שימוש במערכת נתוני אשראי

פרק א' - כללי

מבוא

1. 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 האשראי, לרבות אופן השימוש במידע שמקורו ממאגר נתוני אשראי. שימוש במערכת נתוני אשראי כרוך בסיכונים שונים וביניהם: סיכונים תפעוליים, סיכוני אבטחת מידע והגנת הפרטיות, סיכוני ציות וסיכוני מוניטין, ולפיכך משתמש בנתוני אשראי נדרש להסדיר את השימוש הנאות במערכת נתוני אשראי לפי החוק, ובמטרה לצמצם את החשיפה לסיכונים אלו.
2. מתוקף סמכותי לפי סעיף 68 לחוק ולאחר התייעצות בוועדה המייעצת הריני קובע הוראה זו, המסדירה מסגרת עבודה למשתמשים בנתוני אשראי לשימוש נאות במערכת נתוני אשראי, וזאת לצורך שמירה על עניינם של הלקוחות והגנה על פרטיותם ושמירה על התפעול התקין של מערכת נתוני אשראי.
3. למען הסר ספק, הוראה זו קובעת דרישות נוספות על אלה הקבועות בהוראות כל דין ואינה גורעת מהן, לרבות חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו.
4. למונחים הקבועים בהוראה זו תהיה המשמעות הקבועה בחוק, בהתאם לעניין, אלא אם כן נקבע אחרת בהוראה זו.

תחולה

5. הוראה זו חלה על משתמשים בנתוני אשראי.
6. הממונה רשאי לפטור משתמש בנתוני אשראי מסוים מקיום סעיפים מסוימים בהוראה זו או לקבוע הוראות מסוימות שונות מאלו המפורטות להלן אשר יחולו על משתמש בנתוני אשראי מסוים. זאת, במקרים חריגים לאחר שבחן את בקשתו ונימוקיו, אשר נמסרו לו בכתב, ורשאי הממונה לקבוע כי הפטור או ההוראות השונות יחולו לתקופה קצובה, כפי שתיקבע על ידו.

הגדרות

7. בהוראה זו –

"אבטחת מידע" - אבטחה והגנה על סודיות (Confidentiality), שלמות (Integrity), או זמינות (Availability) של מידע, לרבות אבטחה והגנה מפני תקיפת סייבר, וכן הגנה על מידע מפני עיבוד ללא רשות כדין;

"אירוע אבטחת מידע" - אירוע שבו נפגעה אבטחת המידע;

"אירוע חריג" - אחד מסוגי האירועים המפורטים להלן:

1) אירוע של שימוש במערכת נתוני אשראי שלא לפי החוק;

2) אירוע אבטחת מידע הקשור לשימוש במערכת נתוני אשראי;

"זמינות" - נגישות ואפשרות לשימוש במידת הצורך;

"יום עסקים" - ימים א'-ה', למעט: ימי שבתון, שני ימי ראש השנה, ערב יום כיפור ויום כיפור, ראשון של סוכות ושמיני עצרת, פורים, ראשון ושביעי של פסח, יום העצמאות, חג השבועות ותשעה באב;

"מאסדר של משתמש בנתוני אשראי" - כמפורט להלן, לפי העניין:

(1) לעניין תאגיד בנקאי - המפקח על הבנקים;

(2) לעניין גוף מוסדי כהגדרתו בחוק הפיקוח על שירותים פיננסיים (ביטוח), התשמ"א-1981 - הממונה על שוק ההון, ביטוח וחיסכון;

(3) לעניין בעל רישיון למתן שירותי פיקדון ואשראי, בעל רישיון למתן אשראי ובעל רישיון להפעלת מערכת לתיווך אשראי כמשמעותם בחוק הפיקוח על שירותים פיננסיים (שירותים פיננסיים מוסדרים), התשע"ו-2016 - המפקח על נותני שירותים פיננסיים;

"מידע ממערכת נתוני אשראי" - נתוני אשראי אשר התקבלו ממערכת נתוני אשראי או דירוג אשראי אשר נקבע לפי סעיף 13 (1) לחוק;

"סודיות" - גישה מוגבלת למורשים בלבד;

"עיבוד מידע", "שימוש במידע" - כל פעולה המבוצעת על מידע, לרבות קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילויו, חשיפתו, העברתו, מסירתו או מתן גישה אליו;

