בנק ישראל

הממונה על שיתוף בנתוני אשראי

מזכירות הוועדה המייעצת

מערכת נתוני אשראי
של בנק ישראל

פרוטוקול מישיבת הוועדה המייעצת להוראות הממונה על שיתוף בנתוני אשראי,

שהתקיימה פיזית ובאמצעי תקשורת בתאריך 02/04/2025

משתתפים מקרב חברי הוועדה:	פרופ' רות פלאטו-שנער – יו"ר הוועדה המייעצת כרמי אור רונן הורוביץ עו"ד ראובן אידלמן עו"ד יערה למברגר עו"ד תומר רבינוביץ
חברי ועדה שנעדרו	גל אסטריכר אביגיל ונקרט
משתתפים מקרב עובדי הבנק:	אייל חדד הממונה על שיתוף בנתוני אשראי חן הולצמן, מזכירת הוועדה המייעצת עו"ד שירלי אבנר, המחלקה המשפטית <u>עובדי הממונה</u>: עובדת הממונה אהרון יוסף זכאים רוית מזרחי איתי דגני רואי יעקובי ענת ירון עדו שגב
מוזמנים נוספים	

עיקרי הדיון

הקדמה – דברי פתיחה סיכום 2024	
מזכירת הוועדה המייעצת	מציגה את החברים החדשים בוועדה המייעצת. מציגה סיכום הפעילות של מערכת נתוני אשראי בשנת 2024
חלק א' : טיוטת הוראה 407 בנושא "שימוש במערכת נתוני אשראי"	
עובדת הממונה	מציגה רקע כללי לטיוטת הוראת ממונה חדשה בנושא "שימוש במערכת נתוני אשראי": • חלפו כמעט 6 שנים מאז העלייה לאוויר והגיעה העת להסדיר את השימושיות בקרב המשתמשים בנתוני אשראי. • הצורך באסדרה עלה גם בעקבות פעילות של פיקוח וביקורת על המשתמשים בנתוני אשראי, שמבצעת יחידת פיקוח ובקרה באגף הממונה על שיתוף בנתוני אשראי.

