

13 בפברואר 2025

ט"ו בשבט תשפ"ה

הוראה לחברות תשלומים ליישום חובות איסור הלבנת הון באמצעות טכנולוגיה לזיהוי מקוון

הוראה לפי סעיף 11(ג)1 לחוק איסור הלבנת הון, התש"ס – 2000 וסעיפים 4(ב), 5(ו) ו-8(ג) לצו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של חברת תשלומים למניעת הלבנת הון ומימון טרור), התשפ"ד – 2024.

רקע כללי

חוק הסדרת העיסוק בשירותי תשלום וייזום תשלום התשפ"ג-2023 (להלן גם – **החוק** או **חוק הסדרת העיסוק בשירותי תשלום**) מסמיך את רשות ניירות ערך (להלן – **הרשות**) להעניק רישיונות ולפקח על חברות אשר עוסקות בשירותי תשלום חוץ בנקאיים.

השירותים אשר מוסדרים במסגרת החוק ואשר יחייבו רישיון מאת הרשות הם: הנפקה של אמצעי תשלום; סליקה של פעולת תשלום; ניהול חשבון תשלום – שלושתם פעולות תשלום קלאסיות. בנוסף החוק מאפשר שני סוגים חדשים ומתקדמים של שירותים טכנולוגיים שהם ייזום מתקדם וייזום בסיסי, אלו יאפשרו ביצוע קל ונוח של העברות בנקאיות, באופן שיאפשר לייצר חלופה תחרותית לשימוש בכרטיסי אשראי לצורך ביצוע תשלומים לבתי עסק.

רוב שירותי התשלום המוסדרים במסגרת החוק הם בעלי מאפיינים מקוונים ודיגיטליים, כך שלרוב חברות התשלומים אין סניפים, אלא הן מציעות את שירותיהן באופן מקוון בלבד.

מטרתו העיקרית של החוק היא לעודד את התחרות בשוק שירותי התשלום באמצעות יצירת אפשרות שווה לגורמים חוץ בנקאיים, ישראלים ובינלאומיים, להיכנס לתחום זה ולהתפתח בו, לצד השחקנים הבנקאיים הקיימים בשוק, והכול תוך שמירה על עניינם של הלקוחות. על מנת להגשים מטרה זו הוחלט לבסס את החוק על סטנדרטים בינלאומיים, בהתאמות הנדרשות, ובפרט, על שתי הדירקטיבות האירופאיות המסדירות את שירותי התשלום באירופה – ה- Payment PSD2 Services Directive¹ וה- Electronic Money Directive (EMD) (להלן – **הרגולציה האירופאית**)².

¹ [Directive \(EU\) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market](#)

² [Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions](#)

דברי הסבר

צו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של חברת תשלומים למניעת הלבנת הון ומימון טרור), התשפ"ד – 2024 (להלן – **הצו או צו איסור הלבנת הון של חברות התשלומים**) אושר בכנסת באוגוסט האחרון, ומועד כניסתו לתוקף נקבע חצי שנה מפרסום הוראה בעניין אמצעים דיגיטליים חלופיים לזיהוי ואימות. בהתאם לכך, ההוראה נועדה לאפשר לחברות התשלומים לזהות ולאמת לקוח באופן מקוון, ללא הכרח במפגש פיזי עימו, תוך הבטחת אמינות הזיהוי והפחתת סיכוני הלבנת ההון ומימון טרור הנובעים משימוש באמצעים חלופיים אלו.

הוראה זו מפרטת את הדרכים בהן על חברת התשלומים ליישם את החובות החלות עליה על פי צו איסור הלבנת הון כאשר היא מזהה ומאמתת זהותם של לקוחות באמצעות טכנולוגיה לזיהוי מקוון, לרבות לעניין אופן יישום החובות להכרת הלקוח, קבלת הצהרה על נהנה ובעל שליטה, ניהול סיכוני הלבנת הון ומימון טרור, קביעת מדיניות, ביצוע בקרות, שמירה על מסמכים שהתקבלו במסגרת ההליך המקוון, קביעת מדיניות וניהול סיכונים בהקשר של זיהוי באמצעים החלופיים כאמור.

בדומה לתכליות אשר עמדו בבסיס חקיקת חוק הסדרת העיסוק בשירותי תשלום, אשר התבסס על עקרונות הרגולציה האירופאית על מנת להתאים את הרגולציה הישראלית לסטנדרטים בינלאומיים, גם הוראות צו איסור הלבנת הון של חברות התשלומים הותאמו במידת האפשר, במהלך הליך החקיקה, לעקרונות בינלאומיים מתקדמים ומקובלים בתחום הלבנת הון ומימון טרור ולהתפתחויות הטכנולוגיות בתחום. כך למשל, הביטוי "**חתימת מקור**" אשר מבטא חתימה בכתב ידו של הלקוח אשר מופיע בצווי איסור הלבנת הון אחרים, הוחלף במסגרת הדיונים שהתקיימו בוועדת החוקה, חוק ומשפט של הכנסת, בדרישה לכך ש"**ההצהרה תיעשה באופן שבו ניתן לאמת את זהות המצהיר**" על מנת לאפשר לחברות התשלומים לפעול באופן דיגיטלי מול לקוחותיהם, כפי שנעשה בעולם. דוגמא נוספת היא הקביעה בצו שעל נותן השירות לשמור העתק ממסמך זיהוי **אחד** של הלקוח, חלף **שני** מסמכים הקבועים בצווי איסור הלבנת הון אחרים בישראל. יצוין כי שינוי זה תואם אף הוא לסטנדרטים המקובלים בעולם³ וכן נותן מענה לסוגיות שעלו במסגרת הדיונים בוועדת החוקה, חוק ומשפט, של שמירה על פרטיות הלקוחות וצמצום חשיפות בתחום אבטחת המידע. בנוסף, במסגרת הצו ניתנו הקלות רבות לנותני שירות ייזום מתקדם ברמת סיכון נמוכה, וניתן פטור מרישום פרטי זיהוי של מקבל שירות מזדמן בסיכון נמוך על בסיס מסמך זיהוי, מקום שבוצעה פעולה בסכום נמוך.

יודגש, כבר היום, גופים פיננסיים שונים כגון בנקים, נותני אשראי חוץ בנקאי וחברי בורסה, מבצעים זיהוי מקוון ללקוחות לפי הוראות שהוציאו הרגולטורים הפיננסיים מכוח ובהתאם לצווי איסור

³ ראו לעניין זה את הסקירה הבינלאומית שצורפה להצעת ההוראה - דוח הערכת רגולציה (RIA)

הלבנת הון החלים על גופים אלו. הוראה זו נקבעה גם היא מכוח חוק איסור הלבנת הון וצו איסור הלבנת הון של חברות התשלומים ונכתבה ברוח השינויים שנקבעו בו, תוך התאמה לדרישות המקובלות בעולם ולהתפתחויות הטכנולוגיות. לפיכך, ההוראה קובעת מספר הסדרים אשר שונים מהוראות הזיהוי המקוון החלות על הגופים הפיננסיים האחרים במשק ואשר מטרתם לאפשר פתיחה של אפשרויות שונות ומתקדמות לזיהוי מקוון, תוך הבטחה לזיהוי אמין ומדויק של לקוחות ושמירת תכליות חוק איסור הלבנת הון. כך למשל, וכפי שיוסבר בהרחבה בהמשך, ההוראה מאפשרת לזהות באופן מקוון גם מי שהוא מקבל שירות שאינו תושב ישראל, תוך קביעת בקרות מוגברות על זיהוי זה. דוגמא נוספת היא הוספת הגדרה בדבר "טכנולוגיה לאימות מקוון" שמאפשרת לחברות התשלומים לאמץ דרכים דיגיטליות חלופיות לצורך אימות זהותו של מקבל השירות, כגון אימות באמצעות שימוש בבנקאות פתוחה או בהעברה בנקאית סמלית. ההוראה אף מאפשרת לבצע הליך זיהוי ואימות של מקבל השירות באמצעות שימוש במסמך זיהוי אחד במקום שניים, וכן להצהיר על נהנה ובעל שליטה באמצעי חלופי שיאשר הממונה (שאינו בהצהרה קולית בהכרח, כפי שקיים בהוראות הזיהוי המקוון הקיימות).

סעיף 1 – סעיף ההגדרות

לעניין הגדרת "מקבל שירות" – הגדרה זו כוללת מקבל שירות שהוא יחיד תושב ישראל, יחיד שהוא תושב חוץ, ובלבד שהמדינה או הטריטוריה של מקבל השירות אינן מן המנויות בתוספת הראשונה לצו, תאגיד הרשום בישראל וגוף מוכר, בין אם מקבל השירות פועל עבור נהנה ובין אם אינו פועל עבור נהנה.

לעניין הגדרת "טכנולוגיה לאימות מקוון" – הגדרה זו כוללת טכנולוגיות לאימות זהותו של מקבל השירות, כגון, בנקאות פתוחה (כהגדרתה בחוק שירות מידע פיננסי, התשפ"ב – 2021), העברה בנקאית סמלית או אמצעי אימות חלופי שיאשר הממונה בהיוועצות עם הרשות המוסמכת.

