יד' סיון, תשפ"ב
13 יוני, 2022
חוזר מס ח- 06 - 2715

לכבוד
התאגידים הבנקאיים

הנדון: מחשוב ענן
(ניהול בנקאי תקין הוראה מס' 362)

מבוא

1. שירותי מחשוב הענן מקדמים ומעצימים את יכולות המחשוב הארגוניות ומאפשרים לארגונים ובכללם התאגידים הבנקאיים להתייעל ולהגיב במהירות לצרכי השוק. טכנולוגיית מחשוב הענן עוברת התפתחות מואצת אך בד בבד עדיין בעלת סיכונים הייחודיים לה ומשום כך עלולה לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מוגברים, ובכלל זה סיכוני אבטחת מידע וסייבר, המשכיות עסקית וכן פגיעה במוניטין. הוראה זו באה להנחות בין השאר בניהול סיכונים אלה.
2. הפיקוח על הבנקים רואה את השימוש בשירותי מחשוב ענן כמקרה פרטי של מיקור חוץ, ועל כן על תאגיד בנקאי העושה שימוש בשירותי מחשוב ענן יחולו לבד מהנחיות הוראה זו, גם כל הנחיות הוראת ניהול בנקאי תקין מס' 359A בנושא "מיקור חוץ" (להלן: הוראה 359A). זאת, למעט נושאים מסוימים (ראה פירוט נוסף בנספח א' – " תחולת הוראות 362 ו- 359A על מחשוב ענן מהותי ושאינו מהותי").
בהתאם לאמור לעיל, נעשה שימוש בשיקולים המפורטים בסעיף 27 להוראה 359A והמשמשים שם להגדרת רמת המהותיות של מיקור החוץ, תוך הוספת שיקולים נוספים למהותיות המפורטים בהגדרת "מחשוב ענן מהותי" המופיעה בהוראה זו. כמו כן הותאמה הטרמינולוגיה בהוראה לזו של הוראה 359A, כך שהמילה "ספק" הוחלפה ב"נותן שירות" ו"הסכם התקשרות" הוחלף במילה "חוזה".
3. התאגידים הבנקאיים יחויבו בקביעת מדיניות לשימוש בשירותי מחשוב ענן, במסגרתה, בין השאר, קביעת מאפייני השירותים המוגדרים כ"מחשוב ענן מהותי" בכפוף לשיקולים כאמור וניהול הסיכונים לשימוש בשירותי מחשוב ענן בכלל. כפועל יוצא מכך בוטל השימוש במונח "מערכות ליבה" ובוטל האיסור לתאגידים הבנקאיים לשימוש במערכת ליבה במחשוב ענן. התאגיד הבנקאי יעגן את המדיניות במסמך "מדיניות לשימוש בשירותי מחשוב ענן" אשר יובא לאישור הדירקטוריון.

4. כאמור, מחשוב ענן הוא מקרה פרטי של מיקור חוץ, אולם לשימוש בשירותי מחשוב ענן קיימות דרישות ייחודיות שאינן אופייניות לכל מיקור חוץ ואשר אינן מפורטות בהוראה 359A. הוראה זו מפרטת את הדרישות הייחודיות לשימוש בשירותי מחשוב ענן במגוון הנושאים, לרבות ממשל תאגידי, ניהול סיכונים, התקשרות עם נותן שירותי מחשוב הענן, אבטחת מידע והגנת הסייבר והמשכיות עסקית.
5. מהלך זה מצטרף לשאר הצעדים שנקט הפיקוח על הבנקים בשנים האחרונות להתאמת הבנקאות בישראל לעולם התחרותי המשתנה ולקדמה הטכנולוגית.
6. לאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגיד, החלטתי על עדכון הוראת ניהול בנקאי תקין מס' 362 בנושא "מחשוב ענן".

<u>התיקונים להוראה 362</u>

<u>פרק א' – רקע</u>

תחולה

7. **סעיף 5**

הובהר כי הוראה זו אינה חלה על "ענן פרטי" כהגדרתו בסעיף 6 להוראה זו, אולם על מיקור חוץ בענן פרטי חלה הוראת ניהול בנקאי מס' 359A בנושא "מיקור חוץ".

<u>פרק ב' – כללי</u>

הגדרות

8. **סעיף 6**

8.1. הוגדרו "מחשוב ענן", "ענן פרטי" ו"מחשוב ענן מהותי".

8.2. התוספה הגדרה ל"מחשוב ענן": ההגדרה מבוססת על הגדרות ה- EBA[1] וה- NIST[2] (The NIST Definition of Cloud Computing).

8.3. התוספה הגדרה ל"ענן פרטי": ההגדרה מבוססת על הגדרת ה- NIST. ניתן לרוב לאפיין ענן פרטי כתשתית מחשוב ענן המופעלת לשימושו הבלעדי של תאגיד בנקאי אחד. התשתית יכולה להיות מופעלת על ידי הארגון עצמו או על ידי ספק חיצוני, ויכולה להיות ממוקמת בחצרות התאגיד הבנקאי או מחוצה להם (לדוגמה מרכז מחשוב של הבנקים המסורתיים הממוקם במבנה הבנק או במבנה אחר במיקור חוץ).

8.4. התוספה הגדרה ל"מחשוב ענן מהותי": הגדרה זו נסמכת על הגדרת "מיקור חוץ" בהוראה 359A, כאשר לשיקולים לקביעת מהותיות פעילות מחשוב הענן המפורטים בסעיף 27 להוראה 359A נוספו שיקולים לגבי סוג הענן (ציבורי, קהילתי, היברידי וכד') וסוג שירות מחשוב הענן (IaaS, PaaS, SaaS וכד').

כמו כן, נוספו להגדרה מספר שיקולים, אשר הופיעו בנספח א' להוראה בגרסה הקיימת בחוזר 2669 כדוגמאות למחשוב ענן מהותי.

---

[1] European Banking Authority - EBA

[2] The National Institute of Standards and Technology - NIST

הוראות כלליות

9. בוטל האיסור לשימוש בשירותי מחשוב ענן עבור פעילויות ליבה ו/או מערכות ליבה.

10. **סעיף 7**

הסעיף עודכן בהתאם לרגולציה האירופאית התקפה: רגולציית הגנת המידע של האיחוד האירופי (GDPR - General Data Protection Regulation).

11. **סעיף 8**

11.1. סעיף זה קובע את הכלל לפיו מחשוב ענן הוא מקרה פרטי של מיקור חוץ. בהתאם לכך ככל שמדובר במחשוב ענן מהותי כהגדרתו בהוראה זו, תחול עליו הוראה 359A. חריג מכלל זה: סעיף 33 להוראה 359A בנושא "חובות דיווח למפקח על הבנקים" אשר לא יחול על מחשוב ענן בין אם מהותי ובין אם שאינו מהותי.