	• חלק מהסעיפים בהוראה זו, לדוגמה הדרישה לקביעת נהלים ובקרות, מיושמים על ידי משתמשים בנתוני אשראי, בעיקר הגדולים. המטרה היא להעלות את המודעות בקרב כלל המשתמשים בנתוני אשראי, ולהבטיח שמשתמשים קטנים יותר מסדירים את התהליכים אצלם. פרק א' כללי –סעיף הגדרות: בדומה למבנה המקובל של הוראות הממונה על שיתוף בנתוני אשראי, תת פרק זה מפרט את ההגדרות הרלוונטיות. עוברת על ההגדרות בפרק: ההגדרה של "אירוע אבטחת מידע" היא "אירוע שגורם פגיעה בסודיות, שלמות או זמינות של מידע או פוטנציאל לפגיעה כאמור ובכלל זה מתקפת סייבר".
חבר הוועדה	לדעתי, הגדרה זו מצומצמת ביחס לתקנות אבטחת מידע. לא ברור המינוח "פגיעה בסודיות".
חברת הוועדה	פירוט סוגי האירועים החריגים המשמעותיים בהוראה הוא רחב מאד, ולכן לכאורה אין חשש לצמצום.
עובדת הממונה	ההגדרה של אירוע אבטחת מידע בהוראה היא רחבה, וכמו כן גם הפירוט של אירועים סוגי האירועים שיש לדווח עליהם לממונה רחב. חשוב לציין, שאין הכוונה שהמשתמשים בנתוני אשראי ידווחו על אירועים שאינם משמעותיים. בנוסף, יש לזכור שהממונה אינו המאסדר הראשי שלהם והם נדרשים לדווח על אירועי אבטחת מידע גם למאסדר הראשי שלהם, וכן לרשות הגנת הפרטיות במידה ונדרש.
חבר הוועדה	ממליץ לבחון את ההגדרה שבתקנות אבטחת מידע של הרשות להגנת הפרטיות.
חבר הוועדה	האם בהוראות הממונה הקודמות שפורסמו לציבור לא הוגדר אירוע אבטחת מידע?
עובדת הממונה	אירוע אבטחת מידע לא הוגדר בהוראות הממונה הקיימות. עם זאת, הסתמכנו על הגדרות של מאסדרים מובילים בחו"ל.
יו"ר הוועדה	מצטרפת להמלצה לבחון את ההגדרה בתקנות אבטחת מידע. לגבי זמינות מידע, אירוע טכני למשל כמו הפסקת חשמל, האם נחשב אירוע אבטחת מידע ויש לדווח עליו לממונה?
חברת הוועדה	אולי דיווח בגין הפסקת חשמל חד פעמית אין צורך, אך אם למשל ישנן הפסקות חשמל הולכות ונשנות, לדעתי כדאי שהממונה יקבל דיווח על כך.
עובדת הממונה	יש לדווח בהתאם לרלוונטיות למערכת נתוני אשראי. אנו נבחן את ההגדרה של אירוע אבטחת מידע. הגדרה נוספת היא עבור "אירוע חריג": "אירוע של שימוש במערכת נתוני אשראי שלא לפי החוק או אירוע אבטחת מידע הקשור למערכת נתוני אשראי". אירוע חריג יכול להיות קשור לאירוע אבטחת מידע, אך לא בהכרח, למשל בקשה לדוח אשראי של לקוח ללא הסכמתו. ייתכנו מצבים בהם האירועים יהיו שלובים זה בזה.
יו"ר הוועדה	האם ישנו אירוע אבטחת מידע שאינו קשור למערכת נתוני אשראי?
עובדת הממונה	כן. ייתכנו אירועים מסוג זה שאינם נוגעים לשימוש במערכת נתוני אשראי או למערכות הקשורות למערכת נתוני אשראי, לדוגמה: כל אירוע אבטחת מידע שקשור למערכות אחרות שאין להם נגיעה למערכת נתוני אשראי. אירועים אלו לא ידווחו לממונה, אולם ייתכן

	שידווחו למאסדר הראשי של משתמש בנתוני אשראי בהתאם להוראותיו או לרשות הגנת הפרטיות ככל שנדרש. ממשיכה לפרט את ההגדרות בפרק: "שימוש במידע"- כל פעולה המבוצעת על מידע לרבות קבלתו, איסופו, אחסונו והעתקו, עיון בו, גילויו ועוד. "שימוש במערכת נתוני אשראי" – "שימוש במערכות המידע ובמערכות התפעוליות שבאמצעותן מתקבל המידע ממערכת נתוני אשראי, וכן שימוש במידע שמקורו במאגר נתוני אשראי". הכוונה לכלול את כל ההיבטים הנוגעים לשימוש במערכת נתוני אשראי, ובכלל זאת שימוש במידע ושימוש במערכות הרלוונטיות. "שעות עבודה מקובלות" – ימים א'-ה' שהינם ימי עסקים, בין השעות 8:00 ל-18:00. המונח יום עסקים מוגדר אף הוא.
יו"ר הוועדה	לגבי המונח "יום עסקים" שמחריג את פורים, יש לשים לב שמציינים את חג הפורים במועדים שונים בירושלים וביתר הארץ.
עו"ד אבנר	המונח מקובל בהוראות רגולציה של בנק ישראל לרבות כללי הנגיד.
עובדת הממונה	חשוב לציין שדיווח מידי בעל פה או בכתב נדרש תוך שעתיים מזיהוי האירוע כמחייב דיווח, ללא קשר אם מדובר ביום עסקים. ההגדרה ליום עסקים היא עבור העברת הדיווח המשלים בכתב.
יו"ר הוועדה	בהוראת הממונה מספר 401 הוגדר המונח "נותן שירות", ואילו בהוראה 407 לא הוגדר "נותן שירות" ולא הוגדר מיהם המשתמשים בנתוני אשראי.
עובדת הממונה	הוראה 401 והוראה 401A כוללות הגדרה של "נותן שירות" שאיננה מופיעה בחוק נתוני אשראי. ההגדרה היא לשם הנוחות, במקום בכל פעם לחזור על כל הקבוצות הרלוונטיות שההוראה חלה עליהן: לשכות אשראי, משתמשים בנתוני אשראי ומיופי כוח בתמורה. ההוראה המוצעת 407 תחול רק על משתמש בנתוני אשראי, ולגבי "משתמש בנתוני אשראי" אין צורך להגדיר. ההגדרה היא בחוק נתוני אשראי התשע"ו, 2016.
עו"ד אבנר	ככל שמדובר בחקיקת משנה שנקבעת מכוחו של החוק, כגון: תקנות, צווים, כללים או הוראות של הממונה , לא צריך לחזור על המונחים שהוגדרו בחוק, אלא אם כן רוצים לחרוג מההגדרה שנקבעה בחוק או שיש הגדרות שונות בחוק בשני סעיפים שונים.
עובדת הממונה	<u>מפרטת פרק ב' בהוראה – ממשל תאגידי:</u> ההוראה מטילה חובות שונים על דירקטוריון משתמש בנתוני אשראי, ומדגישה את אחריות הדירקטוריון לעניין השימוש במערכת נתוני אשראי. השימוש במערכת כרוך בסיכונים רבים ובהם דלף מידע ופגיעה בפרטיות הלקוחות, ולפיכך יש חשיבות לכך שהדירקטוריון יתווה ויאשר מדיניות בנושא.
חבר הוועדה	מציין כי יש חפיפה מסוימת עם הנחיית הרשות להגנת הפרטיות לעניין תפקיד הדירקטוריון בקיום חובות תאגיד לפי תקנות הגנת הפרטיות.
חברת הוועדה	לדעתי זה בסדר שיש חפיפה. החשש הוא מסתירה בין רגולטורים.
חבר הוועדה	אני לא רואה סתירה.