סעיף 2 – תנאים מקדימים ועקרונות לשימוש בטכנולוגיה לזיהוי מקוון

נוכח הסיכונים הכרוכים בזיהוי מקוון, ההוראה קובעת תנאים אשר בהתקיימם בלבד רשאי נותן השירות לעשות שימוש בטכנולוגיה לזיהוי מקוון, כמפורט להלן.

סעיף 2(א) – ביצוע הערכת סיכונים

בהתאם לחובות הקבועות בסעיף 20 לצו, לצורך ניהול והפחתת הסיכונים הכרוכים בזיהוי מקוון, על נותן השירות לזהות, להבין ולהעריך את סיכוני הלבנת הון ומימון טרור הטמונים בזיהוי מקוון, וליישם תכנית למזעור הסיכונים שזוהו, לרבות הטמעת בקרות מתאימות. בעניין זה על נותן השירות להבחין, בין היתר, בין מקבל שירות שהוא יחיד תושב ישראל למקבל שירות שהוא תושב חוץ או תאגיד הרשום בישראל.

סעיף 2(ב) ו-3 – קביעת מדיניות ואחריות הדירקטוריון

בהתאם לחובות הקבועות בסעיף 20 לצו, נותן השירות נדרש לקבוע מדיניות לשימוש בטכנולוגיה לזיהוי מקוון, אשר תכלול, לכל הפחות, התייחסות לנושאים הקבועים בהוראה. על הדירקטוריון לדון ולאשר את המדיניות, לרבות מסגרת לניהול סיכוני הלבנת הון ומימון טרור הנובעים מהליך הזיהוי המקוון, אחת לשנתיים לפחות ובכל שינוי מהותי בפעילות של נותן השירות, בסוג השירותים המוצע, או בסביבה העסקית, הטכנולוגית או הרגולטורית של נותן השירות.

בנוסף, הדירקטוריון נדרש לדון ולאשר מראש את אפשרות השימוש בזיהוי מקוון, ובכלל זה את הטכנולוגיה שתשמש את נותן השירות בביצוע זיהוי מקוון.

הדירקטוריון נדרש לוודא את יישומה ויעילותה של המדיניות לזיהוי מקוון, מעת לעת ובהתאם להערכת הסיכונים, וזאת, בין היתר, על ידי קביעת נהלי עבודה וקבלת דיווחים שוטפים בעניין זה.

סעיף 4 – אחראי זיהוי מקוון

במסגרת החובות הקבועות בסעיף 20 לצו, על מנת לוודא יישום מדיניות השימוש בטכנולוגיה לזיהוי מקוון, כפי שאושרה על ידי הדירקטוריון, ולצורך פיקוח ובקרה על השימוש בטכנולוגיה זו, נקבע כי נותן השירות ימנה כאחראי לזיהוי מקוון את אחראי איסור הלבנת הון ומימון טרור בנותן השירות, או חבר הנהלה בנותן השירות או מי שכפוף במישרין לחבר הנהלה. עוד נקבע, כי האחראי לזיהוי מקוון יהיה עצמאי במילוי חובותיו וימלא את תפקידיו באפקטיביות. הסעיף מפרט את תפקידיו של האחראי, הכוללים בין היתר, לוודא קביעת נהלי עבודה לתהליך גיוס עובדים העוסקים בזיהוי מקוון, לרבות בחינת מהימנותם, מיומנותיהם הנדרשות והתאמתם לתפקיד. בנוסף, הסעיף מפרט את הנושאים בהם יש לוודא קביעת נהלים בנותן השירות הכוללים, בין היתר, הגדרת הנסיבות אשר בהתקיימן יופסק תהליך הזיהוי המקוון, בהתאם לניהול הסיכונים של נותן השירות.

סעיף 5 – ביקורת פנימית

בהתאם לחובות הקבועות בסעיף 20 לצו, תפקידה של הביקורת הפנימית, בין היתר, לבחון את תקינותם ויעילותם של תהליכי ניהול הסיכונים בתחום איסור הלבנת הון ומימון טרור בעת ההתקשרות לשם מתן שירות באמצעות טכנולוגיה לזיהוי מקוון, קיומן של חולשות בבקורות הפנימיות ושיפור הליכי הבקרה בתחום פעילות זה.

סעיף 6 – הליכי זיהוי מקוון

נותן השירות רשאי לזהות מקבל שירות שהוא יחיד, מיופה כוח מטעם מקבל שירות שהוא תאגיד, מיופה כוח מטעם מקבל שירות שהוא גוף מוכר בהתאם לסעיף 4(א)(6) לצו או נהנה, באופן מקוון, באמצעות אחת משתי הדרכים שנקבעו בסעיף 6 להוראה.

זיהוי מקבל השירות והנהנה שיעשה באמצעות טכנולוגיה לזיהוי מקוון בהתאם ובכפוף לתנאים שיקבעו בהוראה, יחשב כזיהוי פנים אל פנים שאושר על ידי יו"ר הרשות בהתאם לסמכותו לפי סעיף 8(ג) לצו.

כך, בהתאם להוראות סעיף 4(ב) לצו, אימות פרטי הזיהוי כנדרש בסעיף 4(א)(1) ו-4(א)(2) לצו יכול להתבצע באמצעות טכנולוגיה להיוועדות חזותית, חלף הצגת מסמך זיהוי או העתק מאושר (כהגדרת מונח זה בצו) של מסמך הזיהוי. זיהוי מקבל השירות באמצעות היוועדות חזותית יעשה על פי מסמך זיהוי של מקבל השירות, ונותן השירות נדרש לאמת את פרטי מקבל השירות, כפי שנקראו מתוך תעודת הזהות אל מול מרשם האוכלוסין או לאמת את פרטי מקבל השירות, כפי שנקראו מתוך מסמך הזיהוי באמצעות מסמך זיהוי נוסף או לאמת את פרטי מקבל השירות באמצעות טכנולוגיה לאימות מקוון.

כמו כן, בהתאם להוראות סעיף 4(ב) לצו אימות פרטי הזיהוי כנדרש בצו יכול להתבצע באמצעות טכנולוגיה לזיהוי חזותי, חלף הצגת מסמך זיהוי או העתק מאושר (כהגדרת מונח זה בצו) של מסמך הזיהוי. זיהוי באמצעות טכנולוגיה לזיהוי חזותי יעשה באמצעות מסמך זיהוי של מקבל השירות אשר יוצג לנותן השירות בעת ההתקשרות לקבלת השירות באמצעות הטכנולוגיה. כמו כן, על מנת להגביר את הודאות לגבי מקוריות התעודה וכי היא שייכת למקבל השירות, נוספו מספר בקרות טכנולוגיות המפורטות בהוראה.

בעניין זה יובהר כי ניתן, אך אין חובה, להשוות את פרטי הזיהוי עם מרשם האוכלוסין או לאמת את פרטי הזיהוי עם מסמך נוסף הנושא תמונה ומספר זיהוי של מקבל השירות, כמפורט בסעיף 4(א)(1) ו-4(א)(2) לצו. הוראות פרק אלו מאפשרות למקבל השירות לחלופין לעשות שימוש בבנקאות פתוחה, העברה בנקאית סמלית או טכנולוגיות אחרות לצורך אימות פרטי הזיהוי של מקבל השירות.

סעיף 7 – טכנולוגיה להיוועדות חזותית (Video Conference)

הליכי זיהוי ואימות של מקבל שירות שהוא יחיד המתבצעים באמצעות טכנולוגיה להיוועדות חזותית המחייבת תקשורת וידאו ואודיו בזמן אמת, יעשו על פי מסמך זיהוי אחד, כמפורט בהוראה.

נותן השירות נדרש לאמת את פרטי מקבל השירות, כפי שנקראו מתוך תעודת הזהות אל מול מרשם האוכלוסין או לאמת את פרטי מקבל השירות, כפי שנקראו מתוך מסמך הזיהוי, באמצעות מסמך זיהוי נוסף, או לאמת את פרטי מקבל השירות כפי שנקראו מתוך מסמך הזיהוי, באמצעות טכנולוגיה לאימות מקוון.

סעיף 8 – טכנולוגיה לזיהוי חזותי

טכנולוגיה לזיהוי חזותי מבוססת על תקשורת וידאו היכולה להיות בזמן אמת או שלא בזמן אמת. אם מקבל השירות בוחר לעבור את תהליך הזיהוי שלא בזמן אמת, נקבעו בהוראה בקרות נוספות על התהליך וזאת על מנת לוודא כי התמונה המוצגת בתהליך הזיהוי והאימות היא של אדם ממשי ולא תוצאה של מניפולציה טכנולוגית כלשהי, וכי הליך הזיהוי של מקבל השירות נעשה כדיון. כמו כן, נקבעו בקרות על מנת להגביר את הודאות לגבי מקוריות המסמך ולהבטיח שהוא שייך למקבל

השירות. נותן השירות נדרש לוודא כי האיכות הטכנית של הטכנולוגיה (כגון איכות תקשורת ואיכות תמונת הוידאו) תהיה גבוהה, כך שהזיהוי והאימות יבוצעו ברמת ודאות גבוהה.