11.2. יודגש כי בהחלטה האם מדובר במחשוב ענן מהותי נדרש התאגיד הבנקאי להתחשב בנוסף לשיקולים המפורטים בסעיף 27 להוראה 359A, גם בהיבטים נוספים הייחודים למחשוב ענן והמופיעים בהגדרת "מחשוב ענן מהותי" בהוראה זו (ראה סעיף 8.4 בחוזר זה).

11.3. בוטל האזכור לצורך בעמידת שירותי מחשוב ענן בהוראות הנב"ת הספציפיות המפורטות בסעיף. אין בביטול אזכור הוראות אלו, בכדי לגרוע מחובת התאגיד הבנקאי לעמוד בהן, כמו גם בכל הוראת נב"ת רלבנטית אחרת, בהקשר של מחשוב ענן.

12. **סעיף 9**

הנחיית רשם מאגרי מידע מס' 2/2011 – "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" קובעת את היקף תחולתה על גופים המפוקחים על ידי המפקח על הבנקים, ולכן בוטל אזכור הנחייה זו בהוראה.

13. **סעיף 10**

13.1. האפשרות להיוועצות עם מומחים לעניין הפחתת הסיכונים בנושא מחשוב ענן אינה ייחודית לנושא זה, והיא בוטלה על מנת למנוע מהתאגידים הבנקאיים להסיק כי היוועצות כאמור אינה אפשרית במקרים בהם לא נאמר הדבר במפורש בהוראה זו.

13.2. נוספה דרישה כי על התאגיד הבנקאי לוודא כי נותן שירות מחשוב הענן יישא באחריות כלפי התאגיד הבנקאי, לרבות קיום החובות הכלולות בחוזה ההתקשרות בין נותן שירות מחשוב הענן לתאגיד הבנקאי, גם במקרה בו נותן שירות מחשוב הענן עושה שימוש בנותן שירות משני.

<u>פרק ג' – ממשל תאגידי</u>

14. **סעיף 11**

כאמור בסעיף 11 בחוזר זה, סעיף זה מהווה החרגה לכלל שנקבע בסעיף 8 להוראה זו לפיו הוראה 359A תחול רק במקרה של מחשוב ענן מהותי. הסעיף קובע כי הנחיות הוראה 359A הרלבנטיות לעניין ממשל תאגידי (הנחיות אלו מפורטות בפרק ב' להוראה 359A) יחולו גם במקרה של מחשוב ענן שאינו מהותי, זאת, למעט סעיף 13(ג) וסעיף 16.

דירקטוריון

15. **סעיפים 14-12**

כאמור בסעיף 11 בחוזר זה, מחשוב ענן הינו מקרה פרטי של מיקור חוץ אשר לו מאפיינים ייחודיים. לפיכך, נוספו חובות ייחודיות לדירקטוריון בהקשר של שימוש בשירותי מחשוב ענן המפורטים בסעיף זה, ואשר אינם מופיעים בהוראה 359A.

הנהלה בכירה

16. **סעיף 15**

כאמור בסעיף 11 בחוזר זה, מחשוב ענן הינו מקרה פרטי של מיקור חוץ אשר לו מאפיינים ייחודיים. סעיף זה מפרט את חובות ההנהלה הבכירה הייחודיים בהקשר של שימוש בשירותי מחשוב ענן, ואשר אינם מופיעים בהוראה 359A.

המדיניות שתגובש על ידי ההנהלה הבכירה ותאושר על ידי הדירקטוריון תבחין בין שימוש בשירותי מחשוב ענן מהותי הדורש את אישור הדירקטוריון לבין שימוש בשירותי מחשוב ענן הדורש את אישור ההנהלה הבכירה לבין שימוש בשירותי מחשוב ענן הדורש אישור גורם אחר. המדיניות תעלה בקנה אחד עם הדרישות הרגולטוריות השונות, לרבות ביחס לטכנולוגיית מידע ותקשורת, אבטחת מידע והגנת הסייבר, המשכיות עסקית וניהול סיכונים תפעולי.

17. **סעיף 16**

נוספו נושאים ייחודיים לשימוש בשירותי מחשוב ענן אשר המדיניות שיקבע התאגיד הבנקאי נדרשת להתייחס אליהם.

18. **סעיף 17**

ההנהלה הבכירה תעקוב באופן שוטף אחר יישום מדיניות מסמך "מדיניות לשימוש בשירותי מחשוב ענן", כפי שאושר על ידי הדירקטוריון.

19. **סעיפים 19-18**

19.1. למחשוב ענן מאפיינים ייחודיים וכאמור בסעיף 1 בחוזר זה, יישומו 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.

19.2. במסגרת הקו הראשון יוגדר גורם הכפוף למנהל טכנולוגיית המידע אשר יכיר באופן מעמיק את הסיכונים הכרוכים בשימוש בשירותי מחשוב ענן, וכן את השירותים הטכנולוגיים הניתנים על ידי כל נותני שירותי מחשוב הענן עמם התקשר התאגיד

הבנקאי. בנוסף ישקול התאגיד הבנקאי בהתאם לנסיבות העניין, הגדרת גורם אחראי לכל נותן שירותי מחשוב ענן שעמו התקשר.

19.3. במסגרת הקו השני יוגדר גורם הכפוף למנהל הסיכונים אשר יהיה אחראי על הערכה שוטפת ומעמיקה של סיכוני כלל הפעילות במחשוב ענן בראיה רחבה של כלל שירותי מחשוב הענן שמקבל התאגיד הבנקאי.

20. **סעיף 20**

על ההנהלה הבכירה להכין תכנית עבודה רב שנתית למחשוב ענן. התכנית תכלול בין היתר את הסיכונים הגלומים בשירותי מחשוב ענן והבקרות המיושמות או המתוכננות להפחתתם.

<u>פרק ה' – ניהול סיכונים</u>

21. **סעיף 21**

21.1. הסעיף (סעיף 17 (א) בגרסה הקיימת בחוזר 2669) הועבר במהותו לסעיף 23 להוראה זו.

21.2. סעיף זה מהווה החרגה לכלל שנקבע בסעיף 8 להוראה זו לפיו הוראה 359A תחול רק במקרה של מחשוב ענן מהותי. הסעיף קובע כי הנחיות הוראה 359A הרלבנטיות לעניין ניהול סיכונים (סעיפים 26-24 להוראה 359A) יחולו גם במקרה של מחשוב ענן שאינו מחשוב ענן מהותי.

22. **סעיף 22**

הסעיף (סעיף 18 בגרסה הקיימת בחוזר 2669) הועבר במהותו לפרק ו': התקשרות עם נותן שירותי מחשוב הענן. נושא בדיקת הנאותות נכלל בסעיף 29 להוראה זו.

23. **סעיף 23**

נוספו:

23.1. (א) הפניה להיבטים עיקריים שיש לקחת בחשבון בהערכת סיכונים המובאים בנספח ב' להוראה זו – "היבטים עיקריים להערכת סיכונים במחשוב ענן".

23.2. (ב) חובת ביצוע סקר סיכונים למחשוב ענן מהותי, כאמור בהוראת ניהול בנקאי תקין מס' 350 בנושא "ניהול סיכונים תפעוליים", תהיה לכל הפחות אחת לשנתיים.

