בנק ישראל התיר לבנקים להרחיב את השימוש בענן

לאחרונה פרסם המפקח על הבנקים עדכון להוראת ניהול בנקאי תקין מס' 362 שעניינה מחשוב ענן (להלן: **"ההוראה"** ו**"העדכון"**, בהתאמה). העדכון פורסם על רקע השינויים וההתפתחויות שחלו בשנים האחרונות בטכנולוגיית מחשוב הענן והרצון לאפשר לבנקים ליהנות מהיתרונות של מחשוב ענן. עם זאת, בנק ישראל הצביע על כך שלצד היתרונות הרבים הגלומים בשירותי מחשוב הענן, קיימים בהם סיכונים לא מבוטלים ובהתאם, נועד העדכון להנחות את הבנקים ביחס לניהול סיכונים אלו.

במסמך זה, ריכזנו כמה דגשים מרכזיים מתוך העדכון:

- **ביטול האיסור על שימוש בשירותי מחשוב ענן עבור פעילויות ליבה ומערכות ליבה**: זהו החידוש העיקרי בעדכון ומשמעותו היא למעשה מעבר לבחינת מהותיות מחשוב הענן והסיכונים הגלומים בשימוש בו, חלף האיסור שהיה קיים עד כה, והטלת חובות מוגברות על התאגיד הבנקאי ביחס למחשוב ענן מהותי. מהותיות מחשוב הענן תקבע על פי השיקולים המנויים בהוראת ניהול בנקאי תקין מס' A359 בנושא "מיקור חוץ" (**"הוראה A359"**), ובכלל זה מידת ההשפעה של כשל אצל נותן השירות על מצבו הפיננסי של התאגיד הבנקאי, נזק פוטנציאלי ללקוחות התאגיד הבנקאי במקרה של כשל, עלויות מיקור החוץ, וכן שיקולים נוספים המנויים בעדכון כגון סוג הענן, סוג שירות מחשוב הענן, רגישות המידע שיעובד ואמצעי אבטחת המידע.

- **מיקור חוץ**: הוראה A359 מטילה על התאגידים הבנקאיים חובות מסוימות בכל הנוגע למיקור חוץ, כאשר השימוש בשירותי מחשוב ענן מהווה מקרה פרטי של מיקור חוץ. בהתאם, ככלל תחול ביחס לשירותי מחשוב ענן מהותי גם הוראה A359 (למעט במספר נושאים מסוימים המפורטים בעדכון), ובכלל זה השיקולים הנוגעים להגדרת רמת המהותיות של מיקור החוץ (כמפורט לעיל) ולניהול הסיכונים. התקשרות לקבלת שירותי מחשוב ענן מהותי נדרשת להיות מאושרת על-ידי הדירקטוריון.

- **תחולה**: ההוראה אינה חלה על "ענן פרטי", קרי, תשתית מחשוב ענן המוקצית לשימוש הבלעדי של תאגיד בנקאי אחד.

- **קביעת מדיניות ותכנית עבודה והגדרת אחריות הדירקטוריון וההנהלה הבכירה**:

  - ההנהלה הבכירה בתאגיד בנקאי נדרשת לקבוע מדיניות לשימוש בשירותי מחשוב ענן, אשר תעלה בקנה אחד עם הדרישות הרגולטוריות, לרבות בהיבטים הנוגעים לטכנולוגיית מידע ותקשורת, אבטחת מידע והגנת הסייבר, המשביות עסקית וניהול סיכונים תפעולי (להלן: "**המדיניות**"), ולעקוב אחר יישומה באופן שוטף. המדיניות תקבע, בין היתר, את האישורים הנדרשים לכל סוג של מחשוב ענן בהתאם למאפייניו, תגדיר סמכויות ואחריות ועוד. הדירקטוריון נדרש לדון במדיניות, לאשר אותה ולוודא שהשימוש בשירותי מחשוב הענן יהיה על-פי המדיניות שנקבעה.

  - כמו כן, נדרשת ההנהלה הבכירה להכין תכנית עבודה רב שנתית למחשוב ענן אשר תכלול, בין השאר, התייחסות לסיכונים הגלומים בשירותי מחשוב ענן ובקרות להפחתתם. תכנית העבודה האמורה תאושר על-ידי הדירקטוריון.