בקרה נוספת הקיימת היא כי הטכנולוגיה לא תאפשר הזנה של פרטי זיהוי מסוג מספר זיהוי ותאריך הנפקת מסמך הזיהוי, ככל שהאימות מבוצע מול מרשם האוכלוסין או מול מסמך זיהוי נוסף או מול טכנולוגיה לאימות מקוון, אלא על הטכנולוגיה להזין בעצמה פרטים אלה מתוך מסמך הזיהוי. את שאר פרטי הזיהוי המפורטים בסעיף 3(א) לצו מקבל השירות יכול להזין בעצמו ובלבד שנציג נותן השירות יבדוק שדות אלה אל מול מסמך הזיהוי של מקבל השירות.

כמו כן, נקבעה בקרה של אימות למספר הטלפון של מקבל השירות באמצעות OTP.

בעניין זה יצוין כי בסעיף 2(ג) להוראה נקבעה החובה לקבל מספק הטכנולוגיה לזיהוי חזותי חוות דעת מומחה, שהינו בלתי תלוי וחיצוני לספק הטכנולוגיה. על חוות הדעת להיות ערוכה כדין, בהתאם לתוספת הראשונה לפקודת הראיות, שתפרט, בין היתר, את יכולות המערכת שפיתח, אופן ביצוע הזיהוי ואימות הזהות והפוטנציאל לזיהוי שגוי. חוות דעת זו היא חלק מתהליך שעל חברה לבצע על מנת לבחון את יכולות המערכת כאמור והיא נועדה בראש ובראשונה לשרת תהליך זה. בנוסף, חוות הדעת האמורה עשויה לשמש בסיס לבחינת טענות משפטיות, ככל שיעלו בהליכים משפטיים שיבקשו לתקוף את מהימנות תהליכי הזיהוי והאימות הזהות שמבצע ספק הטכנולוגיה.

סעיף 9 – מקבל שירות מזדמן

נותן השירות רשאי לבצע הליך רישום של מקבל שירות מזדמן באמצעות טכנולוגיה להיוועדות חזותית או טכנולוגיה לזיהוי חזותי. לחלופין, ניתנת לו האפשרות לבצע זאת באמצעות טכנולוגיה לאימות מקוון, כגון בנקאות פתוחה או העברה בנקאית סמלית לבחירתו.

סעיף 10 – מקבל שירות שהוא גוף מוכר

נותן השירות רשאי לבצע זיהוי מקוון למקבל שירות שהוא גוף מוכר באמצעות טכנולוגיה להיוועדות חזותית או טכנולוגיה לזיהוי חזותי, לאחר שהוא נוכח לדעת באמצעות מסמך, כי מקבל השירות מוסמך לפעול בשם הגוף המוכר. נותן השירות יבדוק את אמיתות המסמך על פניו.

סעיף 11 – מקבל שירות שהוא תאגיד

ההוראה מאפשרת לנותן שירות לקבל את המסמך הנדרש בהתאם לסעיף 4(א)(3) לצו, לגבי מקבל שירות שהוא תאגיד, באופן מקוון, כשהוא חתום בחתימה אלקטרונית, כהגדרתה בחוק חתימה אלקטרונית, התשס"א – 2001, של עורך הדין, העונה על תכליות הוראות הצו בעניין זה, וזאת חלק מסמך מקור או העתק מאושר כהגדרתו בצו.

סעיף 12 – קבלת הצהרה על נהנה ובעל שליטה

בהתאם להוראות הצו, על נותן השירות לקבל ממקבל השירות במעמד ההתקשרות, הצהרה באופן שבו ניתן יהיה לאמת את זהות המצהיר, אם הוא פועל בשביל עצמו או בשביל נהנה, וכן הצהרה על פרטי הזיהוי של בעל השליטה, כאשר מקבל השירות הוא תאגיד.

על מנת לאפשר קבלת הצהרות אלו באופן מקוון, נקבע כי מקבל השירות יחתום על הצהרות כאמור באופן מקוון, ובלבד שנותן השירות יתעד את מקבל השירות מצהיר על הנדרש בקולו. כחלופה להצהרה הקולית נותן השירות יוכל לקבל חתימה מקוונת על הצהרה בה מקבל השירות יהיה מחויב לאשר כי קרא והבין את משמעות הצהרתו טרם חתימתו המקוונת עליה. נותן השירות יבצע אימות של מקבל השירות באמצעות סיסמה חד פעמית (OTP) בסמוך לפני החתימה על ההצהרה המקוונת. מקבל השירות יוכל להצהיר על הנדרש גם באמצעי חלופי שיאשר הממונה בהיוועצות עם הרשות המוסמכת. דרישות אלה חלות הן בשימוש בטכנולוגיה להיוועדות חזותית והן בטכנולוגיה לזיהוי מקוון.

כמו כן, נקבע כי במקרה שמקבל השירות פועל בשביל נהנה, נותן השירות יתעד את מקבל השירות באמצעות אחת החלופות המוזכרות בסעיף כי הוא פועל בעבור נהנה, ויבצע זיהוי מקוון גם לנהנה עצמו באחת הדרכים הנזכרות בסעיפים 7 או 8.

סעיף 13 – זיהוי מקוון באמצעות צד שלישי

שימוש בשירותי מיקור חוץ טומן בחובו סיכונים ובהם אספקת שירותים באיכות נמוכה, תלות בנותן שירות במיקור חוץ, ניגוד עניינים פוטנציאלי בין נותן שירות במיקור חוץ ופעילויותיו האחרות ובין נותן השירות ולקוחותיו, דליפת מידע רגיש, חשש להיעדר בקרות מספקות ומנגנוני פיקוח.

על כן, באופן העולה בקנה אחד עם המלצות ארגון ה-FATF⁴, נקבע כי מיקור חוץ של פעילות הנוגעת לביצוע זיהוי מקוון יבוצע על ידי נותן שירות במיקור חוץ שיימצא מתאים להענקת שירותים אלה מבחינת הטכנולוגיה, המיומנות והידע המקצועי שברשותו, ובלבד שהיחסים בינו לבין נותן השירות הוסדרו בהסכם כתוב ומוגדר היטב, וכן כי נותן השירות יטמיע אמצעי בקרה ופיקוח אפקטיביים על השירותים שמסופקים במיקור חוץ.

כמו כן, יובהר כי שימוש בשירותי מיקור חוץ לא מפחית או מעביר חובות ואחריות שחלות על נותן השירות לפי הוראות הדין.

סעיף 14 – הליך הכרת הלקוח

מטרת סעיף זה להבהיר כי ככל שנותן השירות בחר לזהות ולאמת את זהותו של מקבל השירות באמצעות טכנולוגיה לזיהוי מקוון, אין עליו חובה לבצע גם את הליך "הכר את הלקוח" באמצעות

⁴ הבהרה להמלצה מספר 17, עמוד 87 לעדכון מסמך ההמלצות של FATF, נובמבר 2023.

שימוש בטכנולוגיה לזיהוי מקוון, ובלבד שנותן השירות נקט באמצעים סבירים כדי לוודא כי המשיב לשאלון הכרת הלקוח ומקבל השירות המזוהה והמאומת, הם אותו אדם.

עוד נקבע בהוראה כי מקבל שירות שהוא תושב זר, אשר זוהה באמצעות טכנולוגיה לזיהוי מקוון, יסומן ככזה במערכות המחשב של נותן השירות ויבוצע בו מעקב מוגבר למשך תקופה שתקבע על ידי נותן השירות, ובהתאם להערכת הסיכונים שביצע נותן השירות. יחד עם זאת, רמת הסיכון של מקבל השירות שזוהה באופן מקוון תקבע ותותאם להליך הכרת הלקוח שיבוצע לו.

סעיף 15 – שמירה ואבטחת מידע

ההוראה קובעת כי נותן השירות ישמור עותק דיגיטלי של תהליך הזיהוי של מקבל השירות במלואו, לרבות של סרטון הוידאו או של רצף האירועים שצולמו, וסריקת מסמך הזיהוי ומסמכים נוספים שהוצגו באמצעות הטכנולוגיה לזיהוי מקוון. בעניין זה יודגש כי אין בהוראה כדי לגרוע מחובות נותן השירות לפי תקנות הגנת הפרטיות, ובכלל זה ההוראות המתייחסות למאגר מידע הכולל מידע ביומטרי.

על נותן השירות לוודא כי מידע רגיש הכולל פרטים אישיים ומסמכים מזהים של מקבלי השירות, יאוחסן בשרת מאובטח בפני גישה של גורמים שאינם מורשים, ויגובה באופן תדיר. יצוין כי שמירה כאמור תחייב הודעה למקבל השירות, בהתאם לחובות המפורטות בסעיף 11 לחוק הגנת הפרטיות, ומתן הסכמתו לכך.

אחד התנאים הנדרשים מנותן השירות על מנת שיהיה רשאי לעשות שימוש באישור יו"ר רשות ניירות ערך לבצע זיהוי פנים אל פנים ולבצע אימות פרטי הזיהוי באמצעות זיהוי מקוון כאמור לעיל, הוא החובה ליידיע את מקבל השירות על המידע שישמר. בכלל זה על נותן השירות ליידיע את מקבל השירות על כך שנאסף ונשמר אודותיו מידע ביומטרי, לאיזה צורך ישמר המידע, הגורמים אשר עשויים להיות בעלי נגישות למידע ומשך הזמן שהמידע ישמר, וכן לגבי הסיכונים הקשורים באבטחת המידע והגנת הפרטיות ויקבל את הסכמת מקבל השירות לכך, והכל בהתאם לחוק הגנת הפרטיות.

