בנק ישראל

הממונה על שיתוף בנתוני אשראי

מערכת נתוני אשראי
של בנק ישראל

תל אביב, א׳ אייר, תשפ״ה
29 באפריל, 2025
חוזר מס׳ מ-407-01

<u>טיוטה להערות הציבור</u>

הערות ניתן להעביר עד ליום 20 במאי 2025

באמצעות תיבת הדוא״ל: CCR-REG@BOI.ORG.IL

לכבוד,

<u>המשתמשים בנתוני אשראי</u>

הנדון: **<u>הוראה מס׳ 407 בנושא ״שימוש במערכת נתוני אשראי״</u>**

מבוא

1. השימוש במערכת נתוני אשראי מהווה נדבך חשוב בניהול סיכוני האשראי על ידי המשתמשים בנתוני אשראי, אולם כרוך בסיכונים שונים וביניהם: סיכונים תפעוליים, סיכוני אבטחת מידע סיכוני פגיעה בפרטיות, סיכוני ציות וסיכוני מוניטין. חוק נתוני אשראי, התשע״ו-2016 (להלן - **החוק**), הכללים והתקנות מכוחו וכן הוראות הממונה על שיתוף בנתוני אשראי (להלן - **הממונה**) מפרטים את חובות המשתמשים בנתוני אשראי בנוגע לשימוש במערכת נתוני אשראי, לרבות אופן השימוש במידע שמקורו במאגר נתוני אשראי. לפיכך, משתמש בנתוני אשראי נדרש להסדיר שימוש נאות במערכת נתוני אשראי לפי החוק במטרה לצמצם את החשיפה לסיכונים כאמור, ותוך מתן דגש לשמירה על עניינם של הלקוחות והגנה על פרטיותם.

2. על רקע האמור, וכדי לשמור על התפעול התקין של מערכת נתוני אשראי, מוצעת הוראת ממונה מס׳ 407 בנושא ״שימוש במערכת נתוני אשראי״ המצורפת לחוזר זה (להלן - **ההוראה**). ההוראה המוצעת קובעת מסגרת עבודה למשתמשים בנתוני אשראי לשימוש נאות במערכת נתוני אשראי, לרבות הסדרת מנגנונים לזיהוי, טיפול ודיווח על אירועים של שימוש במערכת נתוני אשראי שלא לפי החוק או על אירועי אבטחת מידע הקשורים לשימוש במערכת נתוני אשראי (להלן - **אירועים חריגים**). יודגש כי אירועי אבטחת מידע כוללים, בין השאר, אירועי מתקפת סייבר.

3. ההוראה המוצעת מפרטת, בין השאר: הנחיות לדירקטוריון משתמש בנתוני אשראי להתוויית מדיניות לשימוש נאות במערכת נתוני אשראי; הנחיות להנהלת משתמש בנתוני אשראי להסדרת נהלי עבודה בנושא וכן לקביעת תהליכי פיקוח ובקרה לשימוש נאות במערכת נתוני אשראי, לרבות מנגנונים לזיהוי, וטיפול באירועים חריגים ודיווחם להנהלה ולדירקטוריון בהתאם למדיניות שקבע.
כמו כן, ההוראה המוצעת קובעת חובת דיווח לממונה על אירועים חריגים משמעותיים. מטרות הדיווח לממונה על אירועים כאמור הן לאפשר לממונה לוודא כי משתמש בנתוני אשראי אצלו מתרחש האירוע,

מנהל את האירוע באופן תקין ומבצע את הפעולות הנדרשות לצמצום הסיכונים והחשיפות ולמניעת הישנות אירועים מסוג זה, וכן, לאפשר לממונה לקבל תמונת מצב עדכנית על מנת להעריך האם עליו לנקוט בפעולות מסוימות לשמירה על המשך תפעולה התקין של מערכת נתוני אשראי או לשיפור עמידות המשתמשים בנתוני אשראי להתמודדות עם אירועים מסוג זה בעתיד.

4. מובהר כי החל ממועד תחילת ההוראה המוצעת, משתמש בנתוני אשראי ידווח על אירועים חריגים, לרבות על אירועי אבטחת מידע וסייבר הקשורים להליכי זיהוי לקוח או על חשד ממשי לאירועים כאמור, על פי הוראה זו ולא על פי הוראות הממונה מס' 401 בנושא "אמצעי זיהוי" ומס' 401A בנושא "אמצעי זיהוי מרחוק" (להלן בהתאמה – **הוראה 401, הוראה 401A**). בהתאם לאמור, מוצעים תיקונים להוראה 401 ולהוראה 401A (פירוט התיקונים בחוזר הממונה מס' מ-04-401/ מ-04-401A).

