

כללי נתוני אשראי (אבטחת מידע), התשע"ט-2018¹

בתוקף סמכותי לפי סעיף 60(ג) לחוק נתוני אשראי, התשע"ו-2016 (להלן – החוק), ובהסכמת שרת המשפטים אני קובעת כללים אלה:

1. (א) מקור מידע ימנה גורם מקצועי שיהיה אחראי לאיסוף, רישום ודיווח המידע שיועבר למאגר לפי הוראות הממונה; גורם מקצועי כאמור –
- (1) יהיה עובד בכיר בארגון;
- (2) יהיה בעל כישורים בתחום איסוף המידע ורישום באופן המאפשר להטיל עליו אחריות אישית;
- (3) יהיה כפוף לכללים לשמירת אי-תלותו המקצועית ולמניעת ניגוד עניינים אשר ייקבעו על ידי מקור המידע;
- (4) יפעל בתיאום עם הגורם האחראי על אבטחת המידע של מקור המידע בכל הנוגע להיבטי אבטחת מידע, וכן עם גורמים אחרים במקור המידע הרלוונטיים לביצוע תפקידו.
- (ב) מקור מידע יפעיל מערך לאיסוף המידע אשר יועבר למאגר באופן שיוודא שמירה על שלמותו, מהימנותו, עדכניותו וזמינותו, בין השאר, תוך יישום הרשאות גישה, אמצעי אבטחה מקובלים אשר יבטיחו הגנה על מערכות המידע של הארגון, בקרה וביקורת מתאימים.
- (ג) מערכות המידע המשמשות את מקור המידע לצורך העברת המידע למאגר המידע יהיו אמינות, ויאפשרו שמירה על המשכיות עסקית כך שאיכות המידע ויכולת הדיווח למאגר לא ייפגעו באופן מהותי.
- (ד) מקור מידע יבחן מעת לעת, וכן בהתרחש שינויים טכנולוגיים, עסקיים, ארגוניים ורגולטוריים או אירועי אבטחת מידע, את הצורך בעדכון רמת האבטחה של מערכות המידע המשמשות את מקור המידע לצורך העברת המידע למאגר המידע.
- (ה) מקור המידע יודא אחת לשנה שאין במידע שהוא מעביר למאגר, מידע שאין הוא נדרש להעביר למאגר לפי החוק.
- (ו) גילה מקור מידע ליקוי או תקלה שיש להם השפעה מהותית על המערכת לשתוף בנתוני אשראי, ידווח עליה לממונה באופן מידי וכן ידווח על הצעדים שנקט בעקבות האירוע, לרבות בהתאם להוראות הממונה.

אופן איסוף המידע ורישום בידי מקור מידע לצורך העברתו למאגר

1. ק"ת 8111, התשע"ט (25.11.2018), עמ' 1356.

2. (א) מנהל המאגר יזהה את מקור המידע המדווח כמקור מידע המחויב או הרשאי לדווח למאגר לפי החוק.

(ב) העברת המידע ממקור המידע אל המאגר תיעשה באופן שימנע פגיעה במהימנות ושלמות הנתונים, או חשיפתם ליריעתו או לשימושו של גורם בלתי מורשה, ותהיה מוצפנת באופן אשר יגדיר מנהל המאגר; מנהל המאגר יקיים בקרה על תהליך העברת המידע למאגר ויודא כי הוא מועבר למאגר, והכול בהתאם להוראות הממונה.

(ג) מנהל המאגר יקיים תהליכי בקרה על איכות הקלט ושלמות המידע שהועבר למאגר ויודיע למקור המידע המדווח על מידע שגוי או פגום שהתגלה בתהליך הקלט או כל תקלה אחרת אשר זיהה.

(ד) מנהל המאגר ידווח לממונה על ליקויים כאמור בסעיפים קטנים (ב) ו-(ג); הממונה יפעל לבירור הליקויים מול מקור המידע ולמתן הנחיות למקור המידע לשם תיקונם.