תנאי הכרחי נוסף שנועד לאפשר לתקף ראייתית את תהליך הזיהוי באמצעות טכנולוגיה לזיהוי חזותי, קובע כי על נותן השירות לבצע תהליך חד פעמי לעריכת רשומה מוסדית של הליך הזיהוי המקוון כאמור. תהליך זה ייסתמך על חוות דעת של גורם משפטי אצל נותן השירות, אשר תתייחס לתנאים להוכחת רשומה מוסדית, כמפורט בסעיף 36(א) לפקודת הראיות. הרשומה המוסדית תכלול את הסרטון או את רצף האירועים שצולמו במהלך ההזדהות החזותית באמצעות הטכנולוגיה, כך שיתאפשר במסגרת חקירה או הליך משפטי להתרשם באופן ישיר, ללא תיווך של עד מומחה, האם האדם שבעניינו מתנהל ההליך המשפטי הוא זה שמצולם.

הן שמירת הסרטון או רצף האירועים שצולמו במהלך ההזדהות החזותית באמצעות הטכנולוגיה לזיהוי חזותי, הן שמירת הסרטון שצולם במהלך ההיוועדות החזותית, והן שמירת הסרטון שבו

תועד מקבל השירות מצהיר בנוגע לנהנה או לבעל שליטה, נדרשות לצרכי בקרה פנימית וחיצונית. הן נדרשות בין היתר גם על מנת שבמהלך חקירה או הליך משפטי ניתן יהיה להתרשם באופן ישיר, האם האדם שבעניינו או בקשר אליו מתנהל ההליך המשפטי הוא זה שמצולם.

לעניין הוראה זו יודגש כי במקרה של זיהוי באמצעות טכנולוגיה לזיהוי חזותי, נותן השירות נדרש לשמור את מספר הטלפון, מספר ה"ברזל" (IMEI) של מכשיר הטלפון הנייד, אם קיים, כמו גם כתובת IP ממנה ניתן השירות, אם קיימת.

סעיף 16 – אמצעי ניטור, בקרה על הפעילות וניהול סיכונים

לצורך יישום סעיפים 2, 14, ו-20 לצו, בהתאם למדיניות ניהול הסיכונים ולרמת הסיכון של מקבל השירות, נותן השירות ישקול שלא לבצע את הליך הזיהוי באמצעות טכנולוגיה לזיהוי מקוון או להפסיקו, או לחסום את פעילות שירותי התשלום של הלקוח או לחזק את הליכי הזיהוי באמצעים נוספים, והכל לפי מידת הסיכון והעניין. במקרה שעלה חשש להתנהגות בלתי רגילה של מקבל השירות, על נותן השירות לשקול לזהות את מקבל השירות פנים אל פנים ו/או להגיש דיווח על פעולה בלתי רגילה או שלא לפתוח את החשבון כלל, והכל בהתאם לנסיבות ומידת הסיכון.

עוד נקבע כי על נותן השירות, המבצע זיהוי מקוון, למפות את הסיכונים הייחודיים ולקבוע דרכים לצמצם סיכונים אלה. בנוסף, עליו להטמיע מערך ניטור ובקרה ייעודי שבין היתר, יזהה פעולות חריגות שיבוסס גם על אנומליות טכנולוגיות, תפעוליות ועסקיות.

סעיף 17 – אישור יו"ר הרשות

נותן השירות המעוניין לעשות שימוש בטכנולוגיה לזיהוי חזותי נדרש לקבל לכך את אישור יו"ר הרשות. על נותן השירות להגיש בקשה לקבלת אישור כאמור, תוך הצגת המידע הנדרש בסעיף. בנוסף, הסעיף מבהיר כי כל שינוי מהותי בטכנולוגיה או בשירות הניתן על ידי נותן השירות באמצעות הטכנולוגיה, מחייב קבלת אישור יו"ר רשות ניירות ערך בטרם יישמו.

קביעת בחינה תקופתית ביחס להוראה

סעיף 36 לחוק עקרונות האסדרה, התשפ"ב-2021 (להלן – "חוק עקרונות האסדרה"), שנכנס לתוקף בינואר 2023, קובע הוראות לעניין ביצוע בחינה תקופתית ביחס לאסדרה חדשה. בהתאם להוראות הסעיף, בכל אסדרה חדשה, למעט הצעת חוק, יש לקבוע הוראה לעניין בחינתה בתום תקופה שתיקבע בהוראה כאמור, שלא תעלה על עשר שנים מיום כניסתה לתוקף של האסדרה.

במסגרת הבחינה, יש לבחון אם ובאיזו מידה הושגו היעדים שלשם השגתם נקבעה האסדרה ואם האסדרה עדיין נדרשת בהתחשב במטרות שלשמן נקבעה או מטעמים אחרים. כמו כן, בתום הבחינה התקופתית, על רשות ניירות ערך לפרסם לציבור דוח בדבר ממצאי הבחינה, ובו יצוין המועד הבא לביצוע הבחינה התקופתית שיהיה לא יאוחר מעשר שנים לאחר תום הבחינה הקודמת.

לאור האמור לעיל, בחינה ראשונה של הוראה זו תתבצע בתום 10 שנים מיום תחילתה.

להלן נוסח ההוראה

הוראה לחברות תשלומים ליישום חובות איסור הלבנת הון באמצעות טכנולוגיה לזיהוי מקוון

מתוקף סמכותי לפי סעיף 11ג(ג)(1) לחוק איסור הלבנת הון, התש"ס – 2000 (להלן: "החוק") וסעיפים 4(ב), 5(ו) ו-8(ג) לצו איסור הלבנת הון (חובות זיהוי, דיווח וניהול רישומים של חברת תשלומים למניעת הלבנת הון ומימון טרור), התשפ"ד – 2024 (להלן: "הצו" או "צו איסור הלבנת הון") להלן הוראותיי:

1. הגדרות

"**בנקאות פתוחה**" – אימות זהותו של מקבל השירות על ידי קבלת מידע ממקור מידע באמצעות מערכת הממשק למידע פיננסי כהגדרת מושגים אלו בחוק שירות מידע פיננסי;

"**גוף מוכר**", "**מקבל שירות מזדמן**", "**תאגיד**", "**תושב**", "**תושב חוץ**" – כהגדרתם בצו;

"**הליך הכר את הלקוח**" – הליך הכרת הלקוח לפי סעיף 2 לצו;

"**העברה בנקאית סמלית**" – תהליך אימות במסגרתו מתקבל אצל נותן השירות סכום מדויק של כספים מחשבון הבנק של מקבל השירות;

"**זיהוי מקוון**" – הליכי זיהוי ואימות פרטי זיהוי של מקבל שירות המתבצעים באחת מהדרכים המפורטות בסעיף 6 להוראה;

"**חוק הגנת הפרטיות**" – חוק הגנת הפרטיות, התשמ"א – 1981;

"**חוק שירות מידע פיננסי**" – חוק שירות מידע פיננסי, התשפ"ב – 2021;

"**חתימה אלקטרונית**" – כהגדרתה בחוק חתימה אלקטרונית, התשס"א – 2001;

"**טכנולוגיה להיוועדות חזותית**" – טכנולוגיה המאפשרת תקשורת בין שני מוקדים או יותר, שבה מועברים תמונת וידאו ואודיו בזמן אמת, ובלבד שתהא מאובטחת ומוצפנת לצורך מניעת זליגת מידע, לשמירת סודיות ומהימנות המידע;

"טכנולוגיה לזיהוי חזותי" - טכנולוגיה לזיהוי המבוססת על תקשורת וידאו בין נותן השירות למקבל השירות. תקשורת כאמור יכולה להיות באמצעות אינטרקציה חזותית בזמן אמת או באמצעות צילום וידאו שלא בזמן אמת; ובלבד שתהיה מאובטחת ומוצפנת לצורך מניעת זליגת מידע, לשמירת סודיות ומהימנות המידע;

"טכנולוגיה לזיהוי מקוון" - טכנולוגיה להיוועדות חזותית או טכנולוגיה לזיהוי חזותי המשמשת לזיהוי מקוון;

"טכנולוגיה לאימות מקוון" - בנקאות פתוחה, העברה בנקאית סמלית או אמצעי אימות חלופי שיאשר הממונה בהיוועדות עם הרשות המוסמכת;

"מסמך זיהוי" – אחד מאלה:

- (א) תעודת זהות;
- (ב) תעודת עולה עד 30 ימים מיום הנפקתה;
- (ג) רישיון נהיגה תקף הכולל את תמונת בעל הרישיון;
- (ד) דרכון ישראלי תקף שניתן לפי חוק הדרכונים, התשי"ב – 1952;
- (ה) אם מקבל השירות הוא תושב חוץ – לפי דרכון חוץ או תעודת מסע;

"מקבל השירות" – אחד מאלה:

- 1. יחיד שהוא תושב;
- 2. יחיד שהוא תושב חוץ;
- 3. תאגיד הרשום בישראל;
- 4. גוף מוכר;

"ספק טכנולוגיה" - הגורם שפיתח את הטכנולוגיה לזיהוי חזותי. פותחה הטכנולוגיה על ידי נותן השירות עצמו, יחולו הסעיפים הקשורים לספק הטכנולוגיה בהוראה זו, בשינויים המחויבים, ביחס לנותן השירות;

"פקודת הראיות" – פקודת הראיות (נוסח חדש), התשל"א – 1971;

"תקנות הגנת הפרטיות - אבטחת מידע" - תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017.