	אם בשיח עם המשתמשים יעלה נושא של סתירה ביחס להוראה של רשות הגנת הפרטיות, מבקש להביא לידיעתי.
עובדת הממונה	חשוב לציין שהוראות הממונה מסייגות שאינן פוטרות מהוראות כל דין אחרות.
חברת הוועדה	האם לא נכון יותר שבנק ישראל יקבע את המדיניות?
עובדת הממונה	סבורה שזה לא נכון. הרגולטור מתווה עקרונות במסגרת ההוראות שהוא מסדיר, לרבות נושאים שנכון שייכללו במדיניות. כל גוף ובמקרה זה כל משתמש בנתוני אשראי אחראי על המדיניות שלו, ועל אופן הפיקוח והבקרה שהוא מבצע, וזאת בהתאם לסיכונים והיקף הפעילות שלו. ממשיכה לפרט את ההוראה. הדירקטוריון יאתגר ויבחן את הצורך בשינויים במדיניות. מסמך המדיניות צריך לכלול התייחסות לנושאים הבאים, לכל הפחות: • פירוט הסיכונים הכרוכים בשימוש במערכת נתוני אשראי. • חובת ההנהלה לקבוע נהלי עבודה סדורים לשימוש נאות במערכת נתוני אשראי בהתאם להוראות החוק במטרה לצמצם את הסיכונים הגלומים בשימוש במערכת. • חובת ההנהלה לקבוע מנגנונים לזיהוי ולאיתור אירועים חריגים. הדגש הרגולטורי הוא צמצום פגיעה בלקוחות ובפרטיות שלהם. • קביעת אירועים חריגים אשר נדרש שההנהלה תדווח לדירקטוריון. אין חובה שהדירקטוריון יקבל דיווח מההנהלה על כל אירוע. מדיניות הדיווח לדירקטוריון תביא בחשבון שיקולים שונים, ובין היתר: את היקף הפגיעה במידע, בתהליכים או בלקוחות, לרבות פגיעה פוטנציאלית, משך האירוע, ומידת הנזק. הדירקטוריון יקבע גם את מדיניות הדיווחים לממונה, וזאת בנוסף לדיווחים שנדרש לדווחם לממונה בהתאם להוראה. הדירקטוריון יוודא כי מדיניות השימוש במערכת מיושמת באופן נאות על ידי ההנהלה ויקצה משאבים נאותים בהיבטי כוח אדם ומערכות טכנולוגיות לצורך יישום המדיניות. הנהלת משתמש בנתוני אשראי, תמנה גורם בדרג של חבר הנהלה או מקבילה אחרת, שיהיה "אחראי שימוש במערכת נתוני אשראי". בחוזר ציינו כי הגורם המקצועי האחראי שימונה יכול להיות גם "האחראי למידע" שמשתמש בנתוני אשראי נדרש למנות בהתאם להוראת ממונה מס' 501 בנושא "איסוף מידע ודיווח". כלומר, אפשרי שאותו גורם יהיה אחראי הן לתחום הדיווח והן לתחום השימושיות.
יו"ר הוועדה	כדאי לשקול להכניס להוראה עצמה, כי לא תמיד קוראים את החוזרים.
עובדת הממונה	החוזר מפורסם יחד עם ההוראה. ההוראה אינה קובעת שאסור לו למלא תפקיד נוסף ולכן אפשרי גם מנוסח ההוראה. ככל שיעלו שאלות, ניתן לפנות אלינו ואנחנו נותנים מענה לשאלות שמפנים אלינו. המטרה היא לאפשר גמישות לגופים המפוקחים להחליט האם למנות את אותו אדם לשני התפקידים ולא דווקא לכוון לחייב אותם.
יו"ר הוועדה	האם לא תרצו שיהיה גורם אחד בתחום הדיווח והמשתמשים?
עובדת הממונה	זה תלוי בשיקולי הגוף עצמו, בהתחשב: בגודלו, בצרכים או בתהליכים העסקיים שלו.