"קבוצת לקוחות" - קבוצה של לקוחות הקשורים לאירוע בודד שהתרחש ביחס אליהם או לכמה אירועים נפרדים שהתרחשו ביחס אליהם בנסיבות דומות.
היקף הלקוחות בקבוצת לקוחות ייקבע על פי הנמוך מבין שני אלה:

(1) כפי שיוגדר על ידי המשתמש בנתוני אשראי, בהתייחס לגודלו ולמספר לקוחותיו;

(2) 50 לקוחות;

"שימוש במערכת נתוני אשראי"	-	שימוש במערכות המידע ובמערכות התפעוליות שבאמצעותן מתקבל המידע ממערכת נתוני אשראי, וכן שימוש במידע ממערכת נתוני אשראי;
"שלמות"	-	דיוק, מהימנות והגנה מפני שינוי או מחיקה בלתי מורשים;
"שעות עבודה מקובלות"	-	ימים א'-ה' שהינם ימי עסקים, בין השעות 8:00 ל-18:00.
"תאגיד בנקאי"	-	כהגדרתו בחוק הבנקאות (שירות ללקוח), התשמ"א- 1981.

פרק ב' – ממשל תאגידי

8. **דירקטוריון משתמש בנתוני אשראי**

8.1. הדירקטוריון יתווה ויאשר מדיניות לשימוש נאות במערכת נתוני אשראי (להלן – **מדיניות שימוש במערכת נתוני אשראי** או **המדיניות**), לפחות אחת לשנתיים, וכן בעת ביצוע שינוי מהותי בסביבה הטכנולוגית או בחשיפה לסיכונים לרבות בשל התרחשות אירוע חריג משמעותי.

8.2. מסמך המדיניות יכלול, בין היתר, התייחסות לנושאים הבאים:

8.2.1. פירוט של הסיכונים הגלומים בשימוש במערכת נתוני אשראי, ובכלל זה: סיכונים תפעוליים, סיכוני אבטחת מידע לרבות דלף מידע, סיכוני פגיעה בפרטיות, סיכוני ציות וסיכוני מוניטין;

8.2.2. חובת קיומם של נהלי עבודה סדורים לשימוש נאות במערכת נתוני אשראי לפי החוק, במטרה לצמצם את הסיכונים הגלומים בשימוש במערכת נתוני אשראי ובין השאר, לצורך שמירה על עניינם של הלקוחות והגנה על פרטיותם;

8.2.3. חובת קיומם של מנגנוני פיקוח ובקרה הולמים, ובכללם מנגנונים לזיהוי ואיתור אירועים חריגים, וכן לקיים תהליך סדור לטיפול וניהול אירועים חריגים לרבות תחקור של נסיבות האירוע, הפקת לקחים ובחינה מחדש של מנגנוני הפיקוח והבקרה;

8.2.4. 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. השיקולים שיילקחו בחשבון בקביעת האירועים כאמור הם, בין היתר: היקף הפגיעה במידע ממערכת נתוני אשראי, בתהליכים או בלקוחות, לרבות פגיעה פוטנציאלית, משך האירוע, היקף השיבוש בפעילות הקשורה למערכת נתוני אשראי ומידת הנזק;

8.2.5. אירועים חריגים המחויבים בדיווח לממונה בהתאם למפורט בסעיף 11.1, וכן אירועים נוספים לדיווח לממונה לפי שיקול דעת הדירקטוריון.

8.3. הדירקטוריון יוודא כי מדיניות השימוש במערכת נתוני אשראי מיושמת על ידי ההנהלה, וכי הוקצו משאבים נאותים לצורך יישום מדיניות זו.

9. הנהלת משתמש בנתוני אשראי

9.1. ההנהלה תגבש ותטמיע את המדיניות, ותבחן את הצורך בעדכונה, לכל הפחות אחת לשנתיים, וכן בעת ביצוע שינוי מהותי בסביבה הטכנולוגית או בחשיפה לסיכונים לרבות בשל התרחשות אירוע חריג משמעותי.

9.2. ההנהלה תמנה גורם בדרג של חבר הנהלה או מקבילה אחרת שיהיה אחראי להסדרת השימוש הנאות במערכת נתוני אשראי (להלן – **אחראי שימוש במערכת נתוני אשראי**).