3. (א) לצורך שמירת המידע במאגר, השימוש בו ואבטחתו ינקוט מנהל המאגר, בין השאר, צעדים כמפורט להלן:

(1) יקבע נוהל אבטחת מידע אשר יכלול, בין השאר, הוראות לעניין נושאים אלה:

(א) הגדרת האמצעים לעניין האבטחה הפיזית שנועדו להגן על מערכות המחשוב והתשתית ואופן הפעלתם לשם כך, ובלבד שאמצעים אלה יכללו, לכל הפחות, מתחם ייעודי מבודד ומנוטר, אמצעים להבטחת זיהוי כניסה לאתרים שבהם מצויות מערכות המחשוב והתשתיות, נעילת חדרים וארונות במתחם ומצלמות אבטחה;

(ב) הרשאות גישה למידע במאגר, לרבות לצורך שימוש במידע במאגר, למערכות תשתית המחשוב ולמערכות תקשורת ואבטחת מידע, ובכלל זה הקצאת הרשאות גישה על בסיס תפקיד ואחריות, איסור גישה למידע שלא לצורך מילוי תפקיד, ניהול מרוכז של הרשאות, מתן גישה למשתמשים המתקדמים (מנהלנים) רק באמצעות (Privileged Accounts Security) PAS, ביטול הרשאות בתום העסקת העובד ובקרה תקופתית על ההרשאות; הרשאת גישה למידע במאגר תינתן רק לבעלי הסיווג הביטחוני המתאים הנהוג בבנק ישראל לגבי מורשי גישה למאגרי מידע בבנק ישראל;

(ג) ביצוע הרכות למורשי הגישה למידע במאגר, למורשי הגישה למערכות תשתית המחשוב ולמערכות תקשורת ואבטחת מידע ולמורשי שימוש במידע; הרכות כאמור יכללו הנחיות ועדכונים בתחומי אבטחת המידע והגנת הפרטיות;

(ד) ביצוע סקר סיכונים שיכלול, בין השאר, התייחסות לסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת, לרבות הסיכונים הנובעים ממבנה מערכות המאגר, חומרה ותוכנה, מהשימושים במידע, ומהשתמשים והממשקים; הסקר האמור יכלול תכנית להפחתת הסיכונים, יבוצע בתדירות של אחת ל-18 חודשים לכל הפחות, ותוצאותיו יועברו לממונה;

(ה) אופן הטיפול במידע לצורך הנגשתו כמידע לא מוזהה ללשכות האשראי ולבנק ישראל לשם מילוי תפקידם ובהתאם למדיניות שתיקבע בנושא, ובלבד שהנגשת המידע תתבצע באמצעות הפעלת שירות אירוח מחשוב פרטי ותהליכי העבודה יכללו מגבלות על אופן ההכנסה וההוצאה של מידע, ניהול הרשאות למספר מצומצם של משתמשים, בקרה על מידע שמאושר להוצאה מהמאגר, אבטחה פיזית של מתחמי פעילות, החתמת משתמשים על הסכם שימוש, ביצוע הדרכות וקביעת סנקציות;

(ו) התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ומידת רגישות המידע, וכן ניטור מערכות לאורך כל שעות היממה על ידי צוות ייעודי וכלים ייעודיים למטרה זו, קביעת חוקת התראות ונוהלי דיווח, הגדרת יעדי שירות מזעריים בהתרחש אירועי אבטחת מידע והגדרת צעדי תגובה נדרשים;

(ז) כללי שימוש בהתקנים ניידים לרבות קביעה של סוגי ההתקנים המותרים לשימוש, הסימת אפשרות החיבור של אמצעים אלה לרכיבי המערכת למעט מקרים חריגים כגון עמדות ייעודיות להכנסת מידע ולהוצאת מידע והכול בכפוף להרשאות גישה;

(ח) היבטי אבטחת מידע הקשורים בגיבוי מידע ובלבד שיפורטו תהליכי הגיבוי על סוגיהם השונים, תדירותם, אופן שמירתם ואופן השימוש בהם לצורך השחזור;

(ט) תיאור של אמצעים נוספים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;

(2) יבצע בדיקות תקופתיות לרבות מבדקי חדירות בתדירות של אחת ל-18 חודשים, לכל הפחות, כדי לוודא את קיומם ותקינותם של אמצעי האבטחה השונים, לרבות אמצעי האבטחה שנקבעו לפי פסקה (1);

(3) יורה על הנחיות לגבי אופן ביצוע פעולות הפיתוח במאגר ותייעודן, ובכלל זה הגישה של אנשי הפיתוח לנתונים במאגר, כגון קיום סביבת פיתוח נפרדת, עבודה בהתאם לשיטת פיתוח מאובטחת ושימוש בנתונים סינטיים בלבד.

