מפרטת ההוראה רשימת הנחיות בהן נדרש תאגיד בנקאי לעמוד כאשר יישום מחשוב ענן מחייב היתר. עמידה בהנחיות אלו נדרשת כתנאי מקדים ליישום.

ניהול סיכונים (סעיפים 18 – 22 להוראה)

21. התאגיד הבנקאי נדרש לבצע בדיקת Due Diligence, לא רק לפני התקשרותו עם ספק מחשוב הענן, אלא באופן תקופתי במהלך תקופת ההתקשרות. הבדיקה נועדה, בין היתר, לוודא את חוסנו הכלכלי של הספק, לבדוק את המקצוענות שלו בנושא ואת ניסיונו ביישום מחשוב ענן ומתן שירותים דומים לגופים אחרים. קיים קושי, במיוחד ביישומי ענן מסויימים כדוגמת SaaS, לעבור לספק שירותי ענן אחר תוך פרק זמן סביר (לעתים מעבר כזה עלול להיות בלתי

אפשרי), במקרה של סיום או הפסקת ההתקשרות עם הספק הנוכחי (מכל סיבה שהיא). מכאן חשיבותה של הנחיה זו.

22. ההוראה שמה דגש על הצורך לבצע הערכת סיכונים לכל יישום ענן (כאמור, גם אם לא נדרש היתר). הערכת הסיכונים צריכה להיות על בסיס מתמשך, תוך התייחסות לשינויים רלוונטיים – לא רק טכנולוגיים ועסקיים- גם בתאגיד הבנקאי וגם אצל ספק שירותי הענן. ההוראה מדגישה את הצורך להתייחס, בנוסף לסיכוני מיקור חוץ מסורתיים, גם לסיכונים המאפיינים מחשוב ענן ונותנת דוגמאות לסיכונים אלו בנספח להוראה, כגון: סיכון רגולטורי, סיכונים הנוגעים לטיפול באירועים חריגים, וכד'.

23. ההוראה מדגישה שאין להסתפק בניטור שמבצע ספק שירותי הענן ובכל מקרה על התאגיד הבנקאי לנטר אירועי סייבר ואבטחת מידע בעצמו. לדוגמא: באמצעות העברת מידע על אירועים למערכת הניטור המרכזית שלו.

24. אין להסתפק בווידוא שספק שירותי הענן מגן על המידע הרגיש של התאגיד הבנקאי המאוחסן אצלו; אלא, התאגיד הבנקאי נדרש גם לוודא שיושמו אמצעי הגנת נאותים שימנעו, ככל שניתן, תקיפה של התאגיד באמצעות הממשקים המקשרים בינו לבין הספק.

25. התאגיד הבנקאי נדרש להצפין את המידע המועבר בתקשורת ואת המידע המאוחסן בחצרי ספק שירותי הענן. עם זאת נוכח ההשפעה שעלולה להיות על הצפנת כל המידע על עיבודי היישום (לדוגמא: אחזור נתונים), ההוראה מאפשרת להצפין רק את הנתונים שהתאגיד סיווג כרגישים, שחשיפתם עלולה לפגוע בו ובלקוחותיו.

26. ההוראה מאפשרת שמירת מפתחות ההצפנה בחצרי ספק שירותי הענן. עם זאת, נוכח העובדה שאחסון מפתחות הצפנה אצל התאגיד הבנקאי מהווה בקרה חזקה בהגנה על המידע המאוחסן אצל הספק, הציפיה היא שהתאגיד יאחסן את מפתחות ההצפנה בחצריו, ככל שניתן, אא"כ הבחינה שערך מעלה קשיים, למשל: בהטמעת היישום. במקרה זה התאגיד הבנקאי יצטרך להטמיע בקרות מפצות.

הסכם התקשרות עם ספק שירותי הענן (סעיפים 23 – 24 להוראה)

27. בהסכם ההתקשרות עם ספק שירותי הענן, התאגיד הבנקאי צריך לוודא שהוא כולל אפשרות להפסיק את השירות באופן חד צדדי. ההוראה דורשת לעגן את התחייבות הספק לאפשר לתאגיד הבנקאי להתנתק מההסכם בכל עת ובכל מקרה שיחליט, כגון: חוסר שביעות רצון מהשירות, העברת השירות לספק אחר, הפסקת הצורך בשימוש שירות, וכד'.