23.3. (ג) חובת ווידוא קיום בקרות מפצות מתאימות בהתאם להערכת הסיכונים.

24. **סעיף 24**

24.1. הסעיף (סעיף 20 בגרסה הקיימת בחוזר 2669) הועבר לפרק ז'1: אבטחת מידע וסייבר.

24.2. נוספה חובת הכללת התייחסות פרטנית לסיכוני מחשוב ענן בדוחות הסדירים המוגשים להנהלה הבכירה ולדירקטוריון בנושאי סיכונים תפעוליים כנדרש בהוראת ניהול בנקאי תקין מס' 350.

25. **סעיף 25**

25.1. הסעיף (סעיף 21 בגרסה הקיימת בחוזר 2669) הועבר לפרק ז'1': אבטחת מידע וסייבר.

25.2. נוספו חובת הגדרת תחומי אחריות לניהול, שליטה, אישור ותיעוד של שירותי מחשוב הענן בתאגיד הבנקאי וחובת הגדרת מודל חלוקת אחריות בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן. יחד עם זאת, יש להדגיש כי על התאגיד הבנקאי לעמוד במכלול הדינים וההוראות החלים עליו והתאגיד הבנקאי הוא האחראי הבלעדי כלפי לקוחותיו וכלפי הפיקוח על הבנקים.

26. **סעיפים 26-27**

26.1. הסעיף (סעיף 22 בגרסה הקיימת בחוזר 2669) הועבר לפרק ז'1: אבטחת מידע וסייבר.

26.2. נוספה חובת תיעוד היבטי שרותי מחשוב הענן המפורטים בהוראה זו ועדכונם.

<u>פרק ו' - התקשרות עם נותן שירותי מחשוב הענן</u>

27. **סעיף 28**

למען הסר ספק, במחשוב ענן שאינו מחשוב ענן מהותי לא יחול על התאגיד הבנקאי פרק ו' להוראה זו: "התקשרות עם נותן שירותי מחשוב הענן".

<u>בדיקת נאותות</u>

28. **סעיף 29**

28.1. הסעיף מפרט היבטים נוספים שיש לכלול במסגרת בדיקת הנאותות שיש לקיים לנותן שירות מחשוב ענן מהותי בטרם התקשרות עימו, בנוסף לאלו המפורטים בהוראה 359A.

(א) עמידה של נותן שירותי מחשוב הענן בכל דין ורגולציה הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, לרבות דיני הגנת הפרטיות החלים באותה המדינה בה הוא פועל.

(ב) התאגיד הבנקאי יוודא עמידה ברמת הגנת סייבר נאותה בהתאם לקריטריונים שיוגדרו על ידו. לדוגמא: דיווחים ודו"חות של נותן שירותי מחשוב הענן ומידע מודיעיני בנוגע לאירועים שהתרחשו אצל נותן שירותי מחשוב הענן, ועוד.

28.2. הנושאים המפורטים בסעיף זה מהווים רשימה בסיסית בבדיקת הנאותות, אולם יובהר כי לא מדובר ברשימה סגורה.

<u>חוזה מחשוב ענן</u>

29. **סעיף 30**

29.1. (א) מאחר וכאמור בסעיף 8 להוראה זו, על מחשוב ענן מהותי יחולו סעיפי הוראה 359A ומאחר וההנחיות המפורטות בסעיף זה מופיעות בסעיף 23 (ח) בהוראה 359A, הסעיף בכללותו בוטל, אולם הושם דגש על מחיקה של המידע של התאגיד הבנקאי, או פעולה דומה, ממערכות נותן שירותי מחשוב הענן והתחייבותו כי לא ניתן יהיה לאחזר מידע זה במערכותיו.

29.2. (ב) מאחר וכאמור בסעיף 8 להוראה זו, על מחשוב ענן מהותי יחולו סעיפי הוראה 359A ומאחר וההנחיות המפורטות בסעיף זה מופיעות בסעיף 23 (ו) בהוראה 359A, הסעיף בוטל.

29.3. (ג) מאחר וכאמור בסעיף 8 להוראה זו, על מחשוב ענן מהותי יחולו סעיפי הוראה 359A ומאחר וההנחיות המפורטות בסעיף זה מופיעות בסעיף 23 (ו) בהוראה 359A, הסעיף בוטל.

29.4. (ד) הסעיף נמחק ובמקומו נוספה דרישה להבטחת 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.

29.5. כמו-כן נציין כי סעיף 22 בהוראת ניהול בנקאי 359A בנושא הבטחת יכולת המפקח על הבנקים להפעיל את סמכויותיו חל על מחשוב ענן מהותי.

29.6. (ה) יש לעגן בחוזה את התחייבויותיו של נותן שירות מחשוב הענן במסגרת המודל שנקבע לעניין חלוקת האחריות של התאגיד הבנקאי כנדרש בסעיף 25 להוראה זו.

29.7. (ו) יש לציין בחוזה את מיקום מתקן הענן ממנו יינתן השירות ומיקום אחסון הנתונים, לרבות התחייבות נותן שירות מחשוב הענן להודיע לתאגיד הבנקאי על כל שינוי באמור.

29.8. (ז) החוזה יכלול התייחסות לאופן אחסון המידע הרגיש והנגישות אליו תוך כדי תקופת השירות ולאחריה.

29.9. (ח) החוזה יכלול התייחסות לגיבוי המידע והאפשרות לאחזורו.

29.10. (ט) יש להגדיר בחוזה את יכולת התאגיד הבנקאי להפעיל או להפסיק שירותי מחשוב ענן מהותיים או רכיבים מתוך שירותים אלה לרבות חסימות גישה, ככל שרלוונטי ובעת חירום כדוגמת אירוע סייבר, מתוך הצורך לצמצם סיכונים. זאת, בין באופן עצמאי ובין על ידי ספק שירות מחשוב הענן בהתאם לבקשת התאגיד הבנקאי. 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.

29.11. (י) יש לבחון שילוב בחוזה התחייבות של נותן שירות מחשוב הענן להשתתפות בתרגילי סייבר שיקיים מולו התאגיד הבנקאי אחת לתקופה, בהתאם לאופי היישום.

29.12. (יא) החוזה יכלול התייחסות ליישום בקרות מפצות בהתאם להערכת הסיכונים כמפורט בסעיף 23 להוראה זו.

29.13. הנושאים המפורטים בסעיף מהווים רשימה בסיסית בחוזה מול נותן שירות מחשוב ענן, אולם יובהר כי לא מדובר ברשימה סגורה.

ניהול ההתקשרות עם נותן שירותי מחשוב ענן מהותי

30. **סעיף 31**

30.1. הסעיף הורחב ומפרט את הפעולות אותן נדרש התאגיד הבנקאי לבצע במהלך תקופת ההתקשרות עם נותן שירותי מחשוב ענן מהותי (סעיפים קטנים (א) – (ה)).