2. תנאים מקדימים ועקרונות לשימוש בטכנולוגיה לזיהוי מקוון

נותן שירות רשאי לזהות ולאמת מקבל שירות באמצעות טכנולוגיה לזיהוי מקוון, בכפוף לקיומם של התנאים המפורטים להלן:

א. ביצוע הערכת סיכונים

(1) בהתאם לחובה הקבועה בסעיף 20 לצו – באחריות נותן השירות לזהות, להבין ולהעריך סיכוני הלבנת הון ומימון טרור הכרוכים במתן שירות באמצעות טכנולוגיה לזיהוי מקוון, וליישם תכנית למזעור הסיכונים שזוהו, לרבות הטמעת בקרות מתאימות והטלת מגבלות, והכל בהתאם לגישה מבוססת סיכון. הערכת הסיכונים תתבצע הן ברמת מקבל השירות הבודד והפעולה הבודדת והן בראייה רוחבית של הפעילות המתקיימת אצל נותן השירות, ותוך הבחנה בין מקבל שירות שהוא יחיד ומקבל שירות שאינו יחיד.

(2) במסגרת הערכת הסיכונים נדרש נותן השירות להבנת מרכיבי הטכנולוגיה לזיהוי מקוון וכיצד הם עונים על דרישות של זיהוי ואימות לפי הצו. על נותן השירות להתייחס לרמת הוודאות ("assurance level") של הטכנולוגיה לזיהוי מקוון ולקבוע ספים טכנולוגיים מינימליים שטכנולוגיה כאמור תידרש לעמוד בהם, על מנת שניתן יהיה להסתמך עליה לצורך מתן השירות.

ב. קביעת מדיניות לשימוש בטכנולוגיה לזיהוי מקוון

בהתאם לחובה הקבועה בסעיף 20 בצו – באחריות נותן השירות לקבוע מדיניות לזיהוי מקוון (להלן – **מדיניות לזיהוי מקוון**) אשר תכלול, לכל הפחות, התייחסות לנושאים הבאים:

(1) הגדרת מאפייני השירות לגביהם ניתן לעשות שימוש בטכנולוגיה לזיהוי מקוון, לרבות סוגי השירותים הניתנים, רמת הסיכון של מקבל השירות, ובכלל זה התייחסות לסיכון של מקבל שירות שהוא יחיד תושב ישראל לעומת מקבל שירות שהוא תושב חוץ או תאגיד הרשום בישראל, היקף הפעילות הן ברמת הפעולה הבודדת והן ברמת היקף הפעילות הכולל, ומאפייני הפעילות.

(2) זיהוי, הבנה והערכה של סיכוני הלבנת הון ומימון טרור הטמונים בתהליך מתן שירות למקבל שירות שזוהה ואומת באמצעות טכנולוגיה לזיהוי מקוון, ויישום תכנית למזעור הסיכונים, כמפורט בסעיף 2(א)(1) לעיל.

(3) קביעת בקרות ואמצעי ניטור שוטפים על השימוש בטכנולוגיה לזיהוי מקוון, כמפורט בסעיף 16 להלן.

(4) קביעת דרישות טכנולוגיות מינימאליות לשם הסתמכות על הליך זיהוי מקוון לצורך מתן השירות, בהתאם להערכת הסיכונים שביצע נותן השירות.

(5) הגדרת דרישה לאיכות טכנית של הטכנולוגיה לזיהוי מקוון (כגון איכות תקשורת ואיכות התמונה והקול), כך שהזיהוי יבוצע ברמת ודאות גבוהה.

(6) שמירה, אבטחה וגיבוי של המידע שמתקבל בהליך הזיהוי המקוון בהתאם לסעיף 15 להלן.

(7) קביעת עקרונות אבטחת מידע בתקשורת בין מקבל השירות לבין נותן השירות.

(8) הגדרת משאבים נאותים אשר יוקצו לצורך ביצוע הליכי זיהוי מקוון של מקבלי השירות (לרבות כוח אדם מיומן וציוד טכני).

(9) קביעת בעלי תפקידים בנותן השירות, אחריותם וסמכותם בכל הנוגע להליך הזיהוי המקוון.

ג. נותן שירות המבקש להשתמש בזיהוי באמצעות טכנולוגיה לזיהוי חזותי, יגיש לרשות חוות דעת מומחה שהוא בלתי תלוי וחיצוני לספק הטכנולוגיה. על חוות הדעת להיות ערוכה כדון, בהתאם לתוספת הראשונה לפקודת הראיות, ולפרט, בין היתר, את יכולות המערכת של ספק הטכנולוגיה אופן ביצוע הזיהוי ואימות הזהות והפוטנציאל לזיהוי שגוי.

ד. נותן שירות המבקש להשתמש בזיהוי באמצעות טכנולוגיה לזיהוי חזותי, נדרש לקבל את אישור יו"ר הרשות לכך, כמפורט בסעיף 17 להלן.

3. אחריות הדירקטוריון בנותן השירות

במסגרת יישום החובות הקבועות בסעיף 20 לצו, על הדירקטוריון בנותן השירות, בין היתר:

א. להעריך לפחות אחת לשנה את מידת האפקטיביות של הערכת הסיכונים בנותן השירות לעניין שימוש בטכנולוגיה לזיהוי מקוון, ולנקוט אמצעי בקרה ופיקוח מתאימים להבטיח את עדכונה במידת הצורך.

ב. לדון ולאשר מראש את אפשרות השימוש בזיהוי מקוון ובכלל זה את הטכנולוגיה לזיהוי מקוון שתשמש לצורך כך.

ג. לדון ולאשר את מדיניות השימוש בטכנולוגיה לזיהוי מקוון, לרבות מסגרת לניהול סיכוני הלבנת הון ומימון טרור הנובעים מהליך הזיהוי המקוון אחת לשנתיים לפחות ובעת כל שינוי מהותי בפעילות של נותן השירות, בסוג השירותים המוצע, או בסביבה העסקית, הטכנולוגית או הרגולטורית של נותן השירות.



- ד. לנקוט אמצעי בקרה ופיקוח מתאימים להבטיח את יישומה ויעילותה של המדיניות לזיהוי מקוון, מעת לעת, בהתאם לצורך ולהערכת הסיכונים.
- ה. לנקוט אמצעי בקרה ופיקוח מתאימים להבטיח כי עיקרי המדיניות לזיהוי מקוון הובאו לידיעת העובדים הרלוונטיים.
- ו. לנקוט אמצעי בקרה ופיקוח מתאימים להבטיח קביעת נהלי עבודה לצורך יישום המדיניות לזיהוי מקוון והבטחת יישומם.
- ז. לקבוע דיווחים נדרשים בקשר לזיהוי מקוון, לרבות מהאחראי לזיהוי מקוון כאמור בסעיף 4(ג)2 להלן, ובכלל זה הגדרת מקבלי הדיווחים, מועדי הדיווחים, אירועים חריגים וכשלים בעלי השפעה מהותית המחייבים דיווח מיידי, ומתכונתם.
- ח. לנקוט אמצעי בקרה ופיקוח מתאימים להבטיח כי נותן השירות הקצה משאבים נאותים לניהול סיכונים, יישום בקרות ואמצעי ניטור וכי נקבעו תחומי אחריות ברורים והוקצו מנהלים ועובדים בעלי כישורים וניסיון מתאימים.
- ט. לנקוט אמצעי בקרה ופיקוח מתאימים להבטיח כי נותן השירות הקצה משאבים נאותים למעקב אחרי התפתחויות טכנולוגיות בתחום הטכנולוגיה לזיהוי מקוון והסיכונים הכרוכים בהן.
- י. לדון בממצאי הביקורת הפנימית הקשורים לתחום הזיהוי המקוון, וכן לעקוב אחר יישום ההמלצות או תיקון הליקויים שנמצאו בביקורת.
- 4. אחראי לזיהוי מקוון**
- א. במסגרת יישום המדיניות שקבועה בסעיף 20 לצו, נותן השירות ימנה אחד מאלה לתפקיד אחראי לזיהוי מקוון:
- 1) אחראי איסור הלבנת הון ומימון טרור שמונה לפי סעיף 8 לחוק.
 - 2) חבר הנהלה בנותן השירות או מי שכפוף במישרין לחבר הנהלה.
- ב. לאחראי לזיהוי מקוון יהיו העצמאות, הסמכות, הבכירות, המשאבים, הכישורים הידע והניסיון לבצע את תפקידיו באפקטיביות.
- ג. באחריותו של האחראי לזיהוי מקוון, בין היתר:
- 1) לייעץ לדירקטוריון ולהנהלה בנושא זיהוי מקוון.
 - 2) לדווח לדירקטוריון בקשר לשימוש בזיהוי מקוון בהתאם לסעיף 3(ז) לעיל.