- **ניהול והערכת סיכונים**: נקבעה חובה לכלול התייחסות פרטנית לסיכוני מחשוב ענן בדו"חות הסדירים המוגשים לדירקטוריון ולהנהלה הבכירה. בנוסף, במקרה של מחשוב ענן מהותי, הוטלה חובה על התאגידים הבנקאיים לבצע סקר סיכונים לפחות אחת לשנתיים.

- **חוזה מחשוב ענן:** בעדכון נוספו הוראות מסוימות שיש לכלול בחוזה עם נותן שירותי מחשוב הענן ובכלל זה דרישה להבטחת יכולתו של התאגיד הבנקאי לקבל מידע הרלוונטי לפעילויות שהועברו למיקור חוץ המוחזק אצל נותן השירות, התייחסות לאופן אחסון מידע רגיש, גיבוי המידע ואחזורו ועוד.

- **מינוי בעלי תפקידים**: תאגידים בנקאיים נדרשים למנות גורם הכפוף למנהל טכנולוגיות המידע אשר יכיר באופן מעמיק את הסיכונים הכרוכים בשירותי מחשוב ענן ואת נותני השירותים עימם התקשר התאגיד הבנקאי. כמו כן, נדרש התאגיד הבנקאי למנות גורם הכפוף למנהל הסיכונים אשר יהיה אחרי על הערכה שוטפת ומעמיקה של סיכוני הפעילות במחשוב הענן בראייה רחבה של כלל שירותי מחשוב הענן שמקבל התאגיד הבנקאי.

- **מחשוב ענן מחוץ לגבולות ישראל**:

  - נקבע כי תאגיד בנקאי לא יאחסן, יעביר או יעבד מידע שמוגדר על ידו כ"רגיש" (למשל נתוני לקוחות, מידע עסקי חסוי וכיו"ב) בענן מחוץ לגבולות ישראל, אלא אם וידא שרמת ההגנה של ספק שירותי הענן תואמת את רגולציית אבטחת המידע של האיחוד האירופאי (GDPR – General Data Protection Regulation).
  - עוד נקבע כי במקרה של מחשוב ענן מחוץ לישראל, על התאגיד הבנקאי לבחון תכניות מענה לתרחיש של אי זמינות השירות כתוצאה מנתק תשדורתי לחו"ל או מאירועים גיאופוליטיים מול המדינה הזרה, ולהעריך את יכולת ההמשכיות העסקית של נותן השירות אל מול איומי הייחוס המקומיים של המדינה המארחת.

- **אבטחת מידע וסייבר**: התאגידים הבנקאיים נדרשים לנהל את סיכוני אבטחת המידע והגנת הסייבר במחשוב ענן, תוך התייחסות להיבטים של סיווג מידע, שיטת ההצפנה, ביצוע ניטור רציף ועוד.

- **דיווח**: בכל הנוגע למחשוב ענן מהותי, נדרש התאגיד הבנקאי להעביר דיווח בכתב למפקח על הבנקים, אחת לשנה, בהתאם להוראת דיווח לפיקוח מס' 881 בנושא "דיווח על מחשוב ענן (שנתי)", ובכלל זה לפרט את מטרות שירותי מחשוב הענן, סוג השירות (למשל IaaS, PaaS, SaaS), סוג המידע שנשמר בענן, מיקום הענן ועוד.

- **תחילה**:

  - מועד תחילת ההוראה הוא ביום 1 בינואר 2023, אולם התאגידים הבנקאיים רשאים ליישמה בכללותה עוד בטרם מועד זה.
  - בכל הנוגע לחוזים שנכרתו לפני 13 ביוני 2022 (מועד פרסום ההוראה) – יש להתאים את החוזה להוראה במועד חידוש החוזה הקרוב ולא יאוחר מיום 31 בדצמבר 2026.
  - בכל הנוגע לחוזים שנכרתו לאחר 13 ביוני 2022 ועד ליום 1 בינואר 2023 – יש להתאים את החוזה להוראה לא יאוחר מיום 31 בדצמבר 2023.

בשים לב להיקף ההוראות ולהיערכות הנדרשת, מומלץ לתאגידים הבנקאיים לנקוט כבר כעת בצעדים ליישום ההוראה לקראת מועד תחילתה בעוד כחצי שנה.

אנו עומדים לרשותכם בכל שאלה,

עו"ד אסף הראל, שותף
assafh@gornitzky.com

עו"ד רבקה גניס
rebeccage@gornitzky.com

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.