



תל אביב, כטי' כסלו, תשפ"ה

30 דצמבר, 2024

חוזר מס' מ-301-02

לכבוד

לשכות האשראי**הנדון: תיקון הוראה מספר 301 בנושא "ניהול המידע והגנתו" בנוגע לשירותי מחשוב ענן ונושאים נוספים****מבוא**

1. בשנים האחרונות קיימת עליה ניכרת בשימוש בשירותי מחשוב ענן על ידי ארגונים שונים, ובהם ארגונים מהסקטור הפיננסי. זאת, בין היתר, על רקע תהליכי דיגיטציה שהואצו בעקבות משבר הקורונה. לשימוש בשירותי מחשוב ענן יתרונות רבים, כגון השגת חיסכון בעלויות והגברת היעילות התפעולית. לצד זאת, השימוש בשירותי מחשוב ענן כרוך בסיכונים ייחודיים, לרבות סיכונים אבטחת מידע והגנת הסייבר, המשכיות עסקית ופגיעה במוניטין, שנדרש לזהותם ולנהלם באופן נאות.
2. לאור רצונן של לשכות האשראי להרחיב את השימוש בשירותי מחשוב ענן על רקע היתרונות כמפורט לעיל, ובמטרה לחזק את יכולתן לנהל את הסיכונים הייחודיים הכרוכים בשימוש במחשוב ענן, בוצעו תיקונים להוראה מספר 301 בנושא "ניהול המידע והגנתו" (להלן – **ההוראה**, **הוראה 301**) אשר עיקריהם יפורטו להלן. שימוש בשירותי מחשוב ענן מהווה חלק ממסגרת העבודה הכוללת לניהול המידע והגנתו, ובכלל זאת לעניין הצורך במדיניות לשימוש בשירותי מחשוב ענן, ביצוע סקרי הערכת סיכונים אבטחת מידע ומבחני חדירה מותאמים למחשוב ענן, דיווח על אירועי אבטחת מידע לדירקטוריון ולממונה ועוד.
3. מובהר כי שירותי מחשוב ענן הינם מקרה פרטי של מיקור חוץ. לפיכך, פרט להוראות הרלוונטיות בהוראה 301, יחולו על שימוש בשירותי מחשוב ענן גם הנחיות הוראת הממונה מס' 311 בנושא "מיקור חוץ" (להלן – **"הוראה 311 בנושא מיקור חוץ"**) המפורסמת במקביל לתיקון הוראה זו, כמפורט בחוזר מס' מ-311-01. עוד מובהר, כי אין במודל האחריות המשותפת (Shared Responsibility Model) של הלשכה ושל נותן שירות מחשוב הענן, כמפורט בגוף ההוראה, בכדי לגרוע מאחריות הלשכה לקיום מכלול הדינים וההוראות החלים עליה.
4. בנוסף, בהמשך לפרסום הוראת הממונה מס' 312 בנושא "ניהול המשכיות עסקית" (להלן **הוראה 312 בנושא המשכיות עסקית**), עודכנו ההנחיות הנוגעות לתכנית היערכות לניהול אירועי אבטחת מידע ולגיבוי ושחזור נתונים, בפרקים ג' ו-ז' בהוראה 301, כך שהן כוללות הנחיות משלימות לאלו שנקבעו בהוראה 312 בנושא המשכיות עסקית. בנוסף, בוצעו בהוראה 301 כמה תיקונים לצרכי הבהרה וכמה עדכוני ניסוח.
5. כמו כן, בעקבות התיקונים כאמור בוצעו תיקונים תואמים בהוראת ממונה מס' 308 בנושא "הוראת דיווח ללשכות אשראי" ובהוראת ממונה מס' 308A בנושא "נספחים להוראות דיווח ללשכות אשראי", כמפורט בחוזר מס' מ-308-03/מ-308A-03.
6. האסדרה מלווה בפרסום דוח קביעת אסדרה לפי חוק עקרונות האסדרה, תשפ"ד-2021 (להלן – **"חוק עקרונות האסדרה"**), אשר מצורף כנספח לחוזר זה.

7. בחינה ראשונה של התיקונים להוראה לפי סעיף 36 לחוק עקרונות האסדרה תתבצע בתום תקופה של 10 שנים מיום כניסתם לתוקף או במועד מוקדם יותר, ככל שיעלה הצורך.
8. להלן פירוט עיקרי התיקונים בהוראה.

