

אמצעי זיהוי מרחוק

פרק א' - כללי

מבוא

1. תקנות נתוני אשראי, התשע"ח-2017 (להלן – **התקנות**) קובעות כי לצורך קבלת הסכמת הלקוח, נותן אשראי יזהה את הלקוח, בעצמו או באמצעות צד שלישי, באחת מדרכי הזיהוי המפורטות בתקנות או באמצעות אמצעי זיהוי נוסף שהורה הממונה על שיתוף בנתוני אשראי (להלן – **הממונה**) מכוח סמכותו לפי סעיף 68 לחוק נתוני אשראי, התשע"ו-2016 (להלן – **החוק**), ו**בלבד שמדובר בזיהוי ברמת מהימנות גבוהה**. בנוסף, התקנות קובעות כי לשכת אשראי תעביר דוח ריכוז נתונים רגיל למיופה כוח בתמורה לאחר שזיהתה אותו באחת מדרכי הזיהוי כמפורט לעיל. אמצעי זיהוי אלו משמשים גם לצורך זיהוי לקוח על ידי לשכת אשראי לצורך מסירת דוח ריכוז נתונים רגיל או מתן שירותי ייעוץ פיננסי בתחום האשראי ללקוח. בנוסף, הממונה הוסמך לתת הוראות למיופי כוח בתמורה בפעולתם לפי החוק, בין היתר, לשם השמירה על עניינם של הלקוחות, הגנה על פרטיות הלקוחות ואבטחת מידע.
2. בתוקף סמכותי לפי סעיף 68 לחוק וכן בהתאם להוראות תקנות (1)5 ו-(1)10 ולאחר התייעצות עם הוועדה המייעצת שמונתה לפי סימן ד' בפרק י"א לחוק, הריני קובע הוראה זו, אשר מטרתה לקבוע דרכים נוספות לזיהוי הלקוח ברמת מהימנות גבוהה.
3. לאור השימוש הגובר בטכנולוגיות המאפשרות זיהוי לקוח מרחוק לצורך מתן שירותים פיננסיים ביעילות ובמהירות, ובהתאם לאמור לעיל, ההוראה נועדה להסדיר **אמצעי זיהוי מרחוק** ואת אופן השימוש בהם, בנוסף לאמצעי הזיהוי הקבועים בתקנות, עבור השימושים ועל ידי הגורמים הבאים:
 - 3.1. **זיהוי לקוח על ידי משתמש בנתוני אשראי**, לצורך קבלת הסכמת הלקוח למסירת דוח אשראי לגביו (לעניין זה, "לקוח" - לרבות מי שפועל בשמו).
 - 3.2. **זיהוי לקוח על ידי לשכת אשראי**, לצורך מסירת דוח ריכוז נתונים רגיל ללקוח עצמו, וכן לצורך מתן שירותי ייעוץ פיננסי ללקוח בהתבסס על הדוח האמור, או **לזיהוי מיופה כוח בתמורה** על ידי לשכת אשראי (לעניין זה, "לקוח" - לרבות מי שפועל בשמו).
 - 3.3. **זיהוי לקוח על ידי מיופה כוח בתמורה**, לצורך מסירת דוח ריכוז נתונים ללקוח שייפה את כוחו, וכן לצורך מתן שירותי ייעוץ פיננסי ללקוח בהתבסס על הדוח האמור. כמו כן, ההוראה קובעת דרישות לעניין ממשל תאגידי ותהליכי ניהול סיכונים, פיקוח ובקרה, וכן דיווחים לממונה בהתייחס לשימוש באמצעי זיהוי מרחוק ועל אירועי אבטחת מידע וסייבר.
4. כלל תהליכי הזיהוי המפורטים בהוראה ואופן השימוש בהם, וכן הדרישות הנוספות הקבועות בהוראה לעניין ממשל תאגידי, ניהול הסיכונים ודיווחים לממונה, נקבעו כאמור **על מנת להבטיח זיהוי ברמת מהימנות גבוהה**, תוך צמצום הסיכונים הגלומים בהליכי זיהוי מרחוק.
5. למען הסר ספק, הוראה זו קובעת דרישות נוספות על אלה הקבועות בהוראות כל דין החל על משתמש בנתוני אשראי, לשכת אשראי ומיופי כוח בתמורה, ואינה גורעת מהן.



6. למונחים הקבועים בהוראה זו תהיה המשמעות הקבועה בחוק ובתקנות, בהתאם לעניין, אלא אם כן נקבע אחרת בהוראה זו.