חברת הוועדה	ההוראה דורשת דיווח לממונה על מינוי, מדוע אין דרישה לדווח גם על כל סט הכלים העומד לרשותו.
עובדת הממונה	דיווח על סט הכלים הוא רחב ומורכב. בדרך כלל נושאים כאלה נבחנים במסגרת פעולות הפיקוח כמו למשל ביקורת על הגוף המפוקח. בהוראת הממונה יש גם דרישה למבקרים הפנימיים של המשתמשים לבצע ביקורת בנושא פעם בשלוש שנים. הממונה יכול לבקש להעביר אליו את דוח הביקורת. בנוסף, יש לממונה צוות פיקוח ובקרה ייעודי שמבצע ביקורות על גופים אלו. ממשיכה לפרט את ההוראה: סעיף 9.3.1 מפרט נושאים שחשוב שיהיו בנוהלי העבודה. נושאים אלו עלו מתוך פעולות פיקוח ובקרה של צוות הממונה. ההוראה מגדירה גם חובת תיעוד של כלל האירועים החריגים שאירעו אצל המשתמש, בין היתר, לצורכי פיקוח ובקרה של צוות הממונה.
חברת הוועדה	האם אמדתם את היקף הנטל על המשתמשים הקטנים?
עובדת הממונה	הנושא ייבחן במסגרת תהליך ה-RIA, וגם בשיח מול המשתמשים. אם יעלו הערות מצד המשתמשים הקטנים נבחן בהתאם. תהליכים טכנולוגיים יכולים לתת מענה לחלק מדרישות הוראת הממונה, וזה יכול להוות פתרון טוב לגופים קטנים. <u>מפרטת פרק ג' בהוראה – דיווחים לממונה</u>: • יש לדווח לממונה מי הגורם שמונה כ"אחראי לשימוש במערכת נתוני אשראי", אשר ההנהלה נדרשת למנות כאמור. • יש לדווח לממונה על אירועים חריגים משמעותיים או על חשד ממשי לאירועים כאמור. אין הכוונה לקבל דיווח על כל אירוע אלא רק על אירועים משמעותיים. כלומר, ייתכנו אירועים לא משמעותיים שהטיפול באירוע ייעשה על ידי הגוף מבלי הצורך לדווח לממונה. סעיף 11 בפרק זה, מפרט את סוגי האירועים. הייתה התלבטות בסעיף זה לגבי ההגדרה של "קבוצת לקוחות". קבענו שהכוונה לעשרה לקוחות ומעלה, ונשמח לשמוע את חוות דעתכם בנושא.
חבר הוועדה	לדעתי, כשמגדירים מהם האירועים החריגים, זה עלול לצמצם לרשימה הסגורה. לגבי ההגדרה של קבוצת לקוחות, לדעתי, גם קבוצה של 7 לקוחות למשל, יכול להיות מוגדר כאירוע חמור מבחינה של הגנת הפרטיות. כדי למנוע תהליכים כאלה, אולי כדאי לדרוש החל מהלקוח הראשון. בהתייחס לדיווח על מקרה בודד, אולי כדאי להסדיר זאת בדיווח "רזה" יותר שאינו מחייב דיווח רחב כמפורט בהוראה.
חברת הוועדה	מסכימה עם חבר הוועדה לגבי קבוצת לקוחות ומחזקת. אם למשל בכל שבוע יהיה אירוע של לקוח אחד בלבד, האם זה ייכלל בקבוצת לקוחות?
עו"ד אבנר	כשמדובר במערכות טכנולוגיות כמות האירועים שאינם משמעותיים היא רבה מאוד. זו בעיה להורות לגופים לדווח על כל דבר. זה גם עלול לפגוע בעבודה השוטפת של הגוף המפוקח וגם להציף את הרגולטור בהמון דיווחים שאינם רלוונטיים ויהיה קשה לממונה לפקח על הנושא.