9.3. ההנהלה תגדיר נהלי עבודה אשר יבטיחו שימוש נאות במערכת נתוני אשראי, ותוודא את האפקטיביות שלהם. נהלי העבודה יסדירו, בין היתר, את הנושאים הבאים:

9.3.1. פירוט התנאים ואופן השימוש במערכת נתוני אשראי לפי החוק. בין השאר, יש לכלול התייחסות לנושאים הבאים: מטרות השימוש בנתוני אשראי, דרכי זיהוי לקוח, אופן קבלת הסכמת לקוח לצורך הפקת דוח אשראי, יידוע לקוח לצורך הפקת חיווי, הודעה ללקוח על קבלת דוח אשראי, אופן שמירת נתוני אשראי, מסירתם ללקוח והתנאים למחיקתם;

9.3.2. פירוט הגורמים בעלי הגישה לנתוני אשראי, ופירוט הפעולות הנדרשות בהתייחס לערוצי הפעילות השונים וסוגי עסקאות אשראי, ובהתאם לממשקי הפעילות אל מול לשכות האשראי;

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

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

9.3.5. תיעוד כלל האירועים החריגים, וכן דיווחים נדרשים על אירועים חריגים להנהלה, לדירקטוריון בהתאם למדיניות שקבע, ולממונה בהתאם להוראה;

9.3.6. תהליכי תחקור והפקת לקחים מאירועים חריגים שאירעו, לרבות בחינה מחדש של מנגנוני הפיקוח והבקרה.

9.4. ההנהלה תוודא יישום נהלי העבודה לשימוש נאות במערכת נתוני אשראי, וכן תוודא את האפקטיביות של תהליכי הפיקוח, הבקרה והניטור, ושל תהליכי תחקור האירועים החריגים.

פרק ג' - דיווחים לממונה

10. דיווח על מינוי אחראי לשימוש במערכת נתוני אשראי

10.1. משתמש בנתוני אשראי נדרש לדווח לממונה על פרטי הגורם שמונה כאחראי לשימוש במערכת נתוני אשראי, בהתאם לסעיף 9.2.

10.2. משתמש בנתוני אשראי נדרש לדווח לממונה בכל מקרה בו האחראי לשימוש במערכת נתוני אשראי חדל למלא את תפקידו.

11. **אירוע חריג משמעותי**

11.1. סוגי האירועים

משתמש בנתוני אשראי נדרש לדווח לממונה על אירוע חריג משמעותי או על חשד ממשי לאירוע כאמור, לרבות אירוע הקשור להליכי זיהוי לקוח, בהתאם לסוגי האירועים המפורטים להלן (להלן – **אירוע חריג משמעותי**):

11.1.1. אירוע בו נעשה שימוש במערכת נתוני אשראי שלא לפי החוק, וקשור לקבוצת לקוחות;

11.1.2. אירוע בו נעשה שימוש במערכת נתוני אשראי, בלא הרשאה או בחריגה מהרשאה, וקשור לקבוצת לקוחות;

11.1.3. סימנים המעידים על כך שמידע ממערכת נתוני אשראי אודות קבוצת לקוחות נחשף בחריגה מהרשאה, דלף, שובש או נמחק שלא כדין;

11.1.4. אירוע שגרם לשיבוש או השבתה של פעילות או מערכות מידע או מערכות תפעוליות ואשר כתוצאה מכך נפגע השימוש במערכת נתוני אשראי ליותר משלוש שעות, למעט השבתה יזומה;

11.1.5. אירוע אבטחת מידע הקשור לשימוש 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 ארבע שעות ממועד זיהויו לראשונה;

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

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

11.1.8. כל אירוע שלא נכלל בסעיפים 11.1.1 – 11.1.7 אשר דווח למאסדר של משתמש בנתוני אשראי או לרשות אכיפה, לרבות הרשות להגנת הפרטיות, וקשור למערכת נתוני אשראי.

11.2. אופן הדיווח

11.2.1. דיווח ראשון לממונה על אירוע חריג משמעותי יועבר באמצעות דיווח טלפוני או דיווח בכתב בתוך שעתיים ממועד זיהויו כאירוע חריג משמעותי (להלן – **דיווח ראשוני**). השלמת הדיווח תתבצע בכתב בתוך 8 שעות ממועד הדיווח הראשוני (להלן – **דיווח משלים**); ואולם, אם מועד הדרישה להשלמת הדיווח המשלים חל שלא בשעות העבודה המקובלות, הוא יועבר בכתב עם תחילת שעות העבודה המקובלות של היום העוקב. הממונה רשאי להאריך את המועד האמור לדיווח בכתב בהתקיים נסיבות המצדיקות זאת.