תחולה

7. הוראה זו חלה על:
- 7.1. משתמש בנתוני אשראי, לשכת אשראי, ומיופה כוח בתמורה (להלן – **נותן שירות**), בהתייחס לביצוע הליכי זיהוי ואימות מרחוק לצורך קבלת הסכמת לקוח ולמתן שירותים לפי החוק.
- 7.2. תחולת ההוראה על מיופה כוח בתמורה שהוא יחיד, הינה בהתאמות המתחייבות.
8. על אף האמור בסעיף 7:
- 8.1. הוראות פרק ג' בנושא 'פיקוח וניהול סיכונים' לא יחולו על נותן שירות הנמנה על הגופים המפורטים להלן, ובלבד שיפעל ביחס להליכים הנדרשים בפרק האמור, בהתאם להוראות מאסדר נותן השירות כמפורט להלן:
- 8.1.1. נותן שירות שהוא תאגיד בנקאי – כנדרש בהוראה כאמור.
- 8.1.2. נותן שירות שהוא תאגיד מסוג 'נותן שירותי אשראי' או 'מפעיל מערכת לתיווך אשראי' הכפוף לחוזר רשות שוק ההון – כנדרש בחוזר האמור.
- 8.2. הוראות פרק ט' בנושא "דיווחים לממונה על אירועי אבטחת מידע וסייבר או על חשד ממשי לאירועים כאמור" לא יחולו על משתמש בנתוני אשראי.
9. הממונה רשאי לקבוע הוראות מסוימות, שונות מאלו המפורטות בהוראה זו, שיחולו על נותן שירות מסוים, או לפטור נותן שירות מסוים מקיום סעיפים מסוימים בהוראה זו, זאת, במקרים חריגים לאחר שבחן את בקשתו של נותן השירות ונימוקיו אשר נמסרו לו בכתב. כמו כן, רשאי הממונה לקבוע כי הפטור או ההוראות השונות יחולו לתקופה קצובה, כפי שתקבע על ידו, הכל מנימוקים אשר יירשמו על ידי הממונה.

פרק ב' – הגדרות

בהוראה זו –

"גורם אימות" – אחד מאלה:

- (1) פריט הנמצא ברשות המשתמש (לדוגמה: סיסמה חד פעמית זמנית (OTP-One Time Password) הנוצרת על ידי רכיב חומרה הנמצא בידי המשתמש ומקושר לחשבון שלו, סיסמה חד פעמית זמנית הנוצרת על ידי נותן השירות ומועברת ללקוח על ידי מסרון, ולעניין זה לרבות מסרון קולי, או תעודה דיגיטלית הנשמרת בכרטיס חכם או רכיב אחר אשר ברשות המשתמש);
- (2) פריט הידוע רק למשתמש (לדוגמה: סיסמה קבועה);
- (3) פריט שהוא המשתמש (לרבות מאפיין ביומטרי, כגון: זיהוי קולי, טביעת אצבע וזיהוי פנים);



- **"הליכי זיהוי"** - הליכי זיהוי ואימות;
- **"המפקח על הבנקים"** - כמשמעותו בסעיף 5 לפקודת הבנקאות;
- **"המפקח על נותני שירותים פיננסיים"** - כמשמעותו בסעיף 2 לחוק הפיקוח על שירותים פיננסיים מוסדרים;
- **"זיהוי מרחוק"** - זיהוי מקבל שירות בהתאם להוראות סעיף 12;
- **"חוזר רשות שוק ההון"** - חוזר רשות שוק ההון מספר 5-10-2020 בנושא "התקשרות מרחוק עם מקבל שירות באופן מקוון";
- **"חוק הפיקוח על שירותים פיננסיים מוסדרים"** - חוק הפיקוח על שירותים פיננסיים (שירותים פיננסיים מוסדרים), התשע"ו-2016;
- **"טכנולוגיה לזיהוי חזותי"** - טכנולוגיה להיוועדות חזותית כאמור בסעיף 16 או טכנולוגיה לזיהוי מרחוק כאמור בסעיף 17;
- **"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"** - כמפורט להלן, לפי העניין:
 - (1) לעניין תאגיד בנקאי – המפקח על הבנקים;
 - (2) לעניין נותן שירותי אשראי ו-מפעיל מערכת לתיווך אשראי – המפקח על נותני שירותים פיננסיים;
- **"מסרון קולי"** - הודעת SMS המתקבלת במכשיר הטלפון הנייד של הלקוח כהודעה קולית;
- **"מפעיל מערכת לתיווך אשראי"** - מפעיל מערכת לתיווך אשראי כהגדרתו בחוק שירותים פיננסיים מוסדרים;
- **"מקבל שירות"** - לקוח וכן מי שפועל בשמו כמיופה כוח, אפוטרופוס או כמיופה כוח מתמשך, וכן
 - מיופה כוח בתמורה שהוא יחיד או מורשה חתימה במיופה כוח בתמורה שהוא תאגיד, הנדרש לעבור הליך זיהוי על ידי לשכת אשראי לצורך קבלת דוח ריכוז נתונים רגיל של לקוח אשר ייפה את כוחו;



- "נותן שירות" - משתמש בנתוני אשראי, לשכת אשראי, מיופה כוח בתמורה;
- "נותן שירותי אשראי" - נותן שירותי אשראי כהגדרתו בחוק שירותים פיננסיים מוסדרים;
- "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;
- "תעודה מזהה" - אחד מאלה: תעודת זהות, תעודת עולה עד 30 ימים מיום הנפקתה, דרכון ישראלי או רישיון נהיגה ישראלי.