עובדת הממונה	על פי ההוראה, כאמור, משתמש בנתוני אשראי נדרש לתעד את כל האירועים החריגים, לרבות אירועים שאינם מוגדרים כמשמעותיים לפי ההוראה. לממונה יש כלים נוספים כמו למשל תהליכי פיקוח ובקרה. לדוגמה, בתהליך של ביקורת בגוף מפוקח אפשר לבקש את התיעוד של כל האירועים ולבחון את זה.
חברת הוועדה	לדעתי יש הבדל בין דליפה של מידע אודות לקוח ובין שימוש במערכת ללא הרשאה, לכן מציעה להגדיר לכל אחד מהם מה הכוונה ב"קבוצת לקוחות".
חברת הוועדה	לדעתי כדאי לחדד את ההגדרה לאירוע חריג.
חברת הוועדה	בהיבט ההגנה על פרטיות הלקוחות, מציעה לדייק את ההגדרה לאירוע שקשור לקבוצת לקוחות לפי טווח זמן או קשר בין המקרים כך שלא יהיה למשתמשים שיקול דעת להגדיר אירוע שקשור למספר מועט של לקוחות (פחות מ-10) ואשר חוזר על עצמו, כאירועים נפרדים.
עו"ד אבנר	ההערה לגבי קשר בין אירועים בודדים מובנת וראויה לבחינה.
ממונה	נבחן שוב את ההגדרה.
יו"ר הוועדה	מוצע לוודא אחידות בשימוש במונחים "אירועים חריגים משמעותיים" ו"אירוע חריג מחייב דיווח".
עובדת הממונה	לממונה נדרש לדווח רק על אירוע חריג משמעותי או על חשד ממשי לאירוע כאמור, כאשר אירוע כאמור הוגדר כ"אירוע חריג מחייב דיווח". רשימת סוגי האירועים החריגים המשמעותיים מפורטת בהוראה. נעבור שוב על ההגדרות בהוראה ונראה האם נדרשות הבהרות או שינויים בנושא.
יו"ר הוועדה	תת סעיף 11.1.9 מכליל את כל תתי הסעיף 11.1 למעט 11.1.8, מדוע?
עובדת הממונה	בתת סעיף זה מדובר באירוע שדווח למאסדר אחר ולכן אינו רלוונטי לאירוע שכמעט והתרחש. ממשיכה לפרט את פרק ג' בהוראה – דיווחים לממונה. אופן הדיווח לממונה הכולל: דיווח ראשוני בתוך שעתיים ממועד זיהוי האירוע כחריג, דיווח משלים, דיווח על התפתחויות ודוח הפקת לקחים, וכן דיווח על אירוע שכמעט והתרחש, הינו בדומה לקיים בהוראות אחרות של הממונה כגון הוראה מס' 401 והוראה מס' 401A.
יו"ר הוועדה	האם מסירת דוח הפקת לקחים לממונה בתוך 45 יום ממועד סיום האירוע או בתוך 60 יום ממועד זיהוי האירוע, אינו זמן רב מדי?
עובדת הממונה	המועד שצוין בהוראה בהתאם לפרקטיקה המקובלת ולהוראות מקבילות של הממונה ושל רגולטורים אחרים. צריך לזכור כי תהליך הפקת לקחים דורש זמן וחשוב שהדיווח שיינתן יהיה טוב ואפקטיבי.
עו"ד אבנר	בנוסף, נערכה חשיבה בהקשרים של "אסדרה חכמה" – RIA. אין הכוונה להכביד על הגופים המפוקחים, ובל נשכח שחלות עליהם הוראות דיווח של המאסדר הראשי.
עובד הממונה	מפעולות פיקוח ובקרה שאנחנו מבצעים עולה כי יש גופים שבמקרים מסוימים מדווחים אלינו, ולאחר מכן מתקנים ומעבירים דיווח מעודכן. לכן, חשוב לאפשר להם לבצע תהליך שלם ואפקטיבי.
חברת הוועדה	לדעתי כשמדובר באירועים חריגים, צריך לעצור את העבודה השוטפת ולבחון את האירוע מבלי להתמהמה.