30.2. נוספה דרישה בסעיף קטן (ו) כי התאגיד הבנקאי יבחן את הצורך בעדכון החוזה מול 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.

30.3. תוכן הסעיף (סעיף 24 בגרסה הקיימת בחוזר 2669) העוסק בשינוי בעלות על נותן שירותי מחשוב ענן נכלל בסעיף קטן (ז). המונח בעלות שונה ל"בעל שליטה" על מנת להחיל גם במקרה של חברה ציבורית.

<u>פרק ז'1: אבטחת מידע והגנת הסייבר</u>

31. למען הסר ספק, פרק אבטחת מידע והגנת הסייבר חל על כל מחשוב ענן בין אם מהותי ובין אם אינו מהותי.

32. **סעיפים 33-32**

סעיפים אלה הועברו מסעיף 22 בגרסה הקיימת בחוזר 2669, ועודכנו בהיבטי הדרישה מהתאגיד הבנקאי לנהל את סיכון חשיפת המידע, תוך התייחסות בין היתר להיבטים של סיווג המידע, מיקום מפתחות ההצפנה, מעורבות התאגיד הבנקאי בניהול מפתחות ההצפנה ורמת ההצפנה, שיטת ההצפנה ועוד.

33. **סעיף 34**

סעיף זה הועבר מסעיף 20 בגרסה הקיימת בחוזר 2669. דגשים ייחודיים לניטור אירועי סייבר בעת שימוש בשירות מחשוב ענן ניתן למצוא בנספח ג' להוראה זו - "ניטור אירועי סייבר במחשוב ענן". הניטור צריך להתבצע באופן שיאפשר לזהות אירוע סייבר מוקדם ככל הניתן ובאופן הרלוונטי לסוג שירות מחשוב הענן (IaaS, PaaS, SaaS וכד').

34. **סעיף 35**

התווסף סעיף העוסק בהתמודדות עם אירועי סייבר בשירותי מחשוב ענן, לרבות קיום תרגילי סייבר המכיל דגשים ייחודיים לצורך היערכות התאגיד הבנקאי לאירועי סייבר בשירותי מחשוב ענן.

35. **סעיף 36**

סעיף זה הועבר מסעיף 21 בגרסה הקיימת בחוזר 2669.

<u>פרק ז'2 - המשכיות עסקית</u>

36. **סעיף 37**

ככל שמחשוב הענן מהווה שירות חיוני לתאגיד הבנקאי יחולו עליו הדרישות הרלוונטיות בהוראת ניהול בנקאי תקין מס' 355.

37. **סעיף 38**

ככל שמחשוב הענן הינו מחוץ לישראל, על התאגיד הבנקאי לבחון תכניות מענה לתרחיש של אי זמינות השירות כתוצאה מנתק תקשורתי לחו"ל או מאירועים גיאופוליטיים מול המדינה הזרה. זאת ועוד, התאגיד יעריך את יכולת ההמשכיות העסקית של הספק מול איומי הייחוס המקומיים של המדינה המארחת.

38. **סעיף 39**

באתר מחשוב בענן ראשי או חלופי - התאגיד הבנקאי נדרש לוודא עמידתו של האתר בדרישות Tier3 בהתאם לסטנדרטים שנקבעו בתקן (UpTime Institute (UTI, על ידי קבלת תעודה מ-UTI או על ידי חוות דעת חיצונית מגורם מומחה בלתי תלוי.

<u>פרק ח' – דיווח לפיקוח</u>

39. **סעיף 40**

39.1. אחת לשנה בגין סיום שנה קלנדרית, על תאגיד בנקאי להעביר דיווח בכתב לידי הפיקוח על הבנקים. הדיווח יתבצע על פי הוראת דיווח לפיקוח מס' 881 בנושא "דיווח על מחשוב ענן (שנתי)". יובהר כי בכל מקרה יחול רצף דיווחים בין חובת הדיווח על פי חוזר 2669 לבין חובת הדיווח בחוזר זה.

39.2. יודגש כי כאמור בסעיף 8 להוראה זו, על מחשוב ענן מהותי לא יחול סעיף 33 להוראה 359A והתאגיד הבנקאי לא נדרש להודיע מראש למפקח על הבנקים על יישום של מחשוב ענן מהותי, תוך מתן הנמקה להוצאת הפעילות למחשוב ענן, סמוך ככל הניתן לקבלת החלטה על כך בדרג הנהלה בכירה.

<u>נספח א' – דוגמאות למחשוב ענן מהותי</u>

40. הנספח בוטל היות ודוגמאות הנספח הועברו כשיקולים נוספים לבחינה תחת הגדרת "מחשוב ענן מהותי" - ראה סעיף 8 בחוזר זה: הגדרות.

נספח ב' - היבטים עיקריים להערכת סיכונים במחשוב ענן

41. הנספח כולל היבטים עיקריים לצורך הערכת סיכונים במחשוב ענן. להלן השינויים העיקריים שבוצעו בנספח:

41.1. נמחקו היבטים שמופיעים בהוראה 359A.

41.2. נמחק סיכון סיסטמי.

41.3. (ב) נוספה התייחסות להיבטי סיכון הנובעים משימוש או מאי שימוש בתצורת ענן מרובה (תשתיות ענן המבוססות על שילוב של מספר פתרונות שונים של מחשוב ענן), כגון: פיזור אצל מספר נותני שירות מחשוב ענן לרבות משמעויות מקצועיות כנגד ריכוזיות קבלת שירותי מחשוב ענן מנותן שירותי מחשוב אחד.

41.4. (ה) נוספה התייחסות להיבטי סיכון הכרוכים בקבלת שירות מחשוב ענן המספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד.

41.5. (ז) נוספה התייחסות להיבטי סיכון הכרוכים בשינויים הנדרשים מנותן שירותי מחשוב הענן כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים.

41.6. (יא) הורחבו ההיבטים הקשורים לסיכוני התפעול השוטף (כולל אנשי תמיכה, תהליכי עבודה, ניהול אירועים ועוד), והקטנתם בין היתר באמצעות הסדרת תחומי אחריות בין התאגיד הבנקאי לבין נותן שירותי המחשוב.

41.7. (יד) נוספה התייחסות לקיום הפרדה לוגית ומנהלתית בין המערכות של הלקוחות השונים בענן.

נספח ג' - ניטור אירועי סייבר במחשוב ענן

42. ניהול הניטור והגדרתו יהיו בהתאמה לסוגי השירות השונים (כדוגמת SaaS, PaaS ו- IaaS) כאשר לכל הפחות מצופה שהתאגיד הבנקאי ינהל ויגדיר חוקים, יקבל לוגים ויכיר את החוקים הקיימים ומהם יסיק על שילוב חוקים נוספים במערכות הניטור של הבנק.

