רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

הוראה למבקשי ובעלי רישיון או אישור למתן שירות מידע פיננסי ולמבקשי ובעלי רישיון או אישור למתן שירות ייזום בסיסי

הוראה לפי סעיפים 4, 5, 27(ג)(1), 35, 36 ו- 63(ב) לחוק שירות מידע פיננסי, התשפ"ב-2021 ולפי סעיפים 15(ב), 23(ב), 27(א)(1) ו-(2), ו-43(ב) לחוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, התשפ"ג-2023

דברי הסבר

חוק שירות מידע פיננסי, התשפ"ב - 2021 (להלן: "**חוק שירות מידע פיננסי**") אשר נחקק בחודש נובמבר 2021 ונכנס לתוקף ביוני 2022, הסמיך את רשות ניירות ערך (להלן: "**הרשות**") להעניק רישיונות למתן שירות מידע פיננסי לתאגידים העומדים בדרישות הקבועות בחוק זה, ולפקח על בעלי רישיונות כאמור בהתאם לעקרונות שנקבעו בחוק שירות מידע פיננסי. חוק זה מסדיר לראשונה בחקיקה את תחום הבנקאות הפתוחה בישראל.