5. מובהר כי ההוראה המוצעת קובעת דרישות נוספות על אלה הקבועות בהוראות כל דין, לרבות חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו, ואינה גורעת מהן.

6. האסדרה תלווה בפרסום דוח קביעת אסדרה לפי חוק עקרונות האסדרה, תשפ"ד-2021 (להלן - **חוק עקרונות האסדרה**), אשר יצורף לחוזר של ההוראה הסופית כנספח.

7. בחינה ראשונה של אסדרה זו לפי סעיף 36 לחוק עקרונות האסדרה תתבצע בתום תקופה של 10 שנים מיום תחילתה או במועד מוקדם יותר, ככל שיעלה הצורך.

8. להלן פירוט עיקרי הסעיפים בהוראה המוצעת:

פרק א' - כללי והגדרות

9. פרק א' כולל: מבוא, תחולה, והגדרות (סעיפים 1-7).

פרק ב' - ממשל תאגידי

10. פרק ב' כולל דרישות בנושא ממשל תאגידי שיחולו על הדירקטוריון ועל ההנהלה. דרישות אלו נועדו להבטיח גיבוש והטמעת מדיניות ותהליכי עבודה סדורים אצל משתמש בנתוני אשראי לנושא שימוש נאות במערכת נתוני אשראי. בפרק נכללות, בין היתר, הדרישות שלהלן:

10.1. הדירקטוריון נדרש להתוות ולאשר את מדיניות השימוש במערכת נתוני אשראי, וכן לוודא את יישומה על ידי ההנהלה, וכן לוודא כי הוקצו משאבים נאותים לצורך יישום המדיניות. במסמך המדיניות לשימוש במערכת נתוני אשראי נדרש להתייחס לנושאים המפורטים בהוראה (סעיפים 8.1-8.3), ובכללם:

10.1.1. פירוט הסיכונים הגלומים בשימוש במערכת נתוני אשראי. לתהליך מיפוי וזיהוי הסיכונים כאמור קיימת חשיבות רבה מאחר שעל בסיסו ניתן לקבוע שימוש הולם במערכת נתוני אשראי ואמצעי פיקוח ובקרה אפקטיביים, וזאת לצורך הפחתת הסיכונים.

10.1.2. חובת קיום נהלי עבודה סדורים לשימוש נאות במערכת נתוני אשראי לפי החוק לצמצום הסיכונים הגלומים בשימוש במערכת נתוני אשראי, ובין השאר, לצורך שמירה על עניינם של הלקוחות והגנה על פרטיותם.

10.1.3. קביעת אמצעי פיקוח ובקרה נאותים, לרבות מנגנונים לזיהוי ואיתור אירועים חריגים, וקיום תהליך סדור לטיפול וניהול אירועים חריגים, לרבות תחקור של נסיבות האירוע והפקת לקחים.

10.1.4. קביעת אירועים חריגים אשר נדרש לדווחם לדירקטוריון כדיווח מידי, דיווח משלים או דיווח תקופתי, והפעולות שננקטו על ידי ההנהלה לצמצום הפגיעה בלקוחות ולמניעת הישנות אירועים כאמור. על הדירקטוריון מוטלת האחריות לוודא כי ההנהלה מנהלת את האירוע החריג באופן ראוי ונוקטת בפעולות ובצעדים הנדרשים לצמצום הסיכונים השונים ולצמצום הפגיעה בלקוחות ולשם כך הוא נדרש לדיווחים על אירועים חריגים.
החלטת הדירקטוריון על סוגי האירועים המחויבים לדיווח תתבסס, בין השאר, על השיקולים כמפורט בהוראה ובהם היקף הפגיעה במידע, בתהליכים או בלקוחות, לרבות פגיעה פוטנציאלית, משך האירוע, היקף השיבוש בפעילות הקשורה למערכת נתוני אשראי ומידת הנזק.

10.1.5. אירועים חריגים המחויבים בדיווח לממונה לפי ההוראה, וכן אירועים נוספים לדיווח לממונה לפי שיקול דעת הדירקטוריון.