פרק ג' - פיקוח וניהול סיכונים

10. דירקטוריון נותן השירות

- 10.1. דירקטוריון נותן השירות יאשר את מדיניות נותן השירות לעניין השימוש באמצעי זיהוי מרחוק בעבור זיהוי ואימות מקבל השירות (להלן - **מדיניות זיהוי מרחוק**), לפחות אחת לשנה, וכן בעת ביצוע שינוי מהותי במדיניות, לרבות בשל התרחשות אירוע מהותי המצריך את עדכון המדיניות כאמור.
- 10.2. מדיניות הזיהוי מרחוק תכלול התייחסות למגוון הסיכונים הגלומים בשימוש באמצעים לזיהוי מרחוק, ובכלל זה סיכונים אבטחת מידע וסייבר, סיכונים מיקור חוץ וסיכונים תפעוליים אחרים, סיכונים פגיעה בפרטיות, סיכונים מוניטין, סיכונים משפטיים וסיכונים ציות.
- 10.3. ככל שנותן השירות מבקש לעשות שימוש בצד שלישי בהליכי הזיהוי מרחוק (להלן - **ספק מיקור חוץ**), על דירקטוריון נותן השירות לוודא, טרם קבלת השירות, כי לספק מיקור חוץ היכולות והאמצעים לבצע את הליכי הזיהוי מרחוק ברמת מהימנות גבוהה בהתאם לדרישות הדין ולהוראה זו. בנוסף, הדירקטוריון יבחן באופן תקופתי, את נאותות הליכי הזיהוי המבוצעים באמצעות ספק מיקור החוץ, הסיכונים הגלומים בזיהוי כאמור וכן את הצעדים הנדרשים לצורך צמצום הסיכונים. שימוש בספק מיקור החוץ יעשה בהתאם לאמור בפרק ח' להוראה זו.
- 10.4. דירקטוריון נותן השירות יקבע **דיווחים נדרשים** בנושא זיהוי מרחוק, לרבות דיווחים תקופתיים (כגון: דוח פעילות תקופתי אחת לשנה, אשר יכלול סוגי אמצעי זיהוי מרחוק שנעשה בהם שימוש, נפח פעילות, אירועים מיוחדים ככל שאירעו), וכן סוגי האירועים המצריכים **דיווח מיידי**, והגורמים האחראים על הדיווח ומועדי הדיווח.
- 10.5. דירקטוריון נותן השירות יודא כי מדיניות הזיהוי מרחוק מיושמת על ידי נותן השירות וכי הוקצו המשאבים הנאותים והמספקים לצורך יישום מדיניות זו.



11. הנהלת נותן השירות

- 11.1. הנהלת נותן השירות תגבש ותטמיע את מדיניות הדירקטוריון לעניין הזיהוי מרחוק.
- 11.2. הנהלת נותן השירות תקבע את תחומי האחריות של הגורמים הרלוונטיים לניהול ותפעול הליכי זיהוי מרחוק.
- 11.3. הנהלת נותן השירות תוודא כי הליך הזיהוי נעשה בהתאם למדיניות, לנהלים ולהוראות הנדרשות, ותוודא את אפקטיביות תהליכי הבקרה על הליכי הזיהוי מרחוק.
- 11.4. הנהלת נותן השירות תבחן את הצורך בעדכון מדיניות הזיהוי מרחוק, לכל הפחות אחת לשנה, וכן בכל שינוי מהותי בהליך הזיהוי מרחוק או בעת התרחשות אירוע מהותי המצריך את עדכון המדיניות כאמור.
- 11.5. הנהלת נותן השירות תגדיר את הליכי הזיהוי הנדרשים לצורך קבלת הסכמת מקבל השירות בערוצי הפעילות השונים, לרבות בערוצים המקוונים ותוך אבחנה בין זיהוי מקבל שירות המתבצע לראשונה (להלן – **זיהוי ראשוני**) לבין זיהוי מקבל שירות לאחר שבוצע זיהוי ראשוני (להלן – **הזדהות שוטפת**).
- 11.6. הנהלת נותן השירות תיישם **בקורות וכלי ניטור** אשר יאפשרו לזהות אירועים המעידים על שימוש לרעה בהליכי הזיהוי מרחוק, לרבות גניבות זהות, זיוף תעודות זיהוי, אנומליות טכנולוגיות ועסקיות, בקשות זיהוי מצד מקבל שירות המוגדר כלקוח בסיכון גבוה או מקבל שירות שאינו מורשה לקבל נתוני אשראי.
- 11.7. הנהלת נותן השירות תגדיר **דיווחים מיידיים** על אירועי אבטחת מידע וסייבר המעידים על שימוש לרעה באמצעי הזיהוי ופירוט הגורמים להם יימסרו דיווחים כאמור.
- 11.8. הנהלת נותן השירות תקבע הנחיות לעניין **שמירה וגיבוי של המידע והנתונים המתקבלים בהליכי הזיהוי מרחוק**, לרבות נתוני הלקוחות והנתונים הטכנולוגיים הנדרשים לצורך זיהוי ברמת מהימנות גבוהה, וכן הנחיות לכך שניתן יהיה לבצע שחזור אמין ומהיר של המידע.
- 11.9. הנהלת נותן השירות תגדיר נהלי עבודה אשר יאפשרו תפעול תקין ונאות של הליכי הזיהוי מרחוק בנותן השירות. נהלי עבודה אלו יסדירו, בין היתר, את ההיבטים הבאים:
 - (א) האמצעים הטכנולוגיים באמצעותם ניתן לבצע את הליכי הזיהוי מרחוק. ככל שרלוונטי, לצורך קביעת אמצעים אלו יוגדרו דרישות טכנולוגיות מינימאליות בהתאם לפתרון המיושם (כגון: תנאי הצילום, אופן ותנאי הצילום והצגת תעודות הזיהוי¹, דרישות חומרה מינימאליות, עדכניות ותקפות אמצעי הזיהוי והסיסמאות).
 - (ב) הנסיבות אשר בהתקיימן לא ניתן לאפשר שימוש בהליכי זיהוי מרחוק או לחילופין נדרש יהיה להפסיק את השימוש בהליכי זיהוי מרחוק.
 - (ג) בקורות ותהליכי ניטור אשר נדרש לשלב בהליכי הזיהוי מרחוק.
 - (ד) אסדרת המידע אשר יימסר למקבל השירות בטרם ביצוע הליך הזיהוי. מידע זה יכול, בין היתר, הסבר על מהות ואופן ביצוע הליך הזיהוי, פירוט אודות המסמכים והמידע