הניטור יכלול בין היתר חריגות מפעילות לגיטימית בתשתיות הבנק הקשורות בשירות מחשוב הענן. כלי הניטור יעמדו בסטנדרטים מקובלים המאפשרים שילוב עם מערכות הניטור הקיימות של התאגיד הבנקאי. התאגיד הבנקאי יגדיר פעולות בקרה להמשך רציפות ניטור שירות מחשוב הענן המהותי בעת ניתוק תקשורת בין התאגיד הבנקאי לסביבת הענן.

<u>תחילה והוראות מעבר</u>

43. תחילת האמור בהוראה זו ביום 1.1.23.

44. לעניין חוזים שנכרתו לפני מועד פרסום הוראה זו – במועד החידוש הקרוב של החוזה ולא יאוחר מ- 4 שנים ממועד התחילה, יתאים התאגיד הבנקאי את החוזים להוראה זו ככל שהדבר נדרש.

45. לעניין חוזים שנכרתו לאחר מועד פרסום הוראה זו ועד למועד התחילה – לא יאוחר משנה ממועד התחילה, יתאים התאגיד הבנקאי את החוזים להוראה זו ככל שהדבר נדרש.

46. תאגיד בנקאי רשאי ליישם את הוראה זו בכללותה לפני מועד התחילה.

47. החל ממועד תחילת הוראה זו יבוטל סעיף 29 להוראת ניהול בנקאי תקין מס' 480 בנושא "התאמות להוראות ניהול בנקאי תקין החלות על תאגיד בנקאי חדש".

<u>טיפול בהיתרים קיימים</u>

48. החל ממועד תחילת הוראה זו, היתרים או אישורים שניתנו עבור שירות המוגדר כשירות מחשוב ענן בהוראה זו:

(א) כאשר האישור או ההיתר כולל תנאים או התניות שאינם מחויבים על פי הוראה זו, תנאים והתניות אלה בטלים.

(ב) כאשר האישור או ההיתר כולל תנאים או התניות שאינם עומדים בעקרונות ההוראה יש לנהוג לפי סעיף 44 לחוזר זה.

<u>עדכון הקובץ</u>

49. מצ"ב דפי עדכון לקובץ ניהול בנקאי תקין. להלן הוראות העדכון:

<u>להוציא עמוד</u>	**<u>להכניס עמוד</u>**
362-1-10 [3] (9/21)	362-1-15 [4] (6/22)

בכבוד רב,

יאיר אבידן

המפקח על הבנקים

נספח א' - תחולת הוראות 362 ו- 359A על מחשוב ענן מהותי ושאינו מהותי

362		
העקרון: הוראה 362 חלה על כל מחשוב הענן (מהותי ושאינו מהותי), אלא אם נכתב אחרת בהוראה.		
	מחשוב ענן שאינו מחשוב ענן מהותי	**מחשוב ענן מהותי**
פרק א' - רקע (מבוא + תחולה)	כן	כן
פרק ב' – כללי (הגדרות + הנחיות כלליות)	כן	
פרק ג' - ממשל תאגידי (דירקטוריון + הנהלה בכירה)	כן	
פרק ה' – ניהול סיכונים	כן	
פרק ו' - התקשרות עם נותן שירותי מחשוב ענן (בדיקת נאותות + חוזה מחשוב ענן + ניהול ההתקשרות עם נותן שירותי מחשוב ענן מהותי)	לא	
פרק ז'1 - אבטחת מידע והגנת הסייבר	כן	
פרק ז'2 - המשכיות עסקית	לא	
פרק ח' – דיווח לפיקוח	כן	
359A		
העקרון: הוראה 359A חלה על מחשוב ענן מהותי (למעט חובת הדיווח בסעיף 33). בפרקים מסוימים, כאשר מצוין זאת במפורש בהוראה 362, תחול הוראה 359A גם על מחשוב ענן שאינו מחשוב ענן מהותי.		
	מחשוב ענן שאינו מחשוב ענן מהותי	**מחשוב ענן מהותי**
פרק א' – כללי (מבוא + תחולה + הגדרות)	כן (למעט הגדרות)	כן
פרק ב' - ממשל תאגידי (דירקטוריון + הנהלה בכירה + הביקורת הפנימית)	כן, למעט סעיפים 13(ג) ו- 16.	כן
פרק ג' - מגבלות על מיקור חוץ (פעולות האסורות להעברה למיקור חוץ)	לא	כן
פרק ד' - התקשרות עם נותן שירות (בדיקת נאותות לנותן השירות + חוזה מיקור חוץ)	לא	כן
פרק ה' – ניהול סיכון מיקור חוץ (תכנית לניהול מיקור חוץ + תכנית המשכיות עסקית)	סעיפים 26-24 : כן (בהקשר של ניהול סיכונים). סעיף 27 : כן (בהקשר של קביעת רמת המהותיות). סעיפים 29-28 : לא.	כן
פרק ו' - מיקור חוץ של פעילויות מיוחדות (התקשרות עם נותן שירות הפועל מול לקוחות + מיקור חוץ של הביקורת הפנימית + מיקור חוץ הקשור לציות ואיסור הלבנת הון ומימון טרור)	לא	כן
פרק ז' - דיווח לפיקוח (חובות דיווח למפקח על הבנקים)	לא	סעיף 33 – לא סעיף 34 - כן
פרק ח' - תחילה והוראות מעבר (תחילה והוראות מעבר + טיפול בהוראות ובהיתרים קיימים)	לא	כן, על שירותי מחשוב ענן שהוגדרו כמהותיים בהתאם להגדרת מיקור חוץ בהוראה 359A.

* במקרה בו קיימת אי התאמה בין הנוסח בנספח זה לבין הנוסח המופיע בהוראות 362 ו 359A נוסח ההוראות גובר.

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'. השימוש בשירותי מחשוב ענן על ידי בנקים בעולם ובישראל עשוי לשמש כמענה לצרכים עסקיים דוגמת שדרוג מערכות מהותיות. מגמה זו צפויה להתגבר, בין השאר על רקע התפתחות ושדרוג טכנולוגיית מחשוב הענן והגברת התחרות בין הבנקים.
2. בצד היתרונות הגלומים בשימוש בטכנולוגיות ענן, שימוש בטכנולוגיות אלו עלול לחשוף את התאגיד הבנקאי לסיכונים תפעוליים מהותיים הקשורים לאבטחת מידע והגנת הסייבר, המשכיות עסקית, שליטה ובקרה על נכסי ה- IT, וכד'. סיכונים אלו נגזרים, בין היתר, מתלות בנותני שירותים או טכנולוגיות ספציפיים; כלי ניהול, אבטחה, שליטה ובקרה שמיושמים בצורה שאינה מיטבית; קשיים בהגנה על המידע וביישום בקרות נאותות; העצמת הנזק הפוטנציאלי במקרה של כשל, במיוחד כאשר נוצרות נקודות כשל יחידות (Single Points of Failure); ועוד. נציין כי סיכונים אלו בחלקם אמנם מוכרים, אך נוכח המאפיינים הספציפיים של טכנולוגיות אלו גלומים בהן סיכונים ייחודיים.
3. הגישה הפיקוחית בהיבטי טכנולוגיה ואבטחת מידע והגנת הסייבר היא מאפשרת (Business enabler) ורואה במעבר מערכות התאגידים הבנקאיים למחשוב ענן, לרבות מערכות מהותיות, חלק מהחדשנות וההתפתחות הטכנולוגית. כל זאת בכפוף לניהול סיכונים מושכל, זהיר וקפדני.

