בנק ישראל

הממונה על שיתוף בנתוני אשראי

תל אביב, ח' ניסן, תשפ"ג

30 במרץ, 2023

חוזר מס' מ-301 - 01

לכבוד

<u>לשכות האשראי</u>

הנדון: <u>תיקון הוראה מספר 301 בנושא "ניהול המידע והגנתו"</u>

1. הוראה מספר 301 בנושא "ניהול המידע והגנתו" (להלן - "**ההוראה**"), החלה על לשכות אשראי, נועדה לקבוע עקרונות וכללים לניהול והגנה על נכסי המידע, באופן שתובטח שלמות המידע וזמינותו, תישמר פרטיות הלקוחות, וימוזער הסיכון לחשיפת או העברת המידע לגורמים שלא הורשו להיחשף לו.
למען הסר ספק, ההוראה אינה גורעת מהדרישות הנוספות הקבועות בהוראות הדין השונות, לרבות חוק הגנת הפרטיות, תשמ"א-1981 ותקנותיו, וכללי נתוני אשראי (אבטחת מידע), התשע"ט-2018.
2. מאז פורסמה ועודכנה ההוראה חלף זמן, במהלכו התבצעו בלשכות ביקורות לבחינת נאותות יישום ההוראה מהן עלו ממצאים ותובנות שונות.
3. לאור האמור לעיל ועל רקע איומי הסייבר המתגברים הבאים לידי ביטוי בגידול בניסיונות התקיפה על ארגונים, וכן על רקע התפתחויות בתחום אבטחת המידע, בוצעו מספר תיקונים ועדכונים להוראה אשר עיקריהם יפורטו להלן. בנוסף, בוצעו עדכוני ניסוח בהגדרות ובסעיפים שונים בהוראה, וחלק מההנחיות סווגו מחדש תחת נושאים אחרים לצורך בהירות הדרישות.

פרק ב' - פיקוח וניהול

3.1. **דירקטוריון, הנהלה וממונה אבטחת המידע**: נוספו דרישות לדירקטוריון לצורך חיזוק המעקב והפיקוח אחר ניהול המידע והגנתו בלשכה, לרבות התייחסות לתמונת המצב אודות איומי אבטחת מידע וסייבר במסגרת הדיון בחשיפות לסיכונים, וכן נקבע כי הדירקטוריון ידון בתכנית העבודה הרב שנתית שנקבעה על ידי ההנהלה ויאשר אותה, וכן ידון בתכנית היערכות לניהול אירועי אבטחת מידע. לגבי ההנהלה, נקבע כי עליה לגבש מסמך מדיניות לניהול המידע והגנתו ולבחון את הצורך לעדכנו לכל הפחות אחת לשנה וכן בכל שינוי מהותי, הודגש כי עליה לדון באופן שוטף בסיכונים העולים מפעילות הלשכה ובתמונת המצב אודות איומי אבטחת מידע וסייבר, לגבש תכנית כוללת להפחתת סיכונים, וכן נקבע כי עליה לקבוע תכנית עבודה רב שנתית ולעקוב לכל הפחות ברמה רבעונית אחר יישומה. כמו כן, עודכנו חובות החלות על ממונה אבטחת המידע. (סעיפים 11, 13, 14, 15א, 16, 16א, 20א, 24).

3.2. **דיווחים לממונה**: עודכנו חלק מדרישות הדיווח לממונה לגבי אירועים בתחום ניהול המידע והגנתו, וכן אף שבמבוא להוראה צויין כי ההוראה אינה גורעת מהדרישות הנוספות הקבועות בהוראות הדין השונות, נוספה הבהרה לפיה דיווח לממונה אינו גורע מחובת דיווח לגורמים אחרים על פי דין, לרבות דיווח לרשות להגנת הפרטיות בהתאם לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (סעיפים 27, 28 ו- 29).

פרק ג' – הגנת המידע

3.3. **מסגרת עבודה לניהול הגנת המידע:** נוספו דרישות לפיהן מסגרת העבודה לניהול הגנת המידע תכלול תהליך שוטף של זיהוי המידע הקיים ומיפוי מערכות המידע בהן הוא מאוחסן, פירוט אופן זרימת המידע בין המערכות השונות ומיפוי ערוצי התקשורת של הלשכה עם לקוחותיה ("Data Discovery"), וכן סיווג המידע לקטגוריות ("Data Classification"), כגון: מידע אישי רגיש, מידע אישי אחר, מידע עסקי רגיש, מידע פומבי (סעיף 32.5).