פרק א' - כללי

9. נוספו הגדרות ובוצעו התאמות רלוונטיות לתיקונים בנושא מחשוב ענן ולהוראה 311 בנושא מיקור חוץ.

פרק ב' - פיקוח וניהול

10. **התייחסות לשירותי מחשוב ענן במסמך המדיניות לניהול המידע והגנתו:** נוספה דרישה לפיה בהתייחס לשירותי מחשוב ענן, מסמך המדיניות לניהול המידע והגנתו יכלול התייחסות, בין היתר, להיבטים הבאים: קביעת המהותיות של שירותי מחשוב ענן; מאפייני השירותים והיקפם; תהליכי ודרגי אישור בעת עבודה בענן; חלוקת סמכויות ואחריות הגורמים השונים בלשכה לטיפול בהיבטי מחשוב ענן; ניהול סיכונים וגיבוי בקרות הולמות (סעיף 12א).
11. **אישור הדירקטוריון למחשוב ענן אשר הוגדר כמחשוב ענן מהותי:** נוספה דרישה לדירקטוריון לאשר מראש התקשרות עם נותן שירות בפעילות מהותית, לרבות מחשוב ענן מהותי, בהתאם לסעיף 13 בהוראה 311 בנושא מיקור חוץ (סעיף 13א).
12. **הממונה על אבטחת מידע:** נוספה הבהרה לפיה תחום אחריות הממונה על אבטחת מידע יכלול גם שירותי מחשוב ענן (סעיף 21).
13. **ביקורת פנימית:** נוספה הבהרה לפיה תכנית הביקורת הפנימית לבחינת מסגרת העבודה לניהול המידע והגנתו, תכלול ביקורת בעניין שימוש בשירותי מחשוב ענן (סעיף 25).
14. **דיווחים לממונה:**
- 14.1. **דיווח מראש לממונה -** נוספה חובת דיווח מראש לממונה על כוונת הלשכה להתקשר עם נותן שירות של מחשוב ענן מהותי, לפחות 60 יום בטרם ההתקשרות (סעיף 30א). דרישה זו הינה בדומה לדרישה המפורטת בסעיף 17 בהוראה 311 בנושא מיקור חוץ.
- 14.2. **דיווח מידי לממונה -** למען הסר ספק, מובהר שמאחר ששימוש בשירותי מחשוב ענן הינו מקרה פרטי של מיקור חוץ והוראה 311 בנושא מיקור חוץ חלה גם על שירות מחשוב ענן, דיווח מידי לממונה על התרחשות או כמעט התרחשות של אירוע משמעותי של אבטחת מידע או פגיעה בפרטיות שמקורו אצל נותן שירות, וכן על התרחשות או כמעט התרחשות של אירוע משמעותי שבו התממשו סיכונים בלשכה, שמקורו אצל נותן השירות, יהיה בהתאם לסעיף 18 בהוראה 311 בנושא מיקור חוץ.

פרק ג' - הגנת המידע

15. **סקרי הערכת סיכוני אבטחת מידע ומבחני חדירה ("סקרים"):** נוספו דגשים והנחיות פרטניים לסקרים בהתייחס למחשוב ענן, ובכלל זאת:
- 15.1. ביצוע מבחני חדירה בהתאם למודל האחריות המשותפת בין הלשכה לבין נותן שירות מחשוב הענן ובתיאום עמו, תוך מתן דגש לנושאים המפורטים בסעיף (סעיף 38.2).
- 15.2. עריכת סקרים בהתייחס למחשוב ענן על ידי גורם בעל ידע וניסיון בביצוע סקרים מסוג זה (סעיף 42).