¹ לדוגמה, דרישות לעניין מאפייני זיהוי ייחודיים ופרטי לבוש של הלקוח (משקפיים, שיער פנים) וכן דרישות טכניות כגון: תאורה מספקת, היעדר השתקפות או צל, גודל צילום תעודות הזיהוי וכו'.

אשר יידרש למסור והבהרה כי מידע ונתונים אלו, כמו גם מידע ונתונים טכניים אשר יאספו במהלך הליך הזיהוי, עשויים להישמר על ידי נותן השירות.

(ה) לעניין הזדהות שוטפת בערוצי התקשורת השונים – אופן מסירת אמצעי ההזדהות, צמצום הסיכון לגניבה או העתקה של אמצעי ההזדהות, גישת עובדי נותן השירות ועובדי ספק מיקור החוץ לאמצעי ההזדהות, ניטור התקפות ואירועים חשודים, אפשרויות עדכון פרטיו האישיים של מקבל השירות המשמשים בתהליכי הזיהוי, וקבלת הסכמת מקבל השירות לפעילות בערוצים המקוונים.

(ו) תהליכים שיבטיחו שמירה וגיבוי של המידע והנתונים המתקבלים בהליכי הזיהוי מרחוק.

פרק ד' - זיהוי מרחוק

12. אמצעי זיהוי מרחוק

זיהוי ואימות ראשוני מרחוק של מקבל שירות לצורך קבלת הסכמתו, יכול להיעשות באחת מהדרכים הבאות:

12.1. **באמצעות שימוש בטכנולוגיה להיוועדות חזותית (Video Conference)** – כמפורט בסעיף

16 להוראה, זאת, על ידי משתמשים בנתוני אשראי בלבד.

12.2. **באמצעות טכנולוגיה לזיהוי מרחוק** אשר יכולה להיעשות באמצעות שימוש

באינטראקציה חזותית בזמן אמת או באמצעות צילום וידאו **שלא בזמן אמת** – כמפורט בסעיף 17 להוראה.

12.3. **באמצעות אמצעי אחר לזיהוי מרחוק** שאינו נמנה על האמצעים המפורטים לעיל או בתקנות, אשר יבטיח זיהוי ברמת מהימנות גבוהה - כמפורט בסעיף 18 להוראה.

13. נותן שירות המבקש לעשות שימוש באמצעי הזיהוי המפורטים בסעיפים 12.1-12.3 לעיל, נדרש להעביר לממונה דיווח מראש, לשם קבלת התייחסותו, ולפעול בהתאם למפורט בפרק ח' להוראה.

14. למרות האמור, נותן שירות שהינו תאגיד בנקאי וכן נותן שירותי אשראי או מפעיל מערכת לתיווך אשראי שכפוף לחוזר רשות שוק ההון, פטור מהוראות סעיף 13, במקרה בו הוא מקבל את הסכמת הלקוח במעמד הליך פתיחת חשבון באופן מקוון או במעמד הליך ביצוע זיהוי מקוון, בהתאמה לנותן השירות, המבוצע בהתאם להוראות מאסדר נותן השירות.

15. נותן שירות יבחן את הצורך להגדיר סוגי לקוחות **כלקוחות בסיכון גבוה** אשר בעבורם לא יתאפשר זיהוי מרחוק לצורך קבלת הסכמתם להעברת דוח אשראי לגביהם. כמו כן, נותן השירות נדרש לקבוע אירועים אשר בהתרחשותם יופסק הליך הזיהוי מרחוק.

16. זיהוי ואימות באמצעות טכנולוגיה להיוועדות חזותית

זיהוי ואימות באמצעות טכנולוגיה להיוועדות חזותית ייעשה על ידי הצגת תעודת זהות ותעודת זיהוי רשמית נוספת שהונפקה על ידי מדינת ישראל ונושאת את שם הלקוח, מספר תעודת הזהות



שלו ותאריך לידתו, ובשילוב **ביצוע העברה בנקאית** של סכום אקראי באמצעות חשבון על שם מקבל השירות, בתאגיד בנקאי בישראל.