28. ההנחיה נועדה למנוע מצב שבו נתוני התאגיד הבנקאי (לא רק הנתונים הרגישים) ימשיכו להיות מאוחסנים בחצרי הספק לאחר הפסקת ההתקשרות עמו. לפיכך, בכל מקרה של הפסקת השימוש בשירות, הספק נדרש להתחייב בהסכם להעביר אל התאגיד הבנקאי את נתוני התאגיד המאוחסנים אצלו ולמחוק נתונים אלו משרתי הספק, כך שלא יתאפשר שחזורם ואחזורם בכל דרך שהיא אצל הספק. ההוראה מציינת שפעולות אלו יבוצעו תוך "זמן קצר" – מומלץ שהתאגיד הבנקאי יגדיר זמן זה בהסכם.

29. במקרה שהתאגיד הבנקאי מחליף ספק שירותי ענן או שחל שינוי בבעלות של הספק הנוכחי, התאגיד הבנקאי נדרש לוודא שההסכם החדש או ההסכם הקיים מעגן את כל ההתחייבויות של הספק לרבות אלו שבהוראה.

מכתב ההיתר (סעיפים 25 – 26 להוראה)

30. מכתב ההיתר כולל בד"כ דרישות נוספות לדרישות המפורטות בהוראה זו. הדרישות הנוספות, שבהן נדרש התאגיד לעמוד לפני הפעלת השירות, ספציפיות ורלוונטיות לשירות הענן שעבורו פנה התאגיד הבנקאי בבקשת היתר.

31. קיימות ארבע דרישות שפורטו כדרישות גורפות במכתב המפקח מ-29.06.2015, והן אינן מפורטות יותר כדרישות מחייבות בהוראה. עם זאת, הצורך בהגדרת דרישות אלו ייבחן במסגרת בקשת ההיתר של התאגיד הבנקאי, לגופו של עניין; אם הפיקוח יחליט שהדרישה רלוונטית לשימוש בענן שהתאגיד הבנקאי מבקש ליישם, תיכלל הדרישה במכתב ההיתר. ההוראה מפרטת את ארבעת הנושאים בנוגע לדרישות כאמור.

תחילה

32. תחילת האמור בחוזר זה היא מיידית.

עדכון הקובץ

33. מצ״ב דפי עדכון לקובץ ניהול בנקאי תקין. להלן הוראות העדכון

להוציא עמוד	**להכניס עמוד**

בכבוד רב,

ד״ר חדוה בר
המפקחת על הבנקים

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, 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. הוראה זו מעדכנת את התנאים הנדרשים לשימוש של תאגיד בנקאי בטכנולוגיות ענן (התנאים הוגדרו במכתב המפקח על הבנקים בנושא "ניהול סיכונים בסביבת מחשוב ענן" מיום 29.06.2015), תוך קביעת המקרים בהם נדרש היתר מראש מהפיקוח על הבנקים והמקרים בהם התאגיד הבנקאי רשאי לעשות שימוש בשירותי מחשוב ענן ללא קבלת היתר כאמור.

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) (3א) ו-(3ב);
   3) תאגיד בנקאי כאמור בסעיף 11 (ב);
   4) סולק כהגדרתו בסעף 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 ו-367.
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 להסתייע, לפי העניין, ביועצים חיצוניים מומחים בהפחתת הסיכונים הגלומים בשימוש בטכנולוגיות ענן.

פרק ג': ממשל תאגידי

דירקטוריון והנהלה בכירה

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 והבקרות 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, לפי העניין, את ההנהלה לגבש ולאשר מסמך מדיניות לשימוש בטכנולוגיות מחשוב ענן.

11. בהמשך לאמור בסעיף 10 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 בתאגיד הבנקאי לטיפול בהיבטים משפטיים, תחזוקה, ניטור, אבטחת מידע וכד'. המדיניות תיתן מענה, בין היתר, גם לנדרש בהוראה זו.
12. לפני יישום מחשוב ענן המחייב היתר (ראה סעיף 14 להלן), יערך דיון בהנהלה או בוועדת הנהלה רלוונטית, ולפי העניין, גם בדירקטוריון.
13. על הנהלת התאגיד הבנקאי לוודא שהשימוש בטכנולוגיות מחשוב ענן יהיה ע"פ המדיניות שנקבעה כאמור.