3.4. **סקר הערכת סיכוני אבטחת מידע ומבחני חדירה:** עודכנה הדרישה לתדירות ביצוע הסקרים עבור מערכות שאין אליהן גישה מרשת ציבורית, כך שלא תפחת מאחת ל- 18 חודשים, במקום כל 24 חודשים. כמו כן, עודכנה הדרישה לעריכת סקרים אצל ספקי מיקור חוץ, כך שתחול על כל ספק מיקור חוץ שיש לו גישה למערכות הלשכה (סעיפים 40 ו- 44).

3.5. **איסוף מודיעין:** נוסף נושא חדש – "איסוף מודיעין" אשר לפיו, בין היתר, נדרש לאסוף ולנתח מידע רלוונטי ממקורות פנימיים וחיצוניים (כגון מערך הסייבר הלאומי), לבצע מעקב אחר איומי סייבר משמעותיים בישראל ובעולם, לבסס תמונת מצב ולנקוט צעדים בהתאם (סעיפים 44א ו-44ב).

3.6. **בקרה וניטור:** נוספו הדרישות שלהלן:

3.6.1. הטמעת תהליכי בקרה וניטור על ניסיונות לביצוע שינויים במידע, כחלק ממערך ה SIEM.

3.6.2. הגדרת מתודולוגיה לסיווג התראות המתקבלות ממערך ה-SIEM לפי רמות חומרה, תוך הגדרת שלבי הטיפול שיש לבצע בהתאם לכל רמת חומרה.

3.6.3. הטמעת כללים ייעודיים והתראות במערך ה-SIEM לזיהוי אנומליה או פעילות חריגה עבור מכשירים ניידים.

3.6.4. עריכת תהליכי טיוב של הכללים שהוגדרו במערכות הבקרה והניטור עם כל שינוי מהותי במערכות המידע ובשירותים הניתנים על ידי הלשכה, ולכל הפחות אחת לשנה.

(סעיפים 48, 48א, 48ב, 50א).

3.7. **תהליכי פיתוח, תחזוקה וניהול שינויים:** הובהר כי תהליכי הפיתוח בלשכה יתבצעו באופן מאובטח (SSDLC), ועודכנו השלבים והפעולות לביצוע פיתוח מאובטח. בין היתר, נוסף שלב חדש שעניינו "עיצוב מערכת" הכולל אפיון דרישות למנגנוני הגנה וזיהוי נקודות תורפה במטרה לצמצם את משטח התקיפה, וכן נוספה דרישה להכנת תכנית חזרה לאחור בשלב קליטת המערכת. בנוסף, נקבע כי בעת ביצוע פעילות תחזוקה וניהול שינויים, יש לבחון, בין השאר, את שלבי הפיתוח המאובטח הרלוונטיים לפעילות (סעיפים 51 עד 53).

3.8. **אבטחת רשת וגישה מרחוק:** נקבע כי גישה לרשת הגיבוי תבוצע, לכל הפחות, באותם אמצעי זיהוי המשמשים לגישה לרשת הלשכה. כמו כן, נוספה דרישה לביצוע סריקת חולשות אבטחה במערכות המידע ובתשתיות הלשכה לפחות אחת לרבעון, וטיפול נאות בממצאים בהתאם לרמת הסיכון (סעיפים 59 ו- 61א).

3.9. **מניעת דלף מידע ואבדן מידע:** נוסף נושא חדש "מניעת דלף מידע ואבדן מידע". בין היתר, נכללה דרישה שהלשכה תגדיר כללים למניעת דלף מידע ואבדן מידע, ובהתאם לכך תטמיע כלים טכנולוגיים, תהליכים ובקרות רלוונטיים, ותנקוט פעולות להעלאת מודעות העובדים. כללים אלה כוללים דרישות חדשות שלא הופיעו עד כה בהוראה, לדוגמה: יישום בקרות מתאימות למניעת דלף מידע ואובדן מידע, כגון: הטמעת התראות או חסימות על ניסיונות להעברת או הוצאת מידע רגיש, לצד דרישות שהופיעו בהוראה תחת נושאים אחרים ואוגדו כעת תחת נושא זה (לדוגמה, הדרישה לקביעת אופן הוצאת נתונים

אל מחוץ לחצרות הלשכה בהתאם לרמת רגישותם והגדרת תהליכי הגנה הכרחיים להעברת מידע כאמור) (סעיפים 67א עד 167).