פרק ג' - מחשוב ענן

16. להוראה נוסף פרק ייעודי בנושא מחשוב ענן, הכולל הנחיות בנושאים הבאים :
- 16.1. בוטל סעיף 131 אשר כלל איסור להעביר לסביבת ענן ציבורי מערכות המנהלות מידע רגיש.
- 16.2. הובהר כי שימוש בשירותי מחשוב ענן מהווה מקרה פרטי של מיקור חוץ, ועל הלשכה לפעול בהתאם להנחיות המפורטות בהוראה 311 בנושא מיקור חוץ (סעיף 132).
- 16.3. **מחשוב ענן מהותי**: נקבע כי מחשוב ענן יוגדר כמהותי ככל שהוא מהווה פעילות מהותית בהתאם לסעיפים 23-24 בהוראה 311 בנושא מיקור חוץ, ובנוסף הלשכה תקבע האם מחשוב ענן יוגדר כמהותי לאחר שתביא בחשבון גם השיקולים הבאים (סעיף 132א):
- 16.3.1. סוג הענן (לדוגמה: ענן ציבורי, ענן פרטי, ענן היברידי) וסוג השירות (לדוגמה: Saas, IaaS, PaaS), בהתאם למודל האחרייות המשותפת ולאחר בחינה פרטנית של מאפייני השירות.
- 16.3.2. שירות מחשוב הענן מספק אמצעי אבטחת מידע והגנת הסייבר כרובד הגנה יחיד, ולא קיימים אמצעים דומים מסוגיהם גם בחצרות הלשכה.
- כמו כן, הובהר למען הסר ספק, שעל מחשוב ענן מהותי יחולו, בין היתר, ההנחיות לעניין פעילות מהותית במיקור חוץ כאמור בהוראה 311 בנושא מיקור חוץ.
- 16.4. **דגשים בהיבטי אבטחת מידע והגנת הסייבר בשימוש במחשוב ענן**: ניתנו דגשים לעניין חובות אבטחת מידע והגנת הסייבר במסגרת התקשרות עם נותן שירות מחשוב ענן, לרבות חובת הלשכה ליישם אמצעי אבטחת מידע שלא יפחתו מאלו שנדרש ליישם עבור מערכות שאינן בענן אשר מפורטות בהוראה, וכן דרישות לזיכוי קיומם של אמצעים להגנת הסייבר עבור כלל ערוצי הגישה מנותן שירות מחשוב הענן ואליו, לניטור הפעילות בענן באופן רציף, מלא ובזמן אמת, ושילוב הניטור במערך ה-SIEM עבור מערכות שחלות עליהן דרישות ההוראה לעניין בקרה וניטור בהתאם לסוג שירות מחשוב הענן ומודל האחרייות המשותפת, לזיכוי גישה באמצעות דרכי גישה מאובטחות, לזיכוי הצפנה בתעבורה ובמנוחה וניהול מפתחות ההצפנה בהתאם לדרישות ההוראה ולגיבוי הנתונים בעותק נוסף כנדרש בהוראה, בהתאמות המתחייבות לשירות מחשוב הענן, תוך זיכוי יכולת שחזור המידע המאוחסן בענן בכלל תרחישי האיום והשיבושים התפעוליים המשמעותיים האפשריים, בשים לב למהותיות נותן שירות מחשוב הענן ללשכה (סעיפים 132ב).
- 16.5. סעיפים 133-135 בוטלו.
- 16.6. **ניהול סיכונים**: נקבע כי בטרם התקשרות עם נותן שירות מחשוב ענן הלשכה תבצע הערכה של הסיכונים הגלומים בהתקשרות בהתאם להנחיות שבהוראה 311 בנושא מיקור חוץ, וכן תתייחס בין היתר לסיכונים הרלוונטיים לשירות מחשוב ענן, לרבות ההיבטים: בחינת מודל האחרייות המשותפת בין הלשכה לנותן השירות בהתאם לסוג הענן וסוג השירות; מאפייני שירות הענן ואופן הטמעתו; הנימוקים לשימוש בשירותי מחשוב ענן; תרשים ארכיטקטורה; מיקום מתקני הענן ואחסון הנתונים; מחזור חיי הנתונים וגיבוי הנתונים על ידי נותן השירות; היבטי אבטחת מידע והגנת הסייבר; עמידת נותן שירות מחשוב הענן בתקנים מקובלים והסמכות חיצוניות, בהתאם למאפייני השירות הניתן על ידו; פירוט הבקורות הנדרשות למזעור הסיכונים (סעיף 135א).
- 16.7. **הסכם התקשרות עם נותן שירות מחשוב ענן**: נקבע כי הסכם התקשרות עם נותן שירות מחשוב ענן יכלול בנוסף לנושאים המפורטים בהוראה 311 בנושא מיקור חוץ, התייחסות גם לנושאים המפורטים בהוראה, לרבות: קיום אפשרות חד צדדית של הלשכה להפסיק את השימוש בשירותיו של נותן שירות מחשוב הענן או לעבור לנותן שירות אחר, תוך העברת הנתונים הרלוונטיים ממערכות נותן שירות מחשוב הענן בזמן קצר ובאופן מאובטח, מחיקת המידע ממערכותיו והתחייבותו שלא יתן לאחזר

מידע זה במערכותיו; יישום הנחיות מודל האחריות המשותפת; פירוט מיקום מתקן הענן ממנו יינתן השירות ומיקום אחסון הנתונים והתחייבות נותן השירות להודיע ללשכה על שינוי בהם; גיבוי המידע והאפשרות לאחזורו (סעיף 136).