17. זיהוי ואימות באמצעות טכנולוגיה לזיהוי מרחוק

17.1. זיהוי ואימות באמצעות טכנולוגיה לזיהוי מרחוק (להלן - **הטכנולוגיה**) יעשה על ידי

שימוש באינטראקציה חזותית **בזמן אמת** או באמצעות צילום וידאו **שלא בזמן אמת**, וישלב בהליך, לכל הפחות, את כלל הבקורות הבאות:

(א) בדיקת מקוריות התעודה המזהה המוצגת על ידי מקבל השירות. הבדיקה יכולה להתבצע, בין היתר, בהתבסס על מאפייני התעודה², שלמות התעודה, מיקום ועקביות פרטי המידע המנויים בתעודה;

(ב) אימות כי התעודה המזהה המוצגת היא אכן התעודה של מקבל השירות המזדהה, בין היתר באמצעות השוואת התמונה שבתעודה המזהה לתמונת מקבל השירות המתקבלת באמצעות הטכנולוגיה;

(ג) אימות פרטי מקבל השירות המזדהה, ולכל הפחות מספר הזיהוי שלו ותאריך הנפקת התעודה המזהה אל מול מאגרי מידע רשמיים;

(ד) שימוש בטכנולוגיה לטובת רישום פרטי הלקוח המזהה מתוך התעודה המזהה שלו, ולכל הפחות, שימוש בטכנולוגיה לטובת רישום מספר הזהות של הלקוח ותאריך הנפקת התעודה;

17.2. במקרה של שימוש בטכנולוגיה לזיהוי מרחוק אשר אינה משלבת אינטראקציה חזותית בזמן אמת, נדרש לשלב בהליך, בנוסף, את כלל הבקורות הבאות:

(א) בדיקת חיות – בדיקה המוודאת כי הלקוח המזדהה הינו אדם ממשי;

(ב) בדיקת החיות, כאמור בסעיף 17.2(א) לעיל תעשה במקשה אחת, עם השוואת תמונות הלקוח כאמור בסעיף 17.1(ב) לעיל, ללא הפסקה ביניהם.

(ג) צפייה שוטפת מדגמית של נציגי נותן השירות בתיעוד הדיגיטלי הנשמר, על מנת לוודא את נאותות ההליך המיושם, שישמש כאמצעי בקרה וייעשה בהתאם למדיניות ניהול הסיכונים של נותן השירות.

17.3. זיהוי ואימות באמצעות הטכנולוגיה יבוצע בהסתמך על **ספים טכנולוגיים מינימליים** שטכנולוגיה כאמור תידרש לעמוד בהם, על מנת להבטיח כי ההליך יאפשר זיהוי לקוח ברמת מהימנות גבוהה.

18. זיהוי ואימות באמצעות אמצעי אחר לזיהוי מרחוק

18.1. נותן שירות המעוניין לזהות את לקוחותיו באמצעות **אמצעי אחר לזיהוי מרחוק** שאינו נמנה על האמצעים המפורטים בתקנות ובהוראה זו, נדרש להעביר לממונה דיווח מראש ולפעול בהתאם למפורט בפרק ח' להוראה.

² לדוגמה, גודל וסוג הפונט בתעודה וחיתמת זיהוי של הגורם המנפיק את התעודה.



18.2. אמצעי הזיהוי כאמור לעיל, והטכנולוגיה העומדת בבסיסו, נדרשים לאפשר לנותן השירות לזהות את לקוחותיו ברמת מהימנות גבוהה, תוך נקיטת אמצעים לצמצום הסיכון המובנה הכרוך בביצוע זיהוי מרחוק.

פרק ה' - שימוש בספק מיקור חוץ לביצוע הליכי זיהוי ואימות מרחוק

19. נותן שירות רשאי לעשות שימוש בספק מיקור חוץ לצורך ביצוע הליכי זיהוי מרחוק, ובלבד שיעמוד, לכל הפחות, בדרישות הוראה זו, ובכלל זה, יעביר לממונה דיווח ויפעל בהתאם למפורט בפרק ח'.

20. שימוש בספק מיקור חוץ יבוצע בהתאם לעקרונות הבאים:

20.1. טרם בחירת ספק מיקור החוץ ואסדרת ההתקשרות עמו, נותן השירות יודא כי לספק מיקור החוץ יש את הטכנולוגיה, המיומנות והידע המקצועי הנדרשים לאספקת שירותי זיהוי מרחוק באופן מהימן, מתמשך ובהתאם לדרישות הדין והרגולציה.

20.2. שימוש נותן השירות במיקור חוץ אינו גורע מאחריות נותן השירות לקיום מכלול הדינים וההוראות החלים עליו, ובפרט נותן השירות אינו רשאי להעביר לספק מיקור חוץ את האחריות שחלה עליו כלפי לקוחותיו ובהתאם לכל דין.

20.3. נותן השירות יעגן את התקשרותו עם ספק מיקור החוץ בחוזה בכתב. חוזה ההתקשרות יכלול התייחסות, בין היתר, להיבטים הבאים:

(א) אסדרת יחסי הצדדים לחוזה במתן שירותי הליכי זיהוי, לרבות הגדרת הפעילויות אשר יבוצעו על ידי כל אחד מהצדדים, והגדרת הזכויות והחובות של ספק מיקור החוץ;

(ב) הגדרת אחריות ספק מיקור החוץ כלפי נותן השירות וכלפי מקבלי השירות המזדהים, לרבות אחריותו גם במקרה בו ספק מיקור החוץ עושה שימוש בקבלני משנה;

(ג) הגדרת רמת שירות (SLA) ונהלי המשכיות עסקית;

(ד) הגדרת חובות ספק מיקור החוץ לעניין אבטחת מידע, גיבוי, חובת סודיות והגנת פרטיות הלקוחות המזדהים;

(ה) מתן אפשרות לנותן השירות לבצע ביקורות על פעילות ספק מיקור החוץ, לרבות זכות נותן השירות לקבל גישה למידע ולנתונים הנשמרים בהליכי הזיהוי של מקבלי שירות שהם לקוחותיו;

(ו) איסור על ספק מיקור החוץ להעביר לצד שלישי מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות וללא אישור מראש של נותן השירות;

(ז) בעת הצורך בהעברת נתונים, יבוצע תהליך של גישה מבוקרת לנתונים פרטניים וללא שכפול כלל בסיס הנתונים.