10.2. ההנהלה נדרשת לגבש את המדיניות ולבחון את הצורך בעדכונה במועדים המפורטים בהוראה (סעיף 9.1).

10.3. ההנהלה תמנה גורם בדרג של חבר הנהלה או מקבילה אחרת שיהיה אחראי להסדרת השימוש הנאות במערכת נתוני אשראי. ה"אחראי שימוש במערכת נתוני אשראי" יכול להיות אותו הגורם ה"אחראי למידע" שמשתמש בנתוני אשראי נדרש למנות על פי הוראת ממונה מס' 501 בנושא "איסוף מידע ודיווח" (סעיף 9.2).

10.4. ההנהלה נדרשת להגדיר נהלי עבודה ולוודא את האפקטיביות שלהם. נהלי העבודה יסדירו, בין היתר, את הנושאים הבאים (סעיף 9.3):

10.4.1. תנאי השימוש ואופן השימוש במערכת נתוני אשראי לפי החוק;

10.4.2. פירוט הגורמים בעלי הגישה לנתוני אשראי, ופירוט הפעולות הנדרשות בהתייחס לערוצי הפעילות השונים (לדוגמה: באמצעים דיגיטליים או בשירות פנים אל פנים), וסוגי עסקאות האשראי, ובהתאם לממשקי הפעילות אל מול לשכות האשראי (לדוגמה: ממשק ממוכן או ידני);

10.4.3. קביעת מנגנוני פיקוח ובקרה לזיהוי ואיתור אירועים חריגים, או פוטנציאל להתממשות אירועים כאמור, ובכלל זאת האמצעים הטכנולוגיים באמצעותם ניתן לאתר אירועים כאמור;

10.4.4. הנחיות לתהליך סדור לטיפול וניהול אירועים חריגים אשר יאפשר למשתמש בנתוני אשראי להמשיך או לחדש את פעילותו באופן מאובטח לפי החוק, לרבות זיהוי לקוחות שנפגעו ונקיטת פעולות לצמצום הפגיעה בהם;

10.4.5. תיעוד כלל האירועים החריגים, וכן דיווחים נדרשים להנהלה ולדירקטוריון בהתאם למדיניות שקבע, ולממונה בהתאם להוראה;

10.4.6. תהליכי תחקור והפקת לקחים מאירועים חריגים שאירעו, לרבות בחינה מחדש של מנגנוני הבקרה.

פרק ג' - דיווחים לממונה

פרק ג' כולל דרישות דיווח לממונה כמפורט להלן:

11. דיווח לממונה על פרטי הגורם שמונה כאחראי לשימוש במערכת נתוני אשראי, בהתאם לסעיף 9.2 בהוראה, וכן דיווח לממונה בכל מקרה בו האחראי לשימוש במערכת נתוני אשראי חדל למלא את תפקידו (סעיף 10).

12. דיווח לממונה על אירוע חריג משמעותי או על חשד ממשי לאירוע כאמור, לרבות אירוע הקשור להליכי זיהוי לקוח, בהתאם לסוגי האירועים המפורטים בהוראה (להלן – **אירוע חריג מחייב דיווח**) (סעיף 11.1). קיימת חשיבות רבה לכך שאירועים חריגים הקשורים למערכת נתוני אשראי ידווחו לממונה בשל אחריותו ליציבותה ותפקודה התקין של מערכת נתוני אשראי מתוקף חוק נתוני אשראי, ומאחר שלאירועים כאמור יכולה להיות השפעה על שאר משתתפי המערכת.

12.1. אירוע בו נעשה שימוש במערכת נתוני אשראי שלא לפי החוק, וקשור לקבוצת לקוחות. לדוגמה: הפקת דוח אשראי ללא הסכמת לקוח בהתייחס לקבוצת לקוחות, הפקת חיווי ללא יידוע לקוח בהתייחס לקבוצת לקוחות;

12.2. אירוע בו נעשה שימוש במידע ממערכת נתוני אשראי, בלא הרשאה או בחריגה מהרשאה, וקשור לקבוצת לקוחות. לדוגמה: הפקת דוח אשראי או חיווי על קבוצת לקוחות על ידי עובד של משתמש בנתוני אשראי שאינו מורשה לכך;