16.8. סעיף 137 בוטל.

תיקונים לאור פרסום הוראה 312 בנושא ניהול המשכיות עסקית

17. נוספו הגדרות רלוונטיות לתיקונים בנושא המשכיות עסקית (סעיף 10).
18. נוספה הבהרה לפיה התרגולים המבוצעים במסגרת תכנית ההיערכות לניהול אירועי אבטחת מידע יתבצעו כחלק מהתרגולים המפורטים בהוראה 312 בנושא המשכיות עסקית (סעיף 127א).
19. נוספו הנחיות לעניין "גיבוי ואחזור נתונים" לפיהן הלשכה נדרשת, בין היתר:
 - 19.1. לוודא כי האתר החלופי תומך בצרכי הגיבוי של הלשכה (סעיף 202).
 - 19.2. לגבות את נתוניה בעותק נוסף, על מנת להבטיח התאוששות גם במקרים בהם נפגע המידע באתר הראשי והחלופי בו זמנית (סעיף 203).
 - 19.3. לנקוט באמצעים שיבטיחו אפשרות לשחזור מידע מעותקי גיבוי ולבצע, אחת לרבעון, שחזור לגיבויים (סעיף 203א).

תיקונים נוספים

20. נוספה דרישה לפיה הדירקטוריון ידון באפקטיביות מסמך המדיניות לניהול המידע והגנתו ויקיים פיקוח על יישומו על ידי ההנהלה (סעיף 12ב).
21. תוקן מועד הדיווח מראש לממונה על אירועים או שינויים מהותיים בפעילות הלשכה ל- 60 יום מראש במקום 30 יום מראש, ונעשה עדכון לגבי נושאי הדיווח מראש לממונה (סעיף 30). בהתאם בוצע תיקון תואם בהוראה 308.
22. נוספו הבהרות בנוגע לאופן ותדירות עריכת מבחני חדירה תקופתיים וסקרי אבטחת מידע (סעיפים 38.2 ו-40).
23. בוצעו עדכוני ניסוח שונים בהוראה.

תחילה והוראות מעבר

24. תחילתם של התיקונים להוראה שישה חודשים מיום פרסום חוזר זה באתר מערכת נתוני אשראי בבנק ישראל (להלן – **יום התחילה**); ואולם, לעניין הסכם התקשרות עם נותן שירות מחשוב ענן שנכרת לפני מועד פרסום התיקונים להוראה, תחילת התיקונים להוראה במועד החידוש הקרוב של ההסכם ולא יאוחר מ-18 חודשים מיום התחילה.

25. לחזור זה מצורפת ההוראה המתוקנת.

בכבוד רב,



אייל חדד

הממונה על שיתוף בנתוני אשראי

נספח**דוח קביעת אסדרה**

שם האסדרה :	תיקון הוראת ממונה מס' 301 בנושא "ניהול המידע והגנתו", בנוגע לשירותי מחשוב ענן ונושאים נוספים
מספר חוזר באגף נתוני אשראי :	מ- 02-301
מועד פרסום אסדרה :	30.12.2024
גורם מאסדר באגף נתוני אשראי	יחידת האסדרה באגף נתוני אשראי
סוג האסדרה :	הוראת ממונה לשיתוף בנתוני אשראי
סטטוס אסדרה :	סופי
מועד תחילה :	מועד תחילת ההוראה בתום 6 חודשים מיום פרסומה באתר מערכת נתוני אשראי בבנק ישראל (להלן - "יום התחילה"); ואולם, לעניין הסכם התקשרות עם נותן שירות מחשוב ענן שנכרת לפני מועד פרסום ההוראה תחילת ההוראה במועד החידוש הקרוב של ההסכם ולא יאוחר מ 18 חודש מיום התחילה.
תחולה :	לשכות אשראי כהגדרתן בחוק נתוני אשראי, תשע"ו-2016
מקור הסמכות לקביעת האסדרה :	סעיף 68 לחוק נתוני אשראי, תשע"ו-2016
מועד פרסום דוח קביעת אסדרה :	30.12.2024