20.4. נותן השירות יבחן את סיכוני אבטחת המידע והגנת הסייבר הגלומים בהתקשרות ויקבע צעדים לצמצום.

20.5. נותן השירות יודא כי ספק מיקור החוץ פועל בהתאם להוראות כל דין, ובכלל זה תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 והנחיית רשם מאגרי מידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע", וכן בהתאם להוראה זו.

20.6. נותן השירות יגבש ויקיים תהליכי בקרה וניטור על הליכי הזיהוי מרחוק המבוצעים על ידי ספק מיקור החוץ.

20.7. נותן השירות יודא כי ספק מיקור החוץ יגבש ומקיים נהלים לעניין שמירה, גיבוי ואבטחת המידע של הנתונים, המסמכים והמידע הנאספים בתהליכי הזיהוי מרחוק.

20.8. אספקת שירותי תחזוקה מרחוק על ידי ספק מיקור חוץ תעשה תוך ניהול סיכונים הולם ונקיטת צעדים לצמצום הסיכונים הגלומים בביצוע שירותי תחזוקה כאמור.

20.9. נותן השירות יגדיר תכנית לביצוע סקרי הערכת סיכוני אבטחת מידע אצל ספקי מיקור חוץ המאחסנים או מעבדים נתונים של נותן השירות. רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון, ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות הגנה על המידע ולזהות חשיפות לסיכונים אלו. הסקרים יבוצעו בתדירות המותאמת לרמת הסיכון ולקצב עדכון התהליכים ומערכות הספק, ולכל הפחות אחת ל-24 חודשים.

21. נותן שירות אשר כפוף להוראות מאסדר נותן השירות בנושא של מיקור חוץ, רשאי להגיש לממונה בקשת פטור מסעיף 20, ולנמק את בקשתו זו.

פרק ו' – הזדהות שוטפת ועדכון שם ופרטי התקשרות של לקוח קיים

22. **הזדהות שוטפת** של לקוח מול נותן השירות, תתאפשר רק לאחר השלמת הליך זיהוי ראשוני אשר יבוצע באחת מהדרכים המפורטות להלן, ובתנאי שסוכמו עם הלקוח אמצעי זיהוי (גורמי אימות) להתקשרות עתידית:

22.1. זיהוי ואימות ראשוני כמפורט בסעיף 12 להוראה זו או בהתאם לסעיף 5 לתקנות.

22.2. זיהוי ואימות ראשוני כפי שנדרש לצורך פתיחת חשבון או לצורך זיהוי מקוון של לקוח על ידי נותן שירות שהינו תאגיד בנקאי או נותן שירותי אשראי או מפעיל מערכת לתיווך אשראי, בהתאם להוראות כל דין, לרבות צו איסור הלבנת הון החל עליו והוראות לעניין זה שניתנו על ידי מאסדר נותן השירות.

23. הזדהות שוטפת תתאפשר רק אם היא מבוססת על זיהוי באמצעות **שני גורמי אימות** לפחות.

24. יש להתאים את אמצעי הזיהוי באמצעותם ניתן לבצע הזדהות שוטפת לערוץ השירות ולסיכונים הגלומים בשימוש באותו הערוץ.

25. **עדכון פרטי התקשרות עם לקוח** המשמשים לצורך אימות זהותו (כגון: מספר טלפון נייד, כתובת דואר אלקטרוני) או **עדכון שם הלקוח**, יתאפשרו רק לאחר זיהוי ואימות באמצעות **שני גורמי אימות לפחות**.

פרק ז' - שמירת הנתונים ששימשו לזיהוי מרחוק

26. נותן שירות ישמור עותק דיגיטלי של הליך הזיהוי מרחוק המבוצע על ידו, באופן התואם את אמצעי הזיהוי בו נעשה שימוש. תיעוד זה יכול שיכלול: הקלטת תקשורת הווידאו, צילום או סריקת מסמכי הזיהוי ומסמכים נלווים נוספים, וכל מידע ונתונים אחרים ששימשו לצורך הבטחת זיהוי הלקוח ברמת מהימנות גבוהה.
27. שמירת עותק דיגיטלי כאמור תעשה תוך גיבוי ואחסונו בצורה מאובטחת, בשליטת נותן השירות ובאופן שיבטיח את נגישות נותן השירות לנתונים, ללא אפשרות לעריכתם.
28. על אף האמור לעיל בסעיפים 26 ו-27 לעיל, נותן שירות שהינו תאגיד בנקאי וכן נותן שירותי אשראי או מפעיל מערכת לתיווך אשראי שכפוף לחוזר רשות שוק ההון, רשאי לפעול בהתאם להוראות מאסדר נותן השירות לעניין שמירת הנתונים ששימשו לזיהוי מרחוק.