פרק ד': יישומי מחשוב ענן המחייבים קבלת היתר

14. בנוסף לאמור בסעיף 7 לעיל, לפני שימוש בטכנולוגיות מחשוב ענן במסגרתו מאוחסן ו/או מועבר ו/או מעובד מידע (להלן: "יישום מחשוב ענן") באמצעות התקשרות עם ספק שירותי מחשוב ענן (להלן: "ספק שירותי הענן" או "הספק"), נדרש התאגיד הבנקאי לקבל היתר בכתב מהמפקח על הבנקים, בהתקיים לפחות אחד מהתנאים הבאים:

(א) יישום מחשוב הענן כולל מידע המוגדר על ידי התאגיד הבנקאי כמידע רגיש.

(ב) המידע אינו מוגדר ע"י התאגיד הבנקאי כמידע רגיש, אך כתוצאה מחשיפתו, ניתן להסיק פרטים שיאפשרו לתקוף או לפגוע בתאגיד הבנקאי ו/או בלקוחותיו.

(ג) שיבוש או הפסקת הפעילות של יישום מחשוב הענן, עלולים לפגוע בהתנהלות התאגיד הבנקאי ו/או ביכולתו לתת שירות ומענה ללקוחותיו.

(ד) יישום מחשוב הענן מספק אמצעי הגנת הסייבר ואבטחת מידע כרובד הגנה יחיד, ושלא קיימים אמצעים דומים מסוגיהם גם בחצרי התאגיד הבנקאי.

15. תאגיד בנקאי אינו נדרש לקבל היתר מהפיקוח על הבנקים במקרים בהם לא מתקיים אף אחד מהתנאים המפורטים בסעיף 14 לעיל. לדוגמא: יישום מחשוב ענן לניתוח מידע ללא זיהוי הבעלים של המידע, אתר שיווקי ללא אחסון מידע רגיש, וכד'.

16. לפני יישום מחשוב ענן שאינו מחייב קבלת היתר, כאמור בסעיף 15 לעיל, נדרש התאגיד הבנקאי לבצע תהליכי מיפוי והערכת סיכונים נאותים ומתמשכים, במעורבות כלל הגורמים הרלוונטיים בתאגיד הבנקאי, ובהתייחס לכלל ההיבטים הרלוונטיים, כמפורט בסעיף 19 להלן.

17. לפני יישום מחשוב ענן המחייב היתר כאמור בסעיף 14 לעיל, על התאגיד הבנקאי לעמוד בדרישות המופיעות בהמשך מכתב זה (סעיפים 18 עד 26 להלן).

פרק ה': ניהול סיכונים

18. 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 מחשוב ענן. 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.

20. על התאגיד הבנקאי לוודא שביכולתו לבצע ניטור אירועי אבטחת מידע הקשורים ליישום מחשוב ענן ולשימושו 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. 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 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. 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, 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.

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

25. הפיקוח על הבנקים יבחן את הצורך להגדיר במכתב ההיתר דרישות נוספות כתנאי לקבלת ההיתר, ובין היתר, בנוגע לנושאים הבאים:

(א) מקום אחסון מפתחות ההצפנה.

(ב) מסירה לתאגיד הבנקאי דוחות ביקורת פנימיים של הספק ודוחות ביקורת חיצוניים שנערכו על פעילותו.

(ג) אפשרות לתאגיד הבנקאי לדרוש במקרים מיוחדים מהספק לערוך עבורו ביקורת בנושא מסוים.

(ד) מתן אפשרות לפיקוח על הבנקים לבצע ביקורות אצל ספק שירותי ענן.

26. לצורך קבלת היתר, על התאגיד הבנקאי לפנות לפיקוח על הבנקים לפחות 60 ימים לפני הפעלת השירות.

עדכונים

חוזר XX **מס'**	**גרסה**	**פרטים**	**תאריך**
XXXX	1	חוזר מקורי	29/06/2017

נספח א' - 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.