כללי

1. תיקון הוראת ממונה מס' 301 בנושא "ניהול המידע והגנתו" (להלן – "ההוראה", "הוראה 301") עוסק בעיקרו בקביעת עקרונות והנחיות לשימוש בשירותי מחשוב ענן על ידי לשכות אשראי, וזאת על מנת להבטיח ניהול מיטבי של הסיכונים הייחודיים הכרוכים בשימוש בשירותי מחשוב ענן. שירות מחשוב ענן הוא מקרה פרטי של מיקור חוץ ולפיכך חלה גם הוראה הממונה מס' 311 בנושא "מיקור חוץ" (להלן – "הוראה 311").
2. דוח קביעת אסדרה זה לא יכלול התייחסות לתיקונים בהוראה לעניין תכנית היערכות לניהול אירועי אבטחת מידע וגיבוי ושחזור נתונים שנעשו בהתאמה להוראת ממונה מס' 312 בנושא "המשכיות עסקית" לגביה נערך דוח קביעת אסדרה שפורסם בחודש יולי 2024 (במסגרת חוזר מס' מ-01-312), וכן לא יכלול התייחסות לתיקונים נוספים שאינם מהותיים שנעשו בהוראה בנושאים שאינם מחשוב ענן, וזאת לאור הפטור בסעיף 34(ג)(2) לחוק עקרונות האסדרה.

יעדי האסדרה, מטרותיה והתועלת הצפויה מקביעתה**תיאור המצב הקיים**

3. הוראה 301 במתכונתה טרם התיקון קבעה כי ניתן להעביר לסביבת ענן ציבורי רק מערכות שאינן מנהלות מידע רגיש. הדבר הגביל את לשכות האשראי המעוניינות להרחיב את השימוש בשירותי מחשוב ענן ולרתום את יתרונות מחשוב הענן לטובת פעילותן השוטפת ופיתוחן העסקי והטכנולוגי.

יעדי האסדרה

4. תיקון ההוראה נועד לאפשר ללשכות האשראי להשתמש בשירותי מחשוב ענן כחלק ממודל הפעילות העסקית שלהן, ולמצות את היתרונות הגלומים בכך עבורן, כגון השגת חיסכון בעלויות והגברת היעילות התפעולית ויכולת פיתוח עסקי.

בד בבד, תיקון ההוראה נועד להנחות את הלשכות בניהול סיכונים מיטבי ולוודא כי הלשכות עושות שימוש בשירותי מחשוב ענן תוך יישום סטנדרטים גבוהים לניהול המידע והגנתו, וזאת לאור היותן גורם משמעותי במערכת נתוני האשראי המחזיק במידע רגיש של אזרחי ישראל, ולאור האתגרים הייחודיים הנובעים משימוש בשירותי מחשוב ענן.

ביטול האיסור להעביר לסביבת הענן הציבורי מערכות המנהלות מידע רגיש, לצד קביעת דגשים והנחיות לשימוש בשירותי מחשוב ענן, הכוללים דרישות מוגברות עבור שימוש בשירותי מחשוב ענן מהותי, הינם בהלימה לצעדים דומים שננקטו על ידי רשויות רגולטוריות אחרות בישראל ובעולם.

מטרת האסדרה

5. השימוש בשירותי מחשוב ענן על ידי ארגונים פיננסיים ברחבי העולם הולך ומתרחב על רקע תהליכי דיגיטציה שהואצו בשנים האחרונות. מטרת האסדרה לאפשר ללשכות האשראי לנצל את היתרונות הגלומים בשימוש בשירותי מחשוב ענן, תוך מתן דגשים להיבטי אבטחת מידע והגנת הסייבר ומתן הנחיות לניהול מכלול הסיכונים הגלומים בשירותי מחשוב ענן, כך שתוכלנה להתמודד באופן מיטבי עם הסיכונים כאמור, תוך שמירה על האינטרסים של לקוחות, לרבות פרטיותם. תיקון ההוראה כולל הנחיות ממשל תאגידי לעניין שימוש בשירותי מחשוב ענן, שיקולים להגדרת שירות מחשוב הענן כמהותי בנוסף לשיקולים המפורטים בהוראה 311, דגשים להיבטי אבטחת מידע והגנת הסייבר בשימוש בשירותי מחשוב ענן, דרישות לניהול סיכונים ולתנאים נדרשים בהסכם עם נותן שירות מחשוב ענן, ועוד.