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 כאמור בסעיפים 11(א) (3א) ו-(3ב);
   3) תאגיד כאמור בסעיף 11 (ב);
   4) סולק כהגדרתו בסעיף 36ט.

   (ב) בטל
5. הוראה זו אינה חלה על "ענן פרטי" כהגדרתו בסעיף 6 להוראה זו.

פרק ב': כללי

הגדרות

6. להלן הגדרות ההוראה:

"מחשוב ענן" מודל המאפשר גישה נוחה מכל מקום, לפי דרישה, למאגר משותף של משאבי מחשוב הניתנים להגדרה (למשל: רשתות, שרתים, אחסון, יישומים ושירותים), שניתן להתאימו במהירות.

"ענן פרטי" תשתית מחשוב ענן המוקצית לשימושו הבלעדי של תאגיד בנקאי אחד. התשתית יכולה להיות בבעלותו, בניהולו ובתפעולו של התאגיד הבנקאי או צד שלישי או בכל שילוב ביניהם והיא יכולה להתקיים בחצרי התאגיד הבנקאי או מחוצה להם.

"מחשוב ענן מהותי" שימוש בשירותי מחשוב ענן במיקור חוץ כהגדרתו בסעיף 8 להוראת ניהול בנקאי תקין מס' 359A בנושא "מיקור חוץ" (להלן: "הוראה 359A"), כאשר לעניין זה מהותיות פעילות מחשוב הענן תקבע על פי השיקולים המפורטים בסעיף 27 להוראה 359A ובנוסף גם על פי השיקולים הבאים:

(א) סוג הענן.

(ב) סוג שירות מחשוב הענן.

(ג) שירות מחשוב הענן כולל מידע המוגדר על ידי התאגיד הבנקאי כמידע רגיש.

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

(ה) שירות מחשוב הענן מספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד, ולא קיימים אמצעים דומים מסוגיהם גם בחצרי התאגיד הבנקאי.

הוראות כלליות

7. 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 לרגולציית הגנת המידע של האיחוד האירופי (GDPR - General Data Protection Regulation).

8. שירותי מחשוב ענן מהותי ייחשבו פעילות מהותית במיקור חוץ וככאלה הינם כפופים להוראה 359A (למעט חובת הדיווח בסעיף 33 להוראה 359A) כמו גם להוראה זו, אשר מפרטת ומרחיבה את ההנחיות הייחודיות להם. בהתאם, ההגדרות המופיעות בהוראה 359A רלוונטיות גם להוראה זו.

9. 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.
10. התאגיד הבנקאי יוודא כי נותן שירות מחשוב הענן יישא באחריות כלפי התאגיד הבנקאי, לרבות קיום החובות הכלולות בחוזה ההתקשרות בין נותן שירות מחשוב הענן לתאגיד הבנקאי, גם במקרה בו נותן שירות מחשוב הענן עושה שימוש בנותן שירות משני.

פרק ג': ממשל תאגידי

11. פרק ב' בהוראה 359A בנושא ממשל תאגידי יחול גם על מחשוב ענן שאינו מחשוב ענן מהותי. זאת, למעט סעיפים 13(ג) ו- 16 בהוראה 359A.

דירקטוריון

12. על הדירקטוריון לדון במסמך "מדיניות לשימוש בשירותי מחשוב ענן", כאמור בסעיף 16 להלן, ולאשר אותו.
13. על הדירקטוריון לאשר את תכנית העבודה הרב שנתית למחשוב ענן, כאמור בסעיף 20 להלן, לרבות יישום של כל שירות מחשוב ענן מהותי.
14. על הדירקטוריון לוודא שהשימוש בשירותי מחשוב ענן יהיה על פי המדיניות שנקבעה כאמור.

הנהלה בכירה

15. על ההנהלה הבכירה לגבש מדיניות לשימוש בשירותי מחשוב ענן אשר תקבע, בין היתר, את מאפייני השירותים המוגדרים כמחשוב ענן מהותי ובהם נדרש אישור של הדירקטוריון, את מאפייני שירותי מחשוב הענן בהם נדרש אישור הנהלה בכירה וכן את מאפייני שירותי מחשוב הענן בהם נדרש אישור אחר.
16. מסמך "מדיניות לשימוש בשירותי מחשוב ענן" יתייחס לקביעת רמת מהותיות שירותי מחשוב הענן בהסתמך על הגדרת מחשוב ענן מהותי בהוראה זו ; סמכויות, אחריות ופעולות גורמי ניהול שירותי מחשוב ענן לרבות ניהול נותן שירות מחשוב הענן, גורמי הבקרה והבקרות ; מאפייני השירותים והיקפם, תהליכי אישור ודרגי אישור ; אחריות הגורמים השונים בתאגיד הבנקאי לטיפול בהיבטים משפטיים, תחזוקה, ניטור, אבטחת מידע והגנת הסייבר, טיפול באירוע, המשכיות עסקית ורציפות תפקודית וכד'. המדיניות תיתן מענה גם לנדרש בהוראה זו ובהוראות רלוונטיות נוספות.
17. ההנהלה הבכירה תעקוב באופן שוטף אחר יישום מדיניות מסמך "מדיניות לשימוש בשירותי מחשוב ענן", כפי שאושר על ידי הדירקטוריון.
18. התאגיד הבנקאי יגדיר גורם הכפוף למנהל חטיבת טכנולוגיית המידע שיכיר באופן מעמיק את הסיכונים ואת השירותים הטכנולוגיים של כל נותן שירותי מחשוב ענן עמו התקשר התאגיד הבנקאי. התאגיד הבנקאי יבחן את הצורך להגדיר גורם אחראי לכל נותן שירותי מחשוב ענן שעמו התקשר.
19. התאגיד הבנקאי יגדיר גורם הכפוף למנהל הסיכונים, שיכיר באופן מעמיק את סיכוני כלל הפעילות במחשוב ענן.

20. על ההנהלה הבכירה להכין תכנית עבודה רב שנתית למחשוב ענן. התכנית תתן מענה, בין היתר, לסיכונים הגלומים בשירותי מחשוב הענן והבקרות המיושמות או המתוכננות להפחתתם.

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

פרק ה': ניהול סיכונים

21. סעיפים 24 עד 26 בהוראה 359A יחולו גם על מחשוב ענן שאינו מחשוב ענן מהותי.

22. בטל.