12.3. אינדיקציות לכך שמידע אודות קבוצת לקוחות שמקורו במאגר נתוני אשראי נחשף בחריגה מהרשאה, דלף, שובש או נמחק. לדוגמה: דליפת נתוני לקוחות בעקבות מתקפת סייבר;

12.4. אירוע שגרם לשיבוש או השבתה של פעילות או מערכות מידע או מערכות תפעוליות הקשורות באופן ישיר למערכת נתוני אשראי ליותר מ-3 שעות, למעט השבתה יזומה. לדוגמה: שדרוג או עדכון המערכת המשמשת להפקת דוחות אשראי שהביא להשבתתה;

12.5. אירוע בו נעשה שימוש במערכת נתוני אשראי אשר הטיפול בו דורש מעורבות משמעותית של הממונה על אבטחת מידע והגנת הסייבר או הגורם האמון על נושא זה אצל משתמש בנתוני אשראי, ואשר הטיפול בו לא הסתיים תוך שעתיים ממועד זיהויו לראשונה;

12.6. אירוע במערכות מידע או במערכות תפעוליות, לרבות ניסיונות מהותיים של חדירה ותקיפה או אירוע שהינו בעל מאפייני תקיפה חדשים או רמת מורכבות גבוהה, אשר יכולה להיות לו השפעה מהותית על השימוש במערכת נתוני אשראי;

12.7. כל אירוע אחר שהתרחש בעל השפעה מהותית על השימוש התקין במערכת נתוני אשראי;

12.8. כל אירוע אשר דווח למאסדר אחר וקשור למערכת נתוני אשראי;

12.9. כל אירוע כמפורט בסעיפים 11.1.1-11.1.7 להוראה שכמעט והתרחש.

במונח "קבוצת לקוחות" אשר נכלל בסעיפים 11.1.1-11.1.3 להוראה, הכוונה לעשרה לקוחות ומעלה באירוע בודד או בכמה אירועים שקרו בנסיבות דומות. כלומר, יש להתייחס לכמה אירועים שיש ביניהם קשר מבחינת נסיבות האירוע או הגורמים שבגינם קרה האירוע, כ"אירוע חריג מחייב דיווח", גם אם כל אחד מהם קשור לפחות מעשרה לקוחות אולם בסך הכול קשורים ליותר מעשרה לקוחות.

13. הדיווח לממונה על אירועים חריגים יבוצע בהתאם לסוגי הדיווחים ולהנחיות כמפורט בהוראה המוצעת (סעיף 11.2).

14. בהתייחס לדיווחים בכתב על אירוע חריג מחייב דיווח, משתמש בנתוני אשראי רשאי לעשות שימוש בפורמט הדיווח על אירועי אבטחת מידע וסייבר שקבע מאסדר של משתמש בנתוני אשראי. הפורמטים שניתן להשתמש בהם לדיווח לממונה הם כדלהלן: פורמט הדיווח על אירועי כשל טכנולוגי ואירועי סייבר שנכלל

בהוראת ניהול בנקאי תקין מס' 366 של המפקח על הבנקים אשר חלה על תאגידים בנקאיים ; פורמט הדיווח על אירועי סייבר וכשל טכנולוגי שנכלל בחוזר 2022-9-15 של הממונה על שוק ההון ביטוח וחסכון, אשר חל על גופים מוסדיים. הדיווח לממונה בפורמט של מאסדר אחר כאמור הינו בכפוף לכך שהעברתם לממונה תהיה בהתאם למפורט בהוראה, לרבות לעניין האירועים החריגים המחייבים דיווח וכן, זמני הדיווח הנדרשים (סעיף 11.2.6).

פרק ד' – הביקורת הפנימית

15. בפרק ד' נקבע כי הביקורת הפנימית של משתמש בנתוני אשראי, לרבות גורם מיקור חוץ הפועל מטעמה, תבצע ביקורות לבחינת מסגרת העבודה לשימוש במערכת נתוני אשראי ואופן יישומה בהתאם להוראה זו, בתדירות אשר תיקבע על ידי הדירקטוריון ולכל הפחות אחת לשלוש שנים (סעיף 12).

תחילה

16. תחילתה של ההוראה המוצעת שלושה חודשים מיום פרסומה באתר מערכת נתוני אשראי בבנק ישראל (סעיף 13).

כללי

17. לטיוטת חוזר זה מצורפת טיוטת הוראה.

בכבוד רב,

אייל חדד

הממונה על שיתוף בנתוני אשראי