(4) יבחן אחת ל-18 חודשים את הצורך בעדכון נוהלי אבטחת מידע; אם מתבצע שינוי טכנולוגי, ארגוני או שינוי תהליכי עבודה, שהוא שינוי מהותי, או בהתרחש אירועי אבטחת מידע, ייבחן הצורך בעדכון נוהלי אבטחת המידע באופן מיידי.

(ב) נוהל אבטחת המידע וכל שינוי מהותי בו יובאו לאישורו של הנגיד.

4. (א) הגישה למידע המזוהה במאגר תותר רק לממונה, למנהל המאגר או למי שמי מהם הסמיך מטעמו במפורש ולעניין מסוים, לצורך מילוי תפקידים ובכפוף להרשאות הגישה שיקבעו.

(ב) מנהל המאגר יודא כי ננקטים אמצעים לבקרה ותיעוד של הכניסה והיציאה מהאתר שבו מצויות מערכות המידע ושל הכנסה והוצאה של ציוד אל האתר וממנו.

(ג) מנהל המאגר ינהל רישום מעודכן של מורשי הגישה למידע מזוהה ולמידע לא מזוהה הקיים במאגר, תפקידיהם והרשאות הגישה שלהם אשר נקבעו לפי סעיף 3(א)(1)(ב); הרשאות הגישה ייקבעו על בסיס הגדרות תפקיד ובמידה הנדרשת לביצוע התפקיד.

(ד) מנהל המאגר יקיים נתיבי גישה מוגדרים ומבוקרים לצורך הגישה למידע במאגר ויבטיח כי ניסיון גישה בנתיב שאינו מורשה ייחסם, ינוטר ויתועד.

5. אמצעי הזיהוי של לשכת אשראי לשם שימוש במערכת הטכנולוגית המשמשת את המאגר יהיה מסר אלקטרוני שינפיק בנק ישראל, המאשר כי אמצעי אימות החתימה הוא של עובר מוסמך בלשכה (בסעיף זה – תעודה אלקטרונית); התעודה האלקטרונית תחודש מעת לעת בתדירות שיקבע מנהל המאגר, ולכל הפחות, אחת ל-24 חודשים.

אופן הגישה למידע המזוהה במאגר

אמצעי זיהוי נדרשים מלשכת אשראי לשם שימוש במערכת הטכנולוגית במאגר

6. (א) מנהל המאגר יקים מנגנון בקרה על המערכת הטכנולוגית המשמשת את המאגר והגישה אליה, אשר יתקיימו בו תנאים אלה:

(1) המנגנון יאפשר את תיעוד הגישה למערכות המידע ויכלול את הנתונים הנדרשים לצורך מעקב אחר הגישה למערכות וככלל זה נתונים בדבר זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה (להלן – נתוני הגישה); נתוני הגישה יישמרו למשך 24 חודשים לפחות;

(2) מורשים בלבד אשר נקבעו לשם כך באופן מפורש על ידי מנהל המאגר, יוכלו לשנות או לבטל באופן חריג הפעלה של המנגנון האמור בפסקה (1) בהתאם לנוהל שיקבע מנהל המאגר לשינוי או ביטול המנגנון ובכפוף למסלול אישורים שייקבע בו.

בקרה על המערכת הטכנולוגית במאגר ותיעוד גישה

(ב) מנהל המאגר יקיים מערכות לניטור וניהול אירועי אבטחת מידע שיתייחסו לכלל המידע בנתיבי בקרה מוגדרים; המערכות יפעלו באופן שוטף ובזמן אמת ויתריעו על הפרות שהוגדרו בחוקת ההתראות לפי סעיף 3(א)(1)ו); ייעשה שימוש במערכות כגון: SIEM (Security information and event management), User and Entity Behavior, ו-ABEU (Analytics).