11.2.2. ככל שתהיינה התפתחויות מהותיות במהלך האירוע, יש לעדכן את הממונה על התפתחויות אלו. כמו כן, יש לעדכן את הממונה על סיום האירוע. דיווחים כאמור יתבצעו בכתב.

11.2.3. לאחר השלמת הטיפול באירוע, יימסר לממונה דוח הפקת לקחים והמלצות ליישום. הדוח יועבר לממונה בתוך 45 יום ממועד סיום האירוע או בתוך 60 יום ממועד זיהויו כאירוע חריג משמעותי, לפי המוקדם מביניהם.

11.2.4. הדיווחים בכתב כאמור לעיל, יימסרו בהתאם לפורמט הדיווח שבנספח א' ויכללו, בין השאר, את הפרטים הבאים: תיאור של האירוע שהתרחש, זמן התרחשותו, הפערים שאפשרו את התרחשותו ואופן הטיפול בו. הדיווח הראשוני והדיווח המשלים יכללו את הפרטים הידועים נכון למועד מסירת הדיווח.

11.2.5. בהתייחס לדיווחים בכתב, משתמש בנתוני אשראי רשאי לעשות שימוש בפורמט הדיווח על אירועי אבטחת מידע וסייבר שקבע מאסדר של משתמש בנתוני אשראי, ובלבד שהעברתם לממונה תהיה בהתאם למפורט בהוראה זו, לרבות לעניין סוגי האירועים החריגים המחייבים דיווח, וזמני הדיווח הנדרשים.

11.2.6. על אף האמור בסעיפים 11.2.1 – 11.2.5, דיווח לממונה על אירוע לפי סעיף 11.1.8 יימסר תוך 14 ימים ממועד זיהוי האירוע לפי אחת משתי האפשרויות הבאות:

(א) דיווח בכתב בהתאם לפורמט הדיווח שבנספח ב', שיכלול, בין השאר, את הפרטים הבאים: שם המאסדר של משתמש בנתוני אשראי או רשות האכיפה אליו הועבר הדיווח, תיאור של האירוע שהתרחש, זמן התרחשותו ואופן הטיפול בו.

(ב) העברת העתק מהדיווח שנשלח למאסדר של משתמש בנתוני אשראי או לרשות אכיפה. הממונה רשאי לדרוש השלמת מסמכים ומידע, ככל שיעלה הצורך בכך.

פרק ד' - ביקורת פנימית

12. 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.
הביקורת הפנימית תבחן, בין היתר, את אפקטיביות המנגנונים שנקבעו לזיהוי איתור וטיפול באירועים חריגים, ותהליכי התחקור והפקת הלקחים, וכן תבחן את יישום דרישות ההוראה לעניין דיווחים להנהלה, לדירקטוריון ולממונה.

פרק ה' – מועד תחילה

13. תחילתה של ההוראה שישה חודשים מיום פרסומה באתר מערכת נתוני אשראי בבנק ישראל.