3.10. **הצפנת נתונים:** עודכנה הדרישה להצפנת מידע בתווך, ונוספה דרישה להצפנה במנוחה של נתוני אשראי וכן מידע אחר הנכלל בסעיף 1(3)(ז) ו- 1(3)(ח) בתוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, בבסיס הנתונים (מיד עם כניסת הנתונים לבסיס הנתונים) ובקלטות הגיבוי (סעיף 72א).

3.11. **אבטחת מערכות ועדכונן:** הדרישות בנושא זה עודכנו. בין היתר, נוספה דרישה להגדרת מדיניות לביצוע עדכוני אבטחת מידע ולזיהוי, דירוג ותיקון פרצות אבטחה, אשר תכלול, בין השאר: דירוג חולשות האבטחה שאותרו לפי סדר עדיפות ולוחות זמנים לתיקון, על סמך ציון מקובל לפגיעות והרלוונטיות של הפגיעות ללשכה. כמו כן, נוספה דרישה כי התקני קצה וכן תוכנות חדשות יהיו מותקנים במלואם, לרבות עדכוני אבטחה אחרונים, לפני חיבורם לרשת הארגונית (סעיפים 76 עד 78ד).

3.12. **מניעת קוד עוין:** הדרישות בנושא זה חודדו, ובמסגרת זו הובהר כי ככלל, יש לחסום אפשרות לחיבור התקן זיכרון חיצוני (לרבות USB, DISC ON KEY וכיו"ב) למחשבי הארגון, וכי במקרים בהם יוחלט שקיימת הצדקה עסקית לחיבור התקן זיכרון חיצוני כאמור, יש לקיים מנגנוני הגנה ובקרה אפקטיביים שימנעו דלף מידע או החדרת קוד עוין, בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן זיכרון חיצוני באותם מחשבים וכמפורט בהוראה (סעיף 87).

3.13. **שימוש במכשירים ניידים:** נוסף נושא חדש "שימוש במכשירים ניידים". חלק מהדרישות בנושא זה מתייחסות לכלל המכשירים הניידים (לדוגמה, גיבוש מדיניות ארגונית לשימוש במכשירים ניידים), וחלקן מיועדות למכשירים ניידים שאינם מוגדרים ברשת הארגונית של הלשכה, ולאור זאת קיימת חשיבות לקבוע עבורם בקרות ייעודיות לצמצום הסיכונים, כמפורט בהוראה (סעיף 87א).

3.14. **ניהול משתמשים:** מספר דרישות תחת נושא זה עודכנו. בין היתר, נוספה דרישת תיעוד, ניטור ובקרה אחר משתמשים באופן שוטף וחקירת אנומליות או חריגות, וכן נוספו הנחיות ייעודיות לגבי ניהול חשבונות משתמשים בעלי הרשאות חזקות. כמו כן, התווספה דרישה להגדרת אופן נעילת חשבון משתמש גם במקרה של מספר ניסיונות חיבור כושלים ולא רק בעת אי שימוש בחשבון במשך תקופה ממושכת (סעיפים 95 עד 101).

3.15. **סיסמאות ואמצעי הזדהות:** מספר דרישות בנושא זה חודדו. בין היתר, נוספה דרישה להגדרת כללים לניהול סיסמאות ואמצעי הזדהות, שיכללו בין היתר התייחסות לאורך הסיסמה, מידת מורכבותה ותדירות החלפתה, נקבע כי סיסמאות עבור כל סוגי המשתמשים יוחלפו בתדירות של אחת ל-90 יום לפחות, וכן נקבע כי משתמשים בעלי הרשאות חזקות יבצעו הזדהות באמצעות תהליך Multi-Factor Authentication (MFA) (סעיפים 107 ו-111).