- (3) לוודא את יישום המדיניות לזיהוי מקוון אצל נותן השירות ולפקח על אופן השימוש בטכנולוגיה לזיהוי מקוון ועל הסיכונים הגלומים בה.
- (4) לעקוב אחר התפתחויות טכנולוגיות בתחום הזיהוי המקוון, והסיכונים הכרוכים בהן.
- (5) לוודא כי נותן השירות קבע נהלי עבודה לזיהוי מקוון ופועל ליישומם, לרבות בנושאים שלהלן:
- א. תהליך גיוס עובדים העוסקים בזיהוי מקוון, בחינת מהימנותם, מיומנותם והתאמתם לתפקיד.
 - ב. האיכויות הטכניות של הטכנולוגיה לזיהוי מקוון, ובכלל זה איכות התקשורת, התמונה והקול ואופן ותנאי הצילום של מסמכי הזיהוי ושל מקבל השירות (כגון: רציפות תמונה וקול, רזולוציה, ניגודיות, בהירות, תאורה, גודל תמונה).
 - ג. הליך זיהוי מקוון של מקבל שירות תוך התייחסות לסיכוני הלבנת הון ומימון טרור המאפיינים את מקבל השירות, ובכלל זה מקבל שירות שאינו יחיד או פעילות באמצעות מיופה כוח.
 - ד. נסיבות בהתקיימן יופסק תהליך הזיהוי המקוון, שיתייחסו הן להיבטים טכנולוגיים והן לרמת הסיכון של מקבל השירות.
 - ה. תסריטי שיחה לביצוע ההליך מול מקבל השירות שיכללו בן היתר הסבר מפורט על תהליך הזיהוי המקוון, הבהרה כי הליך הזיהוי המקוון, לרבות המסמכים הנלווים שנמסרו על ידו, מתועדים ונשמרים אצל נותן השירות, וקבלת הסכמת מקבל השירות לאמור, כמפורט בסעיף 14(ו) להלן.
 - ו. הגברת מודעות מקבל השירות לסיכונים הגלומים בזיהוי מקוון, לרבות אלו הקשורים באבטחת מידע ובהגנת הפרטיות, באופן שיתרום להפחתת סיכונים אלו.
- (6) להנחות את העוסקים בזיהוי מקוון ולקבוע עבורם תכנית הכשרה, שתעודכן מעת לעת ובהתאם לצורך.

5. ביקורת פנימית

1. במסגרת יישום החובות הקבועות בסעיף 20 לצו, הביקורת הפנימית תערוך בחינה עצמאית ובלתי-תלויה ותספק לדירקטוריון הערכה אובייקטיבית לגבי מידת הציות של כלל הגורמים והפעילויות, מערכות ותהליכים הנוגעים להיבטי הזיהוי המקוון בנותן השירות, וזאת אל מול מסמכי מדיניות ונהלים פנימיים של נותן השירות ודרישות חיצוניות, לרבות הוראות הדין הרלוונטיות.

2. הביקורת הפנימית תבחן באופן תקופתי, בין היתר, את תקינותם ויעילותם של תהליכי ניהול הסיכונים בתחום איסור הלבנת הון ומימון טרור בעת התקשרות לשם מתן שירות באמצעות זיהוי מקוון, קיומן של חולשות בבקורות הפנימיות ושיפור הליכי הבקרה בתחום פעילות זה.

6. הליכי זיהוי מקוון

בכפוף לקיום הדרישות הקבועות בהוראה זו נותן השירות רשאי לבצע זיהוי של מקבל שירות ואימות פרטי הזיהוי שלו בהתאם לנדרש בסעיפים 4(א)(1), 4(א)(2), 4(א)(3), 4(א)(6) ו-8 לצו, באופן מקוון, ובאחת מהדרכים הנזכרות בסעיפים 7 או 8 להלן.

7. טכנולוגיה להיוועדות חזותית (Video Conference)

הליכי זיהוי ואימות של מקבל שירות שהוא יחיד המתבצעים באמצעות טכנולוגיה להיוועדות חזותית, יעשו כדלקמן:

א. הליכי הזיהוי והאימות יתבצעו על פי מסמך זיהוי הנושא את שם הלקוח, מספר הזיהוי שלו ותאריך לידה.

ב. מקבל השירות ישלח לנותן השירות העתק של מסמך הזיהוי באמצעות דואר אלקטרוני או באמצעים אלקטרוניים אחרים.

ג. נותן השירות יזהה את מקבל השירות באמצעות טכנולוגיה להיוועדות חזותית (video conference) על פי מסמך הזיהוי, שיוצג לנותן השירות על ידי מקבל השירות במהלך ההיוועדות החזותית.

ד. נותן השירות יזהה את מקבל השירות אל מול תמונת הפנים המופיעה במסמך הזיהוי ששלח מקבל השירות כאמור בסעיף 7(ב) לעיל.

ה. נותן השירות יאמת את פרטי מקבל השירות, כפי שנקראו מתוך תעודת הזהות אל מול מרשם האוכלוסין או יאמת את פרטי מקבל השירות, כפי שנקראו מתוך מסמך הזיהוי באמצעות טכנולוגיה לאימות מקוון, או יאמת את פרטי מקבל השירות כפי שנקראו מתוך מסמך הזיהוי עם מסמך זיהוי נוסף כנדרש בסעיף 4(א)(1) ו-4(א)(2) לצו.

ו. ההיוועדות החזותית תוקלט ותישמר בהתאם לאמור בסעיף 15 להלן, ובכלל זה ירשם וישמר שמו של נציג נותן השירות שערך את ההיוועדות החזותית.



8. טכנולוגיה לזיהוי חזותי

הליכי זיהוי ואימות של מקבל שירות שהוא יחיד המתבצעים באמצעות טכנולוגיה לזיהוי חזותי, יעשו כדלקמן:

- א. נותן השירות יבצע את הליכי הזיהוי והאימות על פי מסמך זיהוי של מקבל השירות אשר יוצג לנותן השירות במעמד מתן השירות, תוך שימוש בטכנולוגיה לזיהוי חזותי.
- ב. נותן השירות יאמת באמצעות הטכנולוגיה לזיהוי חזותי את מקוריות מסמך הזיהוי (Authenticity) המוצגת על ידי מקבל השירות שהוא יחיד. בדיקה זו תתבצע, לכל הפחות, על סמך המאפיינים הקבועים של אותו המסמך וסימני הביטחון שהוטמעו בו, בחינת שלמות המסמך ושלמות ועקביות של הפרטים המצויים על המסמך.
- ג. שדה מספר הזיהוי יירשם באמצעות הטכנולוגיה לזיהוי חזותי ללא אפשרות של עדכון השדה על ידי מקבל השירות במקרה שהטכנולוגיה לא זיהתה את הכתוב במסמך הזיהוי.
- ד. עדכון מקבל שירות את פרטי הזיהוי המפורטים בסעיף 3(א) לצו, למעט מספר זיהוי, נדרש נותן השירות לבדוק את השדה שנערך על ידי מקבל השירות אל מול מסמך הזיהוי.
- ה. נותן השירות יאמת באמצעות הטכנולוגיה לזיהוי חזותי כי מסמך הזיהוי הוא אכן המסמך של מקבל השירות, ובכלל זה, אימות באמצעות השוואת התמונה שבמסמך לתמונה ברורה של מקבל השירות שצולמה באמצעות הטכנולוגיה.
- ו. נותן השירות יאמת את פרטי מקבל השירות, כפי שנקראו מתוך תעודת הזהות אל מול מרשם האוכלוסין או יאמת את פרטי מקבל השירות כפי שנקראו מתוך מסמך הזיהוי באמצעות טכנולוגיה לאימות מקוון, או יאמת את פרטי מקבל השירות כפי שנקראו מתוך מסמך הזיהוי עם מסמך זיהוי נוסף כנדרש בסעיף 4(א)1 ו-4(א)2 לצו. תאריך הנפקת מסמך הזיהוי יירשם באמצעות הטכנולוגיה לזיהוי חזותי בלבד, ללא אפשרות של עדכון השדה על-ידי מקבל השירות בדרך אחרת.
- ז. על האיכויות הטכניות של הטכנולוגיה לזיהוי חזותי, ובכלל איכות התקשורת (כגון רציפות התמונה), התמונה (כגון רזולוציה, ניגודיות, בהירות, תאורה) בזמן ביצוע תהליך הזיהוי, לאפשר זיהוי ואימות ברמת ודאות גבוהה של מקבל השירות ושל מסמך הזיהוי שהוצג על ידו.
- ח. במהלך תהליך ההזדהות יתבצע אימות למספר הטלפון של מקבל השירות באמצעות שליחת סיסמא חד פעמית זמנית (One Time Password – "OTP") לטלפון הנייד שבשימוש של מקבל השירות.

נותן השירות המשתמש בסיסמה חד פעמית זמנית הנשלחת באמצעות מסרונים כגורם אימות, ייתן מענה לאותם לקוחות שאין באפשרותם לקבל מסרון, או שאין באפשרותם לקוראו, באמצעות משלוח מסרון קולי.