* * *

נספח א' - פורמט דיווח לממונה על אירוע חריג משמעותי לפי סעיפים 11.1.1 – 11.1.7

דיווח על אירוע חריג משמעותי או על חשד ממשי לאירוע כאמור	
תאריך הדיווח	DD/MM/YYYY
שם הגוף המדווח	
פרטי מאשר הדיווח	שם פרטי ושם משפחה: _____ תפקיד: _____ חתימה: _____
פרטי איש קשר לעניין הדיווח	שם פרטי ושם משפחה: _____ דוא"ל: _____ מס' טלפון: _____
סוג הדיווח	יש לסמן את סוג הדיווח: ☐ דיווח ראשוני ☐ דיווח משלים ☐ דיווח על התפתחויות מהותיות במהלך האירוע ☐ דיווח על סיום האירוע ☐ הפקת לקחים והמלצות ליישום
נושא האירוע	יש לסמן במקומות הרלוונטיים בהתאם לאירוע: ☐ אירוע חריג משמעותי שהתרחש ☐ חשד ממשי לאירוע חריג משמעותי ☐ אירוע החשוד כאירוע תקיפת סייבר
תיאור האירוע והיקפו (לרבות פירוט פגיעה במידע / תהליכים / מערכות / השפעת האירוע על פעילות הארגון ועל לקוחותיו/היקף הלקוחות המעורבים / נזק אחר לרבות כספי, ככל שרלוונטי).	מלל חופשי
מועד זיהוי האירוע	DD/MM/YYYY שעה: _____
מועד משוער של תחילת האירוע	DD/MM/YYYY שעה: _____
מועד סיום האירוע (בהתאם לקביעת ההנהלה)	DD/MM/YYYY שעה: _____
הפערים שאפשרו את התרחשות האירוע	מלל חופשי
התפתחויות מהותיות, ככל שאירעו	מלל חופשי
אופן הטיפול באירוע	מלל חופשי
האם לקוחות עודכנו בדבר התרחשות האירוע?	מלל חופשי
הפקת לקחים מהאירוע והמלצות ליישום (תיאור האמצעים שננקטו או המוצעים לנקוט כדי לטפל באירוע החריג, לרבות, במידת הצורך, אמצעים למניעת הישנות אירועים דומים).	מלל חופשי (יש לצרף דוח)
האם האירוע דווח למאסדר של משתמש בנתוני אשראי או לרשות אכיפה, לרבות הרשות להגנת הפרטיות.	שם המאסדר / הרשות: _____ הגורם אליו הועבר הדיווח: _____ תאריך העברת הדיווח: DD/MM/YYYY

הבהרות:

1. דיווחים בכתב יש להעביר באמצעי מאובטח קיים בין משתמש בנתוני אשראי לממונה או לדוא"ל: Pbcd@boi.org.il תוך סגירת קובץ הדיווח בסיסמה שתימסר טלפונית לנציגי הממונה.
2. דיווח ראשוני יימסר תוך שעתיים ממועד זיהוי האירוע כאירוע חריג משמעותי ככל שהדיווח הראשוני יימסר טלפונית, הוא יועבר על פי פרטי הקשר שנמסרו למשתמש בנתוני אשראי. ככל שהדיווח הראשוני יימסר בכתב, הוא יועבר בהתאם למפורט בסעיף 1 לעיל, תוך מילוי הפרטים הידועים בעת מסירת הדיווח. לגבי הפרטים שאינם ידועים בזמן הדיווח הראשוני, על המשתמש בנתוני אשראי לציין ה'מידע עדיין לא זמין' לרבות הערכה מתי המידע הנוסף יהיה זמין, ככל שניתן. בנוסף, יש לוודא קבלתו של הדיווח הראשוני על ידי נציגי הממונה בסמוך לאחר שליחתו.
3. דיווח משלים יימסר תוך 8 שעות ממועד הדיווח הראשוני, תוך מילוי הפרטים הידועים בעת מסירת הדיווח.

נספח ב' - פורמט דיווח לממונה על אירוע חריג משמעותי לפי סעיף 11.1.8

דיווח על אירוע חריג משמעותי שדווח למאסדר של משתמש בנתוני אשראי או לרשות אכיפה	
שם הגוף המדווח	
פרטי מאשר הדיווח	שם פרטי ושם משפחה: _____ תפקיד: _____ חתימה: _____
פרטי איש קשר לעניין הדיווח	שם פרטי ושם משפחה: _____ דוא"ל: _____ מס' טלפון: _____
האירוע דווח ל:	שם המאסדר של משתמש בנתוני אשראי או רשות האכיפה, לרבות הרשות להגנת הפרטיות: _____
פרטי הגורם אליו הועבר הדיווח	שם פרטי ושם משפחה: _____ תפקיד: _____ דוא"ל: _____ תאריך העברת הדיווח: DD/MM/YYYY
נושא האירוע	מלל חופשי
תיאור האירוע והיקפו	מלל חופשי
מועד זיהוי האירוע	DD/MM/YYYY שעה: _____
מועד משוער של תחילת האירוע	DD/MM/YYYY שעה: _____
מועד סיום האירוע (בהתאם לקביעת ההנהלה)	DD/MM/YYYY שעה: _____
אופן הטיפול באירוע	מלל חופשי

הבהרה:

1. דיווחים בכתב יש להעביר באמצעי מאובטח קיים בין משתמש בנתוני אשראי לממונה או לדוא"ל: Pbcd@boi.org.il תוך סגירת קובץ הדיווח בסיסמה שתימסר טלפונית לנציגי הממונה.