(ג) מנהל המאגר יקיים נוהל בדיקה שגרתית של נתוני נתיב הבקרה ודיווחי הניטור, יורה על לוח זמנים לתיקון ליקוי שהתגלה לפי חומרתו ויודא את תיקונו.

(ד) המערכת לניטור וניהול אירועי אבטחת מידע תקבל דיווחים ממערכות המידע השונות הכלולות במאגר על אודות חשש לאירועים חריגים הנוגעים לאיומים על המידע.

7. (א) נתוני אשראי מזהים לגבי לקוח יועברו מהמאגר ללשכת אשראי רק לאחר שהתקבלה בקשה מפורשת מלשכת האשראי, העומדת בתנאים שנקבעו לפי החוק ובשדות שנקבעו בידי הממונה להעברת מידע על הלקוח.

(ב) המידע יועבר מהמאגר ללשכת האשראי בערוצי תקשורת מבוקרים ומנוטרים, ובשדות שייקבעו בידי הממונה.

(ג) העברת המידע תיעשה באופן מאובטח תוך יישום תהליכי הגנה מקובלים להעברת מידע ובכלל זה שימוש בשיטות הצפנה מקובלות, וידוא הגעת נתונים ליעדם והגבלת גישה לנתונים בהתחשב בצורכי השימוש במידע והמגבלות אשר נקבעו לפי החוק.

(ד) מנהל המאגר יישם טכניקות הגנה והצפנה מקובלות ויתקף מזמן לזמן את הערכניות שלהן תוך הסתמכות על תקנים בין-לאומיים מוכרים.

(ה) מנהל המאגר יגדיר ויישם נוהל לניהול מפתחות הצפנה, שיכלול הוראות לכל מחזור החיים של מפתחות הצפנה, לרבות חילול, הפצה, שמירה, עדכון וביטול.

(ו) לא תינתן גישה למידע המצוי במאגר לגורם שאינו מורשה או לשימושים שאינם מותרים לפי החוק; מנהל המאגר יתעד וידווח לממונה על מקרה שבו בוצע שימוש בלא הרשאה או בחריגה ומהשימושים המותרים.

8. (א) אירע אירוע אבטחה חמור כהגדרתו בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, תודיע על כך הלשכה באופן מיידי לממונה, וכן תדווח על הצעדים שנקטה בעקבות האירוע, לרבות בהתאם להוראות הממונה.

(ב) לשכת אשראי תפעל למחיקת נתוני האשראי המזהים שהועברו אליה מהמאגר בהתאם לקבוע בתקנות נתוני אשראי, התשע"ח-2017, ובהתאם להוראות הממונה.

(ג) מחיקת הנתונים תתבצע באופן שלא יאפשר את קריאתם על ידי יישומים טכנולוגיים, לרבות מערכות הפעלה המשמשות את מערכות המידע של לשכת האשראי, למעט קריאתם תוך הסתמכות על גיבויים או קובצי רישום (log).

אופן העברת מידע
מזוהה ללשכת
אשראי

שמירה, שימוש,
אבטחה ומחיקה
של מידע במערכות
המידע של לשכת
אשראי

(ד) לשכת אשראי תקבע נוהל עבודה להליך מחיקת הנתונים המזוהים המתקבלים מהמאגר, שיכלול, בין השאר, הוראות לעניין הנושאים המפורטים להלן ותביאו לאישור הממונה:

- (1) הגורם האחראי להליך;
- (2) תדירות ועיתוי המחיקה;
- (3) זיהוי המערכות בהן נדרש לבצע מחיקה;
- (4) אמצעי המחיקה;
- (5) תהליכי בקרה שוטפים.

9. הוראות כללים אלה באות להוסיף על הוראות כל דין בעניין אבטחת מידע ולא לגרוע מהן.

שמורת דינים

ה' בכסלו התשע"ט (13 בנובמבר 2018)

קרנית פלוג
נגידת בנק ישראל