23. תאגיד בנקאי יבצע הערכת סיכונים וסקר סיכונים באופן הבא:

(א) מיפוי והערכת סיכונים לכל יישום של שירות מחשוב ענן. הערכת הסיכונים תעשה קודם להתקשרות עם נותן שירותי מחשוב הענן ותעודכן באופן שוטף במהלך תקופת ההתקשרות, בין היתר, בהתאם לשינויים, כגון: טכנולוגיים, משפטיים, רגולטוריים, עסקיים וארגוניים אצלו ואצל נותן שירותי מחשוב הענן. אמנם שירות מחשוב ענן מהווה מקרה פרטי של מיקור חוץ, אך הערכת הסיכונים במקרה זה צריכה לכלול גם סיכונים ייחודיים (טכנולוגיים ואחרים) הקשורים לשימוש במחשוב ענן. היבטים עיקריים שיש לקחת בחשבון מובאים בנספח ב' להוראה זו – "היבטים עיקריים להערכת סיכונים במחשוב ענן".

(ב) בשירותי מחשוב ענן מהותי ביצוע סקר סיכונים, כאמור בהוראת ניהול בנקאי תקין מס' 350 בנושא "ניהול סיכונים תפעוליים", יהיה לכל הפחות אחת לשנתיים.

(ג) ווידוא קיום בקרות מפצות מתאימות בהתאם להערכת הסיכונים.

24. 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.

25. התאגיד הבנקאי יגדיר:

(א) תחומי אחריות לניהול, שליטה, אישור ותיעוד של שירותי מחשוב הענן בתאגיד הבנקאי.

(ב) מודל חלוקת אחריות בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן, ובכלל זה בהיבטי אבטחת מידע והגנת הסייבר. חלוקת אחריות זו אינה גורעת מאחריות התאגיד הבנקאי לקיום מכלול הדינים וההוראות החלים עליו.

26. עבור כל שירות מחשוב ענן התאגיד הבנקאי יתעד, לכל הפחות, את ההיבטים הבאים:

(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 השירות ועלותו, סמכויות שיפוט וכו'.

(ג) מאפייני שירותי מחשוב הענן, כגון: מיפוי ותיאור הארכיטקטורה, הממשקים ודרישות אבטחת המידע והגנת הסייבר וכו'.

27. התאגיד הבנקאי יעדכן את התיעוד, כאמור בסעיף 26 לעיל, בכל מקרה של שינוי באחד המאפיינים המפורטים בסעיף האמור. כמו כן, אחת לתקופה שיקבע, יוודא התאגיד הבנקאי את עדכניות התיעוד האמור.

פרק ו': התקשרות עם נותן שירותי מחשוב הענן

28. פרק זה אינו חל על מחשוב ענן שאינו מחשוב ענן מהותי.

בדיקת נאותות

29. במחשוב ענן מהותי, התאגיד הבנקאי יבצע בדיקת נאותות (Due Diligence) לנותן שירותי מחשוב הענן, לרבות זיהוי והערכת הסיכונים הפוטנציאליים בהתקשרות עמו והשימוש בשירותיו, כאמור בסעיף 23, ולכל הפחות לפי הסיכונים המפורטים בנספח ב' להוראה זו – "היבטים עיקריים להערכת סיכונים במחשוב ענן". בנוסף התאגיד הבנקאי יבדוק:

(א) עמידה של נותן שירותי מחשוב הענן בכל דין ורגולציה הרלבנטיים לשימוש בטכנולוגיות מחשוב ענן, לרבות דיני הגנת הפרטיות החלים באותה המדינה בה הוא פועל.

(ב) עמידה של נותן שירותי מחשוב הענן ברמת הגנת סייבר נאותה, בין היתר כפי שיוגדר במסמך "מדיניות לשימוש בשירותי מחשוב ענן".

חוזה מחשוב ענן

30. מבלי לגרוע מהחובות החלות על התאגיד הבנקאי לפי הוראה 359A והוראת ניהול בנקאי מס' 363 "ניהול סיכוני סייבר בשרשרת אספקה", במחשוב ענן מהותי חוזה ההתקשרות עם נותן שירותי מחשוב הענן יכלול, בין היתר, התייחסות לנושאים הבאים:

(א) מחיקת המידע של התאגיד הבנקאי, או פעולה דומה, ממערכות נותן שירותי מחשוב הענן והתחייבותו כי לא ניתן יהיה לאחזר מידע זה במערכותיו.

(ב) בטל.

(ג) בטל.

(ד) הבטחת 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.

(ה) יישום הנחיות המודל שנקבע לעניין חלוקת האחריות כנדרש בסעיף 25.

(ו) מיקום מתקן הענן ממנו יינתן השירות ומיקום אחסון הנתונים, לרבות התחייבות נותן שירות מחשוב הענן להודיע לתאגיד הבנקאי מראש על כל שינוי באמור.

(ז) אופן אחסון המידע הרגיש והנגישות אליו תוך כדי תקופת השירות ולאחריה.

(ח) גיבוי המידע והאפשרות לאחזורו.

(ט) הגדרת יכולת התאגיד הבנקאי להפעיל או להפסיק שירותי מחשוב ענן מהותיים או רכיבים מתוך שירותים אלה לרבות חסימות גישה, ככל שרלוונטי ובעת חירום כדוגמת אירוע סייבר, מתוך הצורך לצמצם סיכונים. זאת, בין באופן עצמאי ובין על ידי נותן שירות מחשוב הענן בהתאם לבקשת התאגיד הבנקאי. הגדרת התהליכים התומכים ביכולות אלה, תוך התייחסות למשאבים של נותן שירותי מחשוב הענן בהם נעשה שימוש משותף על ידי התאגיד הבנקאי וגורמים אחרים המקבלים שירות מאותו נותן שירות מחשוב ענן.

(י) בחינת שילוב התחייבות נותן שירות מחשוב הענן להשתתפות בתרגילי סייבר שיקיים מולו התאגיד הבנקאי אחת לתקופה, בהתאם לאופי היישום.

(יא) יישום בקרות מפצות הנדרשות מנותן שירות מחשוב הענן בהתאם להערכת סיכונים כמפורט בסעיף 23 להוראה זו.

ניהול ההתקשרות עם נותן שירותי מחשוב ענן מהותי

31. התאגיד הבנקאי ינהל את ההתקשרות עם נותן שירותי מחשוב ענן מהותי על פי העקרונות הבאים:

(א) מעקב אחר ביצועי השירות, הבטחון 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 חלוקת האחריות כנדרש בסעיף 25.

(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 או סיום התקשרות. התכנית תיבדק ותתעדכן אחת לשלוש שנים.

(ו) בחינת 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 או בשירותי מחשוב ענן.

(ז) בכל שינוי בשליטה על נותן שירותי מחשוב הענן, נדרשת בחינה מחדש של ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם על ידי בעלי השליטה החדשים.