פרק ח' – אמצעי זיהוי שיש לדווח בגינו לממונה

29. נותן שירות המבקש לבצע זיהוי ואימות של מקבל שירות באמצעות אחד מאמצעי הזיהוי המפורטים בסעיפים 16-18 לעיל, נדרש לדווח על כך לממונה לפחות 90 יום מראש, ולקבל את הסכמתו.
30. דיווח נותן השירות לממונה, יכלול, לכל הפחות, את המידע והנתונים הבאים:
- (א) תיאור הליך הזיהוי המבוקש;
 - (ב) תיאור הטכנולוגיה העומדת בבסיס אמצעי הזיהוי ומאפייניה;
 - (ג) שמות ופרטי ספקי הטכנולוגיות בהן נעשה שימוש בהליך הזיהוי;
 - (ד) תיאור הבקורות והבדיקות המשולבות בהליך הזיהוי;
 - (ה) ספים טכנולוגיים מינימליים לזיהוי ואימות וודאי;
 - (ו) סוגי לקוחות, שירותים ואירועים שבהתקיימם לא יתאפשר שימוש באמצעי זיהוי מרחוק או יופסק הליך הזיהוי מרחוק;
 - (ז) ככל שנעשה שימוש **בספק טכנולוגיה** (גורם שפיתח את המערכת שבאמצעותה נעשה זיהוי מרחוק), **הסכם בכתב** בין נותן השירות לבין ספק הטכנולוגיה באמצעותה נעשה שימוש בהליך הזיהוי, המסדיר את יחסי הצדדים, הזכויות, החובות והאחריות של הצדדים, באופן אשר יבטיח עמידה בהוראות הדין, הוראות לעניין הגנת הפרטיות ודרישות הוראה זו.
 - (ח) הצהרת המנהל הכללי של נותן השירות או חבר ההנהלה האחראי לנושא, כי אמצעי הזיהוי המבוקש נבחן ונמצא כי השימוש בו תואם את הדרישות המפורטות בהוראה זו, וכן כי בוצע תהליך הערכת סיכונים סדור, הן לאמצעי הזיהוי והן לספקי הטכנולוגיות הרלוונטיים, וכי לא נמצאו סיכונים מהותיים העשויים להשפיע על מהימנות זיהוי מקבלי השירות;



(ט) **אישור כי התקבלה חוות דעת מומחה של ספק הטכנולוגיה**, בדבר נאותות אמצעי הזיהוי המבוקש, ובכלל זה, נאותות הטכנולוגיה העומדת בבסיס אמצעי הזיהוי, הפוטנציאל לזיהוי שגוי ועמידת ההליך בדרישות הדין ודרישות הוראה זו.

31. נותן השירות ימנה גורם בלתי תלוי, אשר יבצע בחינה לנאותות אמצעי הזיהוי ועמידת אמצעי הזיהוי בדרישות הוראה זו ובדרישות חוק רלוונטיות. תוצאות הבחינה וצעדים לטיפול בממצאים ככל שיעלו, יועברו לעיון הממונה בתום 12 חודשים ממועד תחילת השימוש באמצעי הזיהוי.

32. נותן שירות שהינו תאגיד בנקאי וכן נותן שירותי אשראי או מפעיל מערכת לתיווך אשראי אשר כפוף לחוזר רשות שוק ההון ועושה שימוש באחד מאמצעי הזיהוי המפורטים בסעיפים 16-18, ישלח לממונה את התייחסות מאסדר נותן השירות לאמצעי הזיהוי כאמור, בצירוף המידע שהעביר למאסדר לצורך שימוש באמצעי הזיהוי, וזאת בכדי שהממונה יוכל להביא מידע זה בחשבון בעת בחינת פניית נותן השירות. יובהר כי נותן שירות כאמור, אינו רשאי להסתמך באופן בלעדי על ההליכים שקיים מול המאסדר.

הממונה רשאי לדרוש השלמת מסמכים ומידע, לרבות בהתאם לסעיף 30. זאת, לצורך מתן הסכמתו לשימוש באמצעי הזיהוי בהתאם לסעיף 29.

33. נותן השירות ימסור לממונה דיווח טרם ביצוע שינוי מהותי בשירות או בטכנולוגיה באמצעותה מתבצע זיהוי מרחוק.

פרק ט' - דיווחים לממונה על אירועי אבטחת מידע וסייבר או על חשד ממשי לאירועים כאמור

34. נותן שירות נדרש לדווח לממונה על אירועי אבטחת מידע וסייבר בהליכי הזיהוי מרחוק המופעלים על ידי נותן השירות או על ידי ספק מיקור חוץ, או על חשד ממשי לאירועים כאמור, בהתאם לסוגי האירועים המפורטים להלן (להלן – **אירוע מחייב דיווח**):

- 34.1. אירוע אשר להערכת נותן השירות יש לו השפעה מהותית על מתן השירות.
- 34.2. אירוע אשר לצורך הטיפול בו נדרשת מעורבות משמעותית של מנהל הגנת הסייבר או הגורם האחראי על נושא זה בארגון, ואשר הטיפול בו לא הסתיים תוך שעתיים ממועד זיהויו לראשונה.
- 34.3. אירוע המשפיע על מספר רב של לקוחות. לעניין זה, השפעה על מספר רב של לקוחות תיבחן על ידי כל נותן שירות בהתייחס לגודלו ולמספר לקוחותיו העושים שימוש בתהליכי הזיהוי מרחוק.