בעלי העניין הרלוונטיים

6. תיקון ההוראה צפוי להשפיע באופן ישיר על לשכות האשראי ולהטיל עליהן נטל רגולטורי של עמידה בדרישות ההוראה לצורך שימוש בשירותי מחשוב ענן. קביעת מסגרת עבודה לניהול סיכונים הנובעים משימוש בשירותי מחשוב ענן אמנם מטילה נטל רגולטורי מסוים על לשכות האשראי, אולם תצמצם את הסיכונים הייחודיים הנובעים משימוש בשירותים אלו, אשר התממשותם עלולה לפגוע בפעילותן העסקית ובמידע הנשמר על ידי לשכות האשראי וגם תאפשר שימוש בשירותי מחשוב ענן עבור מידע רגיש המנוהל על ידי הלשכות. תיקון ההוראה צפוי לחזק את מערך אבטחת המידע והגנת הסייבר של לשכות האשראי המבצעות שימוש בשירותי מחשוב ענן, ובכך להיטיב עם כלל הגורמים אשר נכללים באקו-סיסטם של מערכת נתוני האשראי, לרבות לקוחות האשראי הצרכני בישראל.

בחינת קיום אסדרה סותרת

7. למיטב ידיעתנו, לא קיימת אסדרה סותרת לאסדרה המפורסמת.

סקירה רגולטורית בארץ ובחו"ל

8. מאסדרים פיננסיים מובילים בארץ ובעולם פרסמו הוראות ייעודיות בנושא שימוש בשירותי מחשוב ענן. כך לדוגמה, בישראל: הפיקוח על הבנקים פרסם בחודש יוני 2022 את הוראת ניהול בנקאי תקין מס' 362 בנושא "מחשוב ענן", אשר התירה שימוש במחשוב ענן בפעילויות ליבה של הבנקים ובנוסף נקבעו בה עקרונות והנחיות לניהול סיכונים הנובעים משימוש בשירותי מחשוב ענן. בנוסף, רשות ניירות ערך קבעה בהוראתה למבקשי ובעלי רישיון למתן שירות מידע פיננסי שפורסמה בחודש מרץ 2022, דרישות החלות על גופים המבצעים שימוש בשירותי מחשוב ענן במסגרת פעילותם כנותני שירות מידע פיננסי כחלק מאסדרת הבנקאות הפתוחה בישראל. בנוסף, רשות שוק ההון התייחסה להיבטי ניהול הסיכונים הנובעים משימוש בשירותי מחשוב ענן בהוראתה בנושא "ניהול סיכוני סייבר לנותני שירותים פיננסיים" (9-10-2022) מחודש מאי 2022.

בנוסף, גופים בינלאומיים המפרסמים עקרונות והמלצות לגופים פיננסיים שונים (כגון: Basel Committee on Banking Supervision) וכן רגולטורים פיננסיים במדינות מפותחות פרסמו מדריכים והוראות לאסדרת ניהול הסיכונים הנובעים משימוש בשירותי מחשב ענן. בין היתר, ניתן למנות את הרגולטורים הבאים אשר נסקרו לצורך קביעת האסדרה: ה-Financial Conduct Authority (FCA) באנגליה אשר פרסם מדריך ייעודי בנושא מחשב ענן לגופים המפוקחים על ידו, וכן Australian Prudential Regulation Authority (APRA) באוסטרליה. האסדרה כאמור מדגישה, בין היתר, כי מחשב ענן הנו מקרה פרטי של מיקור חוץ וכוללת דגשים והנחיות לעניין האמצעים שיש לנקוט על מנת לנהל את הסיכונים הגלומים בשירותי מחשב ענן.

בנוסף, קיימת תקינה בינלאומית ענפה העוסקת בניהול סיכונים הנובעים משימוש במערכות מחשב ענן, ובין היתר ISO27017, ISO27018, NIST 800-53 וכן מטריצת הבקורות בענן של Cloud Security Alliance (The Cloud Security Alliance Cloud Control Matrix).

מהסקירה שביצענו כמפורט לעיל עולה כי רגולטורים פיננסיים בארץ ובחו"ל רואים חשיבות רבה באסדרת ניהול הסיכונים הנובעים משימוש בשירותי מחשב ענן עבור גופים פיננסיים המפוקחים על ידם. הדרישות בהוראה מבוססות על עקרונות בינלאומיים והמלצות שהתוו הגופים כאמור, תוך התאמתן לגודלן של לשכות האשראי בישראל, ותוך שקילת שיקולי מידתיות ואיזון בין הכבדת הנטל הרגולטורי לשמירה על האינטרסים של בעלי העניין השונים.