ט. במקרה של שימוש בטכנולוגיה לזיהוי חזותי אשר אינה מחייבת אינטראקציה חזותית עם נציג נותן השירות בזמן אמת, על נותן השירות לשלב גם את הבקורות הבאות:

(1) "בדיקת חיות" - ביצוע בדיקות אשר מטרתן היא לוודא שמקבל השירות הוא אדם ממשי. הבדיקה יכולה להיות אקטיבית (מקבל השירות מתבקש לבצע פעולה מסוימת) או פסיבית (ללא שמבקש השירות נדרש לבצע פעולה כלשהי).

(2) א) ביצוע הליך בקרה שוטף על מדגם מקבלי השירות וזאת תוך פרק זמן סביר לאחר מועד קבלת השירות.

ב) במקרה של מקבל שירות שסווג בסיכון גבוה בהיבטי איסור הלבנת הון ומימון טרור, יבוצע הליך הבקרה בטרם יתאפשר ללקוח לקבל את השירות. לחלופין יבוצע הליך הבקרה תוך פרק זמן סביר לאחר מועד קבלת השירות, בכפוף לנוהל שיקבע על ידי האחראי לזיהוי מקוון. על הנוהל כאמור, להתייחס, בין היתר, להיקפי הפעילות של מקבל השירות, למהות הפעולות שהוא מבקש לבצע, ולהערכת הסיכונים שביצע נותן השירות.

לעניין זה:

"הליך בקרה" - בדיקה אפקטיבית שתתייחס לנאותות התהליך המיושם ובכלל זה תקינות הנתונים שנמסרו על ידי הלקוח במסגרת הליך הרישום לקבלת השירות;

"מדגם" - מדגם של שני אחוזים מהחשבונות החדשים של מקבלי שירות שזוהו בטכנולוגיה לזיהוי חזותי אשר אינה מחייבת אינטראקציה חזותית עם נציג בזמן אמת, או ארבע מאות חשבונות, כאמור, בשנה, לפי הגבוה. המדגם יכלול את כל מקבלי השירות כאמור שסווגו בסיכון גבוה בהיבטי איסור הלבנת הון ומימון טרור.

(3) סוגי הבקורות המפורטים בסעיף קטן (ה) ובסעיף קטן ט(1) לעיל, יבוצעו כמקשה אחת, ללא הפסקה ביניהם.

9. מקבל שירות מזדמן

נותן שירות רשאי לבצע את תהליך רישום פרטי הזיהוי של מקבל שירות מזדמן באחת מהדרכים הנזכרות בסעיפים 7 או 8 לעיל או באמצעות טכנולוגיה לאימות מקוון.

10. מקבל שירות שהוא גוף מוכר

נותן שירות רשאי לבצע את תהליך הזיהוי של מקבל שירות שהוא גוף מוכר, כנדרש בסעיף 4(א)6 לצו באמצעות הליך זיהוי מקוון, באחת הדרכים הנזכרות בסעיפים 7 או 8 לעיל, לאחר שנותן השירות נוכח לדעת, לפי מסמך, שמקבל השירות מוסמך לפעול בשם הגוף המוכר. נותן השירות יבדוק את אמיתות המסמך על פניו.

11. מקבל שירות שהוא תאגיד

- א. נותן השירות יזהה ויאמת את זהותם של מיופי הכוח שהם יחידים כאמור בסעיף 6 לעיל.
- ב. נותן השירות רשאי לבצע את תהליך הזיהוי של התאגיד כנדרש בסעיף 4(א)3 לצו לפי תעודת הרישום של התאגיד שנחתמה אלקטרונית על ידי רשות התאגידים או העתק מאושר שלה כהגדרתו בסעיף 4(ו) לצו, החתום בחתימה אלקטרונית העונה על תכליות הוראות הצו בעניין זה, ואשר הוצגה במעמד קבלת השירות, או העתקים מאושרים ממסמכי היסוד של התאגיד שנחתמו אלקטרונית על ידי הרשם הרלוונטי ברשות התאגידים, או נסח עדכני של פרטי התאגיד במרשם המתאים, שנחתם אלקטרונית על ידי הרשם הרלוונטי ברשות התאגידים, או אישור עורך דין על קיום התאגיד, שמו, מספר זהותו ותאריך ההתאגדות שלו החתום בחתימה אלקטרונית העונה על תכליות הוראות הצו בעניין זה.
- ג. בנוסף, במעמד מתן השירות, יקבל נותן השירות את המסמך הנדרש בסעיף 4(א)3 לצו ויתעד אותו. העתק מאושר כהגדרתו בסעיף 4(ו) לצו ואישור עורך דין כאמור בסעיף 4(א)3 לצו יכול שיתקבלו גם באופן מקוון שהם חתומים בחתימה אלקטרונית העונה על תכליות הוראות הצו בעניין זה.

12. קבלת הצהרה על נהנה ובעל שליטה – סעיף 5 לצו

- א. הצהרה על נהנה והצהרה על בעל שליטה בהתאם להוראות סעיף 5 לצו, יכולה להיעשות על ידי החתמת מקבל השירות על הצהרה באופן מקוון, בדרך המאפשרת תיעוד איכותי של החתימה וקישורה באופן מאובטח להצהרה.
- ב. במקרה של מקבל שירות שפועל בעבור עצמו ולא בעבור נהנה, נותן השירות יתעד את מקבל השירות מצהיר בקולו כי הוא פועל בעבור עצמו ולא בעבור נהנה.
- ג. במקרה של מקבל השירות שפועל בעבור נהנה, נותן השירות יתעד את מקבל השירות מצהיר בקולו כי הוא פועל בעבור נהנה, ויבצע זיהוי מקוון גם לנהנה עצמו באחת הדרכים הנזכרות בסעיפים 7 או 8.

- ד. במקרה של מקבל השירות שהוא תאגיד, יחתים נותן השירות את מיופה הכוח באופן מקוון על טופס הצהרה על בעל שליטה, ויתעד את מיופה הכוח מצהיר בקולו בדבר נכונות הטופס.
- ה. כחלופה להצהרה הקולית המפורטת בסעיפים 12(ב), 12(ג) ו-12(ד), נותן השירות יוכל לקבל חתימה מקוונת על הצהרה בה מקבל השירות יהיה מחויב לאשר כי קרא והבין את משמעות הצהרתו טרם חתימתו המקוונת עליה. נותן השירות יבצע אימות של מקבל השירות באמצעות סיסמה חד פעמית (OTP) בסמוך לפני החתימה על ההצהרה המקוונת.
- ו. כחלופה נוספת להצהרה הקולית המפורטת בסעיפים 12(ב), 12(ג) ו-12(ד) מקבל השירות יוכל לתת הצהרה בהתאם לסעיף 5 לצו, באמצעי חלופי שיאשר הממונה לנותן השירות, בהיוועצות עם הרשות המוסמכת.

13. זיהוי מקוון באמצעות צד שלישי

- נותן השירות רשאי לקבל שירותים מצד שלישי לצורך התקשרות עם מקבל שירות וביצוע זיהוי מקוון, על דרך של מיקור חוץ (להלן – "נותן שירות במיקור חוץ"), ובלבד שהתקיימו כל אלה:
- א. נותן השירות יודא כי לנותן השירות במיקור חוץ יש את הטכנולוגיה, המיומנות והידע המקצועי הנדרשים לאספקת השירותים וכי שירותים אלו מתבצעים בהתאם להוראות כל דין, ובכלל זה תקנה 15 לתקנות הגנת הפרטיות - אבטחת מידע והנחיית רשם מאגרי מידע מס' 2/2011 'שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע, וכן הוראות פרק זה;
- ב. קיומו של הסכם בכתב בין נותן השירות לבין נותן השירות במיקור חוץ, המסדיר את יחסי הצדדים בקשר למתן השירותים לזיהוי מקוון, ובכלל זה מגדיר את הפעילויות שיבוצעו על ידי נותן שירות במיקור חוץ וקובע את הזכויות, החובות והאחריות של הצדדים להסכם, באופן שמבטיח עמידה בהוראות הדין;
- ג. נותן השירות יטמיע אמצעי פיקוח ובקרה על השירותים שמסופקים על ידי נותן השירות במיקור חוץ;
- ד. נותן השירות יודא שמירה, גיבוי ואבטחת מידע של המסמכים וההקלטות כאמור בסעיף 15 להלן;
- ה. אין בסעיף זה כדי לגרוע מאחריות נותן השירות לפעילות של מקבל שירות המתבצעת באופן מקוון, על פי כל דין, ונותן השירות אינו רשאי להעביר לגורם שלישי את האחריות שחלה עליו על פי הוראות הדין.