3.16. **ניהול הרשאות ובקרת גישה:** עודכנה הדרישה לפיה תיושם בפרופילי הרשאות המשתמשים הפרדת סמכויות, לרבות מניעת גישה של עובד פיתוח לסביבת הייצור, למעט הרשאות צפייה ולמעט במקרים חריגים לצורך טיפול בתקלות בסביבת הייצור, בהתאם לתנאים המפורטים בסעיף. כמו כן, נוספה דרישה לזיהוי ואימות משתמשים במערכות בסיכון גבוה ובגישה מרחוק תוך שימוש בתהליך Multi-Factor Authentication (MFA) (סעיפים 113א ו-115).

3.17. **תכנית היערכות לניהול אירועי אבטחת מידע:** נוספה הבהרה לעניין תכולת התרגול השנתי לתכנית ההיערכות לניהול אירועי אבטחת מידע, כך שהנ"ל יכלול הן תרגול עיוני אסטרטגי והן תרגיל מעשי (סעיף 127).

3.18. **מיקור חוץ:** ההבהרה לפיה "אין בהנחיות לגבי מיקור חוץ בכדי לגרוע מאחריות הלשכה לכל פעולה הנעשית מטעמה או בהסכמתה ע"י אחרים" הועברה מנושא שירותי מחשוב ענן לנושא מיקור חוץ, בשינויי נוסח קלים, מאחר שהבהרה זו הינה רלוונטית לכלל הפעילויות שבמיקור חוץ, ולא רק למחשוב ענן (סעיף 130א).
בהקשר זה יצוין כי הממונה נמצא בתהליך גיבוש טיוטת הוראה ללשכות אשראי בנושא סיכונים תפעוליים וטכנולוגיים, אשר תסדיר, בין היתר, את הנושאים הבאים: מיקור חוץ, מחשוב ענן והמשכיות עסקית.

פרק ו' – פעילות בערוצי תקשורת

3.19. **בקרות בתהליך הרישום לביצוע פעולות:** נוספה דרישה ליישום אמצעים למניעת התקפות על ערוצי תקשורת (כגון ניחוש שמות משתמשים, ניחוש סיסמאות וכיו"ב) (סעיף 173).

3.20. **מסירת מידע באמצעים דיגיטליים:** נוספה דרישה כי דוח ריכוז נתונים הנמסר ללקוח באמצעים דיגיטליים יוגן בסיסמה (סעיף 192).

פרק ז' – תיעוד, מחיקה, איחזור וגיבוי המידע, והפסקת פעילות לשכה

3.21. **תיעוד:** עודכנו הדרישות לתיעוד פניות לקוחות, וכן מסמכים הקשורים לפעילות הלשכה, לרבות מדיניות, תכנית היערכות לניהול אירועי אבטחת מידע ואופן הטיפול באירועי אבטחת מידע, הערכות סיכונים, דוחות ביקורת ותכניות עבודה וטיפול בליקויים שזוהו בדוחות הביקורת כך שישמרו לתקופה שלא תפחת מ-7 שנים. כמו כן, נוספה דרישה לשמירה ותיעוד תהליכי בקרה ופעולות שהלשכה מבצעת לצורך יישום הנחיות ההוראה, וכן נתוני אירועי אבטחת מידע ותקלות שמעלות חשד לאירועי אבטחת מידע, למשך תקופה של 24 חודש לפחות (סעיפים 193.1, 193.2, 193.5, 194.1).

4. בהתאמה לתיקונים בנושא דיווחים לממונה (כמפורט בסעיף 3.2 לעיל), בוצעו תיקונים בהוראת ממונה מספר 308 בנושא "הוראת דיווח ללשכות אשראי" (בסעיף 14.2) ובהוראת ממונה מספר 308A בנושא "נספחים להוראות דיווח ללשכות אשראי" (בנספח 9), כמפורט בחוזר מספר מ-308-02/מ-308A-02.

5. מצורפת לחוזר זה ההוראה המעודכנת.

תחילה

6. תחילת התיקונים להוראה 6 חודשים מיום פרסום חוזר זה באתר האינטרנט של מערכת נתוני אשראי בבנק ישראל; ואולם, התיקון לסעיפים 27 ו- 28 להוראה, כמפורט בסעיף 3.2 לעיל, בנוגע לדרישות הדיווח לממונה לגבי אירועים בתחום ניהול המידע והגנתו, יחל ביום פרסום החוזר כאמור.

בכבוד רב,

אייל חדד

הממונה על שיתוף בנתוני אשראי