חלופות מרכזיות ונימוקים לחלופה שנבחרה

9. חלופה 0 - שימור מצב קיים

9.1. תיאור החלופה: המשך המצב הקיים ללא ביצוע תיקון ההוראה. בהתאם למצב הקיים טרם תיקון ההוראה, קיימת התייחסות מצומצמת לשירותי מחשב ענן בהוראה 301 וקיימת במסגרתה מגבלה על העברת מידע רגיש לסביבת ענן, וכן לשכות האשראי נדרשות לקבל את אישור הממונה מראש לכל שימוש בשירותי מחשב ענן.

בהתאם לחלופה זו, לא ייעשו פעולות מצד הרגולטור.

9.2. יתרונות: לא נדרשת התערבות רגולטורית, אי הטלת נטל רגולטורי חדש על הלשכות.

9.3. חסרונות: גישת הרגולטורים הפיננסיים בישראל ובמדינות מפותחות למחשב ענן השתנתה עם התפתחות הדיגיטציה מגישה שמרנית ומחמירה לגישה מקלה ומאפשרת יותר. במצב הקיים, קיימת מגבלה על לשכות האשראי להעביר מערכות המנהלות מידע רגיש לענן, ובהתאם מוגבלת יכולתן של הלשכות להפיק תועלת מהיתרונות המשמעותיים הנובעים משימוש במערכות מחשב ענן, ובפרט הפחתת עלויות והגברת היעילות התפעולית.

9.4. עלויות: לא רלוונטי.

9.5. חסמים וקשיים: לא רלוונטי.

9.6. הערכת ישימות ואפקטיביות: ישימות גבוהה. אפקטיביות נמוכה.

10. חלופה 1 – אסדרת נושא השימוש במחשב ענן

10.1. תיאור החלופה: אסדרת ניהול סיכונים הנובעים משימוש במערכות מחשב ענן על ידי לשכות האשראי במסגרת תיקון הוראה 301 בנושא ניהול המידע והגנתו, כך שתכלול עקרונות והנחיות הנוגעות לשימוש במחשב ענן על ידי הלשכות.

10.2. יתרונות: תיקון ההוראה יאפשר ללשכות האשראי להעביר מערכות ופעילויות לסביבת ענן ולהפיק תועלת מהיתרונות המשמעותיים הנובעים משימוש בשירותי מחשוב ענן, בדומה לגופים פיננסיים רבים בארץ ובעולם. קביעת עקרונות ייעודיים לתחום מחשוב ענן יאפשר ללשכות האשראי לנהל את הסיכונים הכרוכים בשימוש כאמור באופן מיטבי ולצמצם משמעותית את הסיכון לדלף מידע של לקוחות או לפגיעה בבעלי העניין השונים. בנוסף, לשכות האשראי תידרשנה לדווח מראש לממונה על כוונתן להתקשר עם נותני שירות מחשוב ענן מהותי בלבד, ולא על כל מערכת המועברת לסביבת ענן ציבורי כפי שנדרש במצב שטרם תיקון ההוראה. האסדרה מבוססת כאמור על הוראות מקבילות אצל מאסדרים פיננסיים מובילים בארץ ובעולם, כמפורט לעיל, דבר המלמד על פרקטיקה מיטבית והכרחית לניהול סיכון מחשוב ענן.

10.3. חסרונות: לשכות האשראי המעוניינות להעביר מערכות מסוימות לענן ידרשו לבצע התאמות ולעמוד בהנחיות שנקבעו לעניין ניהול הסיכונים הנובעים משימוש במערכות מבוססות ענן, ובין היתר לבצע הערכת סיכונים, מבדקי חדירה ותרגולי אבטחה ייעודיים למערכות אלו.

10.4. עלויות: העברת פעילויות לענן תהיה כרוכה בעלויות מסוימות כתוצאה מההתאמות שידרשו לצורך יישום הדרישות המפורטות בתיקון הוראה הנוגעות להיבטי אבטחת מידע והגנת הסייבר בשימוש בשירותי מחשוב ענן. יחד עם זאת, לאור החסכון הצפוי בעלויות התפעוליות של הלשכות עקב השימוש בשירותי מחשוב ענן, בטווח הארוך התועלת הכלכלית צפויה להיות גדולה מהעלויות הנלוות להעברת המערכות לענן.