34.4. אירוע שהינו בעל מאפייני תקיפה חדשים או רמת מורכבות גבוהה.

34.5. כל אירוע דלף מידע מהותי שלא נכלל לעיל.

35. הדיווח לממונה על אירוע מחייב דיווח יועבר באמצעות דיווח טלפוני או דיווח בכתב בתוך שעתיים ממועד זיהויו כאירוע המחייב דיווח (להלן – **דיווח ראשוני**). השלמת הדיווח (להלן – **דיווח משלים**) תתבצע בכתב בתוך 8 שעות ממועד הדיווח הראשוני (אם מועד הדרישה להשלמת הדיווח בכתב חל שלא בשעות העבודה המקובלות, הוא יועבר בכתב עם תחילת שעות העבודה



המקובלות של היום העוקב). דיווח בכתב על אירוע שכמעט והתרחש יועבר לממונה תוך 7 ימים ממועד הזיהוי של האירוע.

ככל שתהיינה התפתחויות מהותיות במהלך האירוע, יש לעדכן את הממונה על התפתחויות אלו. כמו כן, יש לעדכן את הממונה על סיום האירוע.

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 זיהוי כאירוע המחייב דיווח, לפי המוקדם מביניהם.

36. הדיווחים בכתב כאמור לעיל יימסרו **בהתאם לפורמט הדיווח** שבנספח א' להוראה זו 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.

37. בהתייחס לדיווחים בכתב כאמור לעיל, נותן שירות רשאי לעשות שימוש בפורמט הדיווח על אירועי אבטחת מידע וסייבר שקבע מאסדר נותן השירות ובלבד שהעברתם לממונה תהיה בהתאם למפורט בהוראה זו, לרבות לעניין האירועים המחייבים דיווח וכן, זמני הדיווח הנדרשים.

פרק י' - ביקורת פנימית

38. הביקורת הפנימית, לרבות מבקר חיצוני הפועל מטעם נותן השירות, תכלול בתוכנית הביקורת הרב שנתית התייחסות להליכי הזיהוי מרחוק המופעלים על ידי נותן השירות, וכן תדון, תבחן ותוודא כי ממצאי הביקורת הפנימית מובאים לידיעת ההנהלה והדירקטוריון.

פרק יא' - תחילה והוראות מעבר

39. תחילתה של הוראה זו ביום 5 בספטמבר 2021 (להלן – **יום התחילה**); ואולם, נותן שירות שאינו ערוך ליישום ההוראה ביום התחילה, רשאי לפעול בהתאם לדרכי הזיהוי אשר נקבעו בתקנות (1)5 ו-10(1) טרם תיקון, וזאת **למשך 6 חודשים** ממועד התחילה.

39א. על אף האמור בסעיף 39 לעיל, נותן שירות שהוא מיופה כוח בתמורה רשאי לפעול בהתאם לדרכי הזיהוי אשר נקבעו בתקנה (1)5 טרם תיקונה, וזאת **עד ליום 31.12.22**. אין באמור כדי להפחית מהצורך לעמוד בכל יתר דרישות הוראה זו, בהתאמות הנדרשות.

40. על אף האמור בסעיף 39 לעיל, מועד התחילה של פרק ט' בנושא דיווחים לממונה על אירועי אבטחת מידע וסייבר או על חשד ממשי לאירועים כאמור, יהיה לא יאוחר מ-3 חודשים ממועד התחילה.



נספח א' להוראה 401A - פורמט דיווח לממונה

דיווח לממונה על אירועי אבטחת מידע וסייבר או על חשד ממשי לאירועים 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	<u>יש לסמן את סוג הדיווח:</u> ☐ דיווח ראשוני ☐ דיווח משלים ☐ דיווח על התפתחויות מהותיות במהלך האירוע ☐ דיווח על סיום האירוע ☐ דיווח על אירוע שכמעט והתרחש ☐ הפקת לקחים והמלצות ליישום
נושא האירוע	<u>יש לסמן את סוג האירוע:</u> ☐ אירוע אבטחת מידע או אירוע סייבר ☐ חשד לאירוע אבטחת מידע או לאירוע סייבר
תיאור האירוע (לרבות פירוט פגיעה במידע / תהליכים/ מערכות/לקוחות/ נזק אחר כולל 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
הפקת לקחים מהאירוע והמלצות ליישום	מלל חופשי (יש לצרף דוח)
האם האירוע דווח למאסדר של נותן השירות או לרשות אכיפה	שם המאסדר/ הרשות: _____ הגורם אליו הועבר הדיווח: _____ תאריך העברת הדיווח: DD/MM/YYYY

הבהרות:

- 1 - **דיווחים בכתב** יש להעביר באמצעי מאובטח קיים בין נותן השירות 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 כמחייב דיווח. ככל שהדיווח הראשוני יימסר טלפונית הוא יועבר על פי פרטי הקשר שנמסרו לנותן השירות. ככל שהדיווח הראשוני יימסר בכתב הוא יועבר בהתאם למפורט בסעיף 1 לעיל, תוך מילוי הפרטים הידועים בעת מסירת הדיווח. בנוסף, יש לוודא קבלתו ע"י נציגי הממונה בסמוך לאחר שליחתו.
- 3 - **דיווח משלים** יימסר תוך 8 שעות ממועד הדיווח הראשוני, תוך מילוי הפרטים הידועים בעת מסירת הדיווח.