עובדת הממונה	אכן מצופה שהמשתמשים בנתוני אשראי יבחנו ויטפלו באירועים באופן מידי בכדי לצמצם נזקים. כאשר מדובר על אירוע שמוגדר משמעותי הוא גם מדווח לממונה אשר עוקב אחר אופן הטיפול של המשתמש בנתוני אשראי באירוע. במקרים מסוימים, ככל שנדרש, ייתכן שינקוט בצעדים רוחביים.
חלק ג': הוראה 401 בנושא "אמצעי זיהוי, והוראה401A בנושא "אמצע זיהוי מרחוק" – תיקון בהוראות קיימות	
עובדת הממונה	מציגה תיקונים מוצעים בהוראות 401 ו-401A בעקבות כתיבת הוראה 407: מאחר שנושא הדיווחים לממונה על אירועים חריגים, לרבות אירועי אבטחת מידע הקשורים לזיהוי לקוחות, הוסדר בהוראה 407, מוצע לבצע תיקונים קלים בהוראות כאמור: • מוצע לתקן את סעיף 2.1 להוראה 401, כך שיובהר בו שסעיף 4ב בנושא "דיווחים לממונה על אירועי אבטחת מידע וסייבר או חשד ממשי לאירועים כאמור" לא יחול על משתמש בנתוני אשראי. • מוצע להוסיף את סעיף 8.2 להוראה 401A, לפיו הוראות פרק ט' בנושא "דיווחים לממונה על אירועי אבטחת מידע וסייבר או על חשד ממשי לאירועים כאמור" לא יחולו על משתמש בנתוני אשראי. יש לציין כי נושא הדיווחים הוסדר בהוראה 407 המוצעת, כאשר בנושאים מסוימים החמרנו. כמו למשל בהתייחס להגדרת "קבוצת לקוחות": בהוראות 401 ו-401A ההיקף היה גבוה מ-10 לקוחות, והתייחס לאירוע המשפיע על מספר רב של לקוחות, כאשר השפעה כאמור תיבחן על ידי כל נותן שירות בהתייחס לגודלו ולמספר לקוחותיו העושים שימוש בהליכי הזיהוי.
חברת הוועדה	אכן החמרתם ביחס להוראה, אך לדעתי זה עדיין גבוה. כל לקוח זה עולם בפני עצמו.
חברת הוועדה	גם לדעתי קבוצה של 10 זה גבוה מדי.
ממונה	כפי שציינו קודם הנושא ייבחן. תודה על הדיון הפורה.

3.6.2025

תאריך אישור הפרוטוקול

חתימת יו"ר הוועדה