10.5. חסמים וקשיים: להערכתנו לא צפויים חסמים וקשיים משמעותיים בחלופה זו. יתכנו קשיים ביישום חלק מן הדרישות הנוגעות להכללת תנאים מסויימים בהסכמי ההתקשרות של הלשכות עם נותני שירות במחשוב ענן, אולם כאמור הדרישות מבוססות על סטנדרטים בינלאומיים ונדרשות לצורך הפחתת סיכונים ומניעת דלף מידע. בנוסף לכך, לשכה שאינה מעוניינת להעביר מערכות מסוימות לסביבת הענן אינה מחויבת לעשות כן. לעניין חידוש הסכמי מחשוב ענן קיימים, ניתנה דחייה של שנה וחצי במועד התחילה בכדי לאפשר ללשכות להיערך באופן הולם. במקרים חריגים, ובהתאם לשיקול דעת הממונה הוא יהיה רשאי לפטור לשכת אשראי מקיום סעיפים בהוראה.

10.6. הערכת ישימות ואפקטיביות: ישימות גבוהה, אפקטיביות גבוהה.

11. החלופה המועדפת והנימוקים לבחירתה

11.1. החלופה המועדפת היא חלופה מס' 1 - תיקון הוראת הממונה מס' 301 בדבר "ניהול המידע והגנתו" כך שתכלול התייחסות מפורטת להיבטי מחשוב ענן.

11.2. נימוקים לבחירת החלופה: האסדרה תוכל להבטיח את יכולתן של הלשכות להעביר מערכות לסביבת הענן ובכך להביא לצמצום עלויות תוך הגברת יעילות תפעולית.

השפעות צפויות של האסדרה (ישירות ועקיפות), זמן היערכות

12. האסדרה תאפשר ללשכות האשראי לעשות שימוש בשירותי מחשוב ענן תוך ניהול מיטבי של הסיכונים הייחודיים הכרוכים בסביבה זו, וניצול היתרונות העסקיים והטכנולוגיים הנלווים לשימוש במחשוב ענן. לשכות האשראי אשר יהיו מעוניינות לעשות שימוש בשירותי מחשוב ענן יידרשו לבצע התאמות בהתאם לדרישות המפורטות בהוראה המתוקנת. קיומה של מסגרת עבודה הולמת לניהול סיכונים מחשוב ענן בקרב הלשכות תצמצם את ההסתברות לפגיעה בפעילותה התקינה של מערכת נתוני האשראי בישראל בעקבות אירועי אבטחת מידע ודלף מידע שעלולים להתרחש.

13. לצורך מתן זמן היערכות מספק ללשכות לעמידה בדרישות ההוראה המתוקנת, נקבע כי תחילתם של התיקונים להוראה הינו שישה חודשים מיום פרסומה באתר מערכת נתוני אשראי בבנק ישראל (להלן-

"יום התחילה"; וכן נקבע כי לעניין הסכם התקשרות עם נותן שירות מחשוב ענן שנכרת לפני מועד פרסום ההוראה תחילת ההוראה תהיה במועד החידוש הקרוב של ההסכם ולא יאוחר מ 18 חודש מיום התחילה.

תיאור תהליך שיתוף הציבור

14. ביום 16.7.24 התקיים דיון על טיוטת ההוראה עם חברי הוועדה המייעצת בהתאם לנדרש בסעיף 70 לחוק. פרוטוקול הוועדה מפורסם באתר מערכת נתוני אשראי שבבנק ישראל.
15. ביום 30.9.2024 פורסמה טיוטת ההוראה באתר מערכת נתוני אשראי שבבנק ישראל להערות הציבור עד ליום 10.11.2024, וכן נשלחה ללשכות האשראי לקבלת הערותיהן עד למועד כאמור.
16. לשכות האשראי העבירו את הערותיהן והתקיים עימן שיח על ההערות שהועברו. בעקבות ההערות והשיח כאמור עם הלשכות נעשו כמה שינויים בתיקון ההוראה שנועדו להבהיר את אופן היישום של הנחיות שונות בהוראה לגבי שירותי מחשוב ענן. בין היתר, הובהרו הדרישות לעניין ניטור הפעילות במחשוב ענן במערך ה-SIEM של הלשכה, אופן ניהול מפתחות ההצפנה, וגיבוי נתונים שיש ליישם בשימוש בשירותי מחשוב ענן. בנוסף, נקבע מועד תחילה מאוחר יותר לגבי הסכמים קיימים עם נותני שירות, של 18 חודש מיום התחילה במקום שנה מיום התחילה כפי שהוצע בטיטת ההוראה.

בחינה בדיעבד

17. התיקונים להוראה בעניין מחשוב הענן יבחנו בדיעבד בהתאם לדרישות חוק עקרונות האסדרה, התשפ"ב-2021 בתום תקופה של 10 שנים ממועד כניסתה לתוקף, או במועד מוקדם יותר, ככל שיעלה הצורך.