14. הכר את הלקוח – סעיף 2 לצו

- א. נותן השירות רשאי לבצע את הליך "הכר את הלקוח" באמצעים טכנולוגיים שונים מאלו המשמשים אותו לצורך זיהוי מקוון, ובלבד שנקט באמצעים סבירים לוודא כי המשיב לשאלון "הכר את הלקוח" ומקבל השירות המזוהה והמאומת בהתאם להוראה זו, אחד הם, ובמקרה שמקבל השירות הוא תאגיד, כי המשיב לשאלון הוא מיופה הכוח בתאגיד.
- ב. מקבל שירות שהוא תושב זר אשר זוהה באמצעות טכנולוגיה לזיהוי מקוון, יסומן ויזוהה ככזה במערכות המחשב של נותן השירות לצורך ניטור סיכונים ויבוצע בו מעקב מוגבר למשך תקופה שתקבע על ידי נותן השירות, ובהתאם להערכת הסיכונים שביצע נותן השירות, המתחשבת, בין היתר, במדינה המקור של מקבל השירות, ובלבד שהמדינה או הטריטוריה של מקבל השירות אינן מן המנויות בתוספת הראשונה לצו.
- ג. רמת הסיכון של מקבל שירות שזוהה באופן מקוון תותאם להליך "הכרת הלקוח" שבוצע למקבל השירות.

15. שמירה, אבטחה וגיבוי

- א. נותן השירות יודא ויפעל למניעת זליגת מידע בביצוע הליך הזיהוי המקוון.
- ב. נותן השירות ישמור עותק דיגיטלי של תהליך הזיהוי של מקבל שירות (לרבות הליך "הכר את הלקוח" וקבלת הצהרה על נהנה ובעל שליטה), ובכלל זה, הקלטת תקשורת וידאו-אודיו או רצף האירועים שצולמו, צילום או סריקת מסמך הזיהוי ו/או מסמכים אחרים שהוצגו על ידי מקבל השירות באמצעות הטכנולוגיה לזיהוי מקוון. יובהר כי אין בהוראות אלה כדי לגרוע מחובות נותן השירות לפי הוראות הדין לעניין הגנת הפרטיות ובכלל זה תקנות הגנת הפרטיות – אבטחת מידע.
- ג. במקרה של זיהוי באמצעות טכנולוגיה לזיהוי חזותי, ובהמשך לביצוע האימות למספר הטלפון של מקבל השירות כאמור בסעיף 8(ח), נותן השירות ישמור את מספר הטלפון, מספר הברזל (IMEI) של מכשיר הנייד של מקבל השירות, אם קיים, כמו גם כתובת IP ממנה ניתן השירות, אם קיימת. מידע זה יישמר בידי נותן השירות באופן מאובטח על מנת לאפשר להתחקות בדיעבד אחר זהות מקבל השירות.
- ד. נותן השירות ישמור תיעוד של הבקרה שנערכה כמפורט בסעיף 8(ט) לעיל.
- ה. מידע כאמור בסעיפים קטנים (ב) ו- (ג) ייחשב כ"מסמך זיהוי" לעניין סעיף 4(א) ו-4(א)(2) לצו, ויישמר לתקופה הנקובה בסעיף זה. כמו כן, המידע יאוחסן בשרת מאובטח שבשליטת נותן השירות ויגובה מידי תקופה באופן שיאפשר בעת הצורך שחזור עדכני, מהיר ואמין וכן שמירה על הנתונים, כפי שהם, ללא אפשרות עריכה. אופן שמירת המידע יאפשר שחזור אמין ומהיר שלו.

- ו. נותן השירות יידע את מקבל השירות על המידע שישמר, לרבות כי נאסף ונשמר אודותיו מידע ביומטרי, לאיזה צורך ישמר, הגורמים אשר עשויים להיות בעלי נגישות למידע ומשך הזמן שהמידע ישמר, וכן לגבי סיכונים הקשורים באבטחת המידע והגנת הפרטיות ויקבל את הסכמת מקבל השירות לכך, והכל בהתאם לחוק הגנת הפרטיות.
- ז. במקרה של זיהוי באמצעות טכנולוגיה לזיהוי חזותי, נותן השירות יבצע תהליך לעריכת רשומה מוסדית, שתיסמך על חוות דעת של גורם משפטי אצל נותן השירות, ואשר תתייחס לתנאים להוכחת רשומה מוסדית, לרבות פלט של רשומה מוסדית, כמפורט בסעיף 36(א) לפקודת הראיות, התעודה תחתם בידי גורם מטעמו של נותן השירות, אשר ישמש, בהתאם לצורך, כ"עד מגיש" של התעודה בדבר הרשומה המוסדית.
- ח. במסגרת עריכת "רשומה מוסדית" כאמור לעיל, נותן השירות יכלול את הסרטון או את רצף האירועים שצולמו במהלך ההזדהות החזותית באמצעות הטכנולוגיה.

16. אמצעי ניטור, בקרה וניהול סיכונים

- א. נותן השירות שמזהה, אגב מתן השירות באמצעות טכנולוגיה לזיהוי מקוון, כי מדובר במקבל שירות בסיכון גבוה להלבנת הון ומימון טרור, ישקול לזהות את מקבל השירות פנים אל פנים או שלא לתת שירות כלל או לחסום את הפעילות הקיימת או לחזק את הליכי הזיהוי באמצעים נוספים, לפי מידת הסיכון והעניין.
- ב. עלה חשש אצל נותן השירות להתנהגות בלתי רגילה של מקבל השירות, אשר זוהה באמצעות טכנולוגיה לזיהוי מקוון, ישקול נותן השירות לזהות את מקבל השירות פנים אל פנים ו/או להגיש דיווח על פעולה בלתי רגילה או שלא לתת שירות כלל, והכל בהתאם לנסיבות ומידת הסיכון.
- ג. על נותן השירות להטמיע מערך ניטור ובקרה לצורך מילוי חובותיו על פי הצו באמצעות שימוש בטכנולוגיה לזיהוי מקוון. זיהוי פעולות חריגות יבוסס, בין היתר, על אנומליות טכנולוגיות ותפעוליות וכן אנומליות עסקיות לפי הצורך, וישמש גם לכלי נוסף לניטור דיווחים לפי סעיף 15 לצו.
- ד. נותן השירות יעקוב אחר התפתחות שיטות הונאה בישראל ובעולם ויעדכן במידת הצורך את מערך הניטור והבקרה.

17. קבלת אישור יו"ר הרשות

א. נותן השירות המבקש ליישם טכנולוגיה לזיהוי חזותי לצורך מתן שירות למקבלי השירות, נדרש לקבל לכך את אישור יו"ר רשות ניירות ערך.

ב. נותן השירות המגיש בקשה לקבלת אישור כאמור, יציג בפני יו"ר רשות ניירות ערך כי התקיימו לגביו כלל התנאים והעקרונות האמורים בהוראה זו. בקשה כאמור תכלול לכל הפחות את הפרטים הבאים:

(1) שמו ופרטי הקשר של ספק הטכנולוגיה לזיהוי חזותי.

(2) תיאור מפורט של מאפייני הטכנולוגיה לזיהוי חזותי.

(3) חוות דעת מומחה שהינו חיצוני לספק הטכנולוגיה ובלתי תלוי. על חוות הדעת להיות ערוכה כדין, בהתאם לתוספת הראשונה לפקודת הראיות, שתפרט, בין היתר, את יכולות המערכת שפיתח, אופן ביצוע הזיהוי ואימות הזהות והפוטנציאל לזיהוי שגוי.

(4) הצהרה מאומתת של המנהל הכללי של נותן השירות כי מילא אחר כלל דרישות הדין בכל הקשור בשימוש בטכנולוגיה ובכלל זה הוראות הגנת הפרטיות הקבועות בדין. התחייבות נותן השירות להגביר את מודעות מקבל השירות ולמסור לו פרטים כנדרש בסעיפים 4(ג)(5) ו-15(ו) להוראה זו.

(5) פירוט הבקורות שהוטמעו אצל נותן השירות בקשר לשימוש בטכנולוגיה לזיהוי חזותי.

(6) הסכם בכתב בין נותן השירות לבין ספק הטכנולוגיה, ככל שקיים, המסדיר את יחסי הצדדים בקשר לטכנולוגיה והשימוש בה לצורך זיהוי חזותי, וקובע את הזכויות, החובות והאחריות של הצדדים להסכם, באופן שמבטיח עמידה בהוראות הדין ובכלל זה הוראות תקנה 15 לתקנות הגנת הפרטיות – אבטחת מידע.

ג. כל שינוי מהותי בטכנולוגיה או בשירות הניתן על ידי נותן השירות באמצעות הטכנולוגיה מחייב קבלת אישור יו"ר רשות ניירות ערך בטרם יישומו.



18. חובות נותן השירות

יובהר כי עניינה של הוראה זו באופן קיום חובות שבצו איסור הלבנת הון, במתן השירות באמצעות טכנולוגיה לזיהוי מקוון. אין באמור בהוראה כדי להפחית מחובות אחרות של נותן השירות החלות עליו במתן השירות באמצעות טכנולוגיה לזיהוי מקוון, על פי כל דין, ובכלל זה חובת נותן השירות לניהול מכלול הסיכונים הגלומים בשימוש בטכנולוגיה לזיהוי מקוון, לרבות סיכוני התחזות שיובילו למעילות והונאות או לאירועי סייבר, סיכוני אבטחת מידע וסייבר, סיכוני פגיעה בפרטיות, סיכונים משפטיים וסיכוני ציות.





עו"ד ספי זינגר

יושב ראש רשות ניירות ערך