פרק ז': מכתב ההיתר - בטל

פרק ז'1: אבטחת מידע והגנת הסייבר

32. על התאגיד הבנקאי לנהל את סיכוני אבטחת המידע והגנת הסייבר במחשוב ענן (מהותי ושאינו מהותי), תוך התייחסות בין היתר להיבטים של סיווג המידע, מיקום מפתחות ההצפנה, מעורבות התאגיד הבנקאי בניהול מפתחות ההצפנה ורמת ההצפנה, שיטת ההצפנה ועוד.
33. על המידע של התאגיד הבנקאי להיות מוצפן בעת העברתו בתקשורת וכן בעת אחסונו. 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.
34. 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 ("אירוע סייבר" כהגדרתו בהוראת ניהול בנקאי תקין מס' 361 בנושא "הגנת הסייבר") הקשורים לשירותי מחשוב ענן בין היתר כמפורט בנספח ג' להוראה זו - "ניטור אירועי סייבר במחשוב ענן".
35. 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, שיכללו, 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.
    (ג) ביצוע, לכל הפחות, של תרחיש קיצון אחד מייצג בפעילות אחת או יותר משירותי מחשוב הענן המהותיים שלו.
36. 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.

פרק ז'2: המשכיות עסקית

37. ככל שמחשוב הענן מהווה שירות חיוני לתאגיד הבנקאי יחולו עליו הדרישות הרלוונטיות בהוראת ניהול בנקאי תקין מס' 355 בנושא "ניהול המשכיות עסקית".

38. ככל שמחשוב הענן הינו מחוץ לישראל, על התאגיד הבנקאי לבחון תכניות מענה לתרחיש של אי זמינות השירות כתוצאה מנתק תקשורתי לחו"ל או מאירועים גיאופוליטיים מול המדינה הזרה. זאת ועוד, התאגיד יעריך את יכולת ההמשכיות העסקית של נותן השירות אל מול איומי הייחוס המקומיים של המדינה המארחת.

39. באתר מחשוב בענן ראשי או חלופי - התאגיד הבנקאי נדרש לוודא עמידתו של האתר בדרישות Tier3 בהתאם לסטנדרטים שנקבעו בתקן UpTime Institute (UTI) על ידי קבלת תעודה מ-UTI או חוות דעת חיצונית מגורם מומחה בלתי תלוי.

פרק ח': דיווח לפיקוח

40. אחת לשנה בגין סיום שנה קלנדרית, על תאגיד בנקאי להעביר דיווח בכתב לידי הפיקוח על הבנקים. הדיווח יתבצע על פי הוראת דיווח לפיקוח מס' 881 בנושא "דיווח על מחשוב ענן (שנתי)".

עדכונים

חוזר מס'	גרסה	פרטים	תאריך
2536	1	מכתב מפקח מקורי	05/07/2017
2579	2	עדכון	13/11/2018
2669	3	עדכון	30/09/2021
2715	4	עדכון	13/06/2022

נספח א' – דוגמאות למחשוב ענן מהותי - בטל

נספח ב' – היבטים עיקריים להערכת סיכונים במחשוב ענן

(א) סיכון רגולטורי הנובע משימוש בענן הממוקם מחוץ לגבולות מדינת ישראל - קושי בעמידה בחוקים, תקנות ורגולציות של מדינת ישראל ושל המדינה שבה פועל או מאוחסן השירות או הנתונים. מאחר וקיימים הבדלים בחקיקה בין המדינות יש חשיבות, בין היתר, להתייחס לסוגיות כגון חובת נותן שירותי מחשוב הענן למסור מידע לגורמי חוק ואכיפה גם ללא ידיעת התאגיד הבנקאי והיבטים של הגנת הפרטיות.

(ב) סיכון הנובע משימוש או מאי שימוש בתצורת ענן מרובה (תשתיות ענן המבוססות על שילוב של מספר פתרונות שונים של מחשוב ענן).

(ג) מחזור חיי הנתונים, לרבות מיקום, ריבוי העתקים וחשיפת נתונים.

(ד) ניידות נתונים, רכיבים ומערכות - למשל, האם השימוש ברכיבי מחשוב ענן של נותן שירותי מחשוב ענן מסוים מגביל את התאגיד הבנקאי ועלול למנוע ממנו את האפשרות לעבור לנותן שירותי מחשוב ענן אחר או להעביר את המידע או המערכות חזרה לחצרי הבנק.

(ה) סיכוני אבטחת מידע והגנת הסייבר, לרבות דלף מידע, שימוש בכלי אבטחה ייעודיים, אופן ניהול מפתחות ההצפנה, שירות מחשוב ענן המספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד.

(ו) הרשאות גישה, תוך הפעלת כלים המתאימים לסביבת מחשוב ענן.

(ז) ניהול שינויים וניהול נכסי טכנולוגית המידע, לרבות התייחסות לצורך בשינויים הנדרשים מנותן שירותי מחשוב הענן כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים, לשליטה של התאגיד הבנקאי על שינויים במערכות ותאימות תהליכי השינויים למדיניות התאגיד הבנקאי ונהליו.

(ח) סיכונים הקשורים להמשכיות עסקית ו - BCP/DRP, לרבות שינויים בתצורת רשת התאגיד הבנקאי, ומיקומם הגאוגרפי של שרתי הענן ובכללם שרתי הגיבוי.

(ט) סיכונים הקשורים לסביבות העבודה וכלי הניהול העלולים להוסיף מורכבות לתפעול המערכות.

(י) סיכונים משפטיים וביניהם היבטי סודיות, שמירת נתונים ואחזורם, הבעלות על המידע ורישוי תוכנות.

(יא) סיכוני תפעול שוטף (כולל אנשי תמיכה, תהליכי עבודה, ניהול אירועים ועוד), טיפול באירועים חריגים, והקטנתם בין היתר באמצעות הסדרי דיווח וטיפול, הסדרת תחומי האחריות בין התאגיד הבנקאי לבין נותן שירותי מחשוב הענן.

(יב) סיכונים הנוגעים למעטפת התקיפה כגון: שילוב מכשירים ניידים (טלפונים ניידים, טאבלטים וכל אמצעי נייד אחר) בשירות מחשוב הענן.

(יג) סיכונים הכרוכים בשרשרת אספקה של שירות מחשוב ענן.

(יד) קיום הפרדה לוגית ומנהלתית בין המערכות של הלקוחות השונים בענן.

נספח ג' – ניטור אירועי סייבר במחשוב ענן

(א) ניטור הפעילות בענן ישתלב במערך הניטור השוטף של התאגיד הבנקאי. ניהול הניטור והגדרתו יהיו בידי התאגיד הבנקאי, כך שניהול הניטור יהיה לכל הפחות בהתאמה לאופן היישום בענן.

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

(ג) אם ניטור זה מבוצע באמצעות כלים המסופקים ע"י נותן שירותי מחשוב הענן, יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של התאגיד הבנקאי.

(ד) במידה והתאגיד הבנקאי ישתמש במערכת ניטור המצויה בסביבות הענן באותה סביבת תשתיתית בה מצוי שירות מחשוב ענן מהותי של התאגיד הבנקאי, התאגיד הבנקאי יגדיר פעולות בקרה להמשך רציפות ניטור שירות מחשוב הענן המהותי בעת ניתוק תקשורת בין התאגיד הבנקאי למערכת הניטור של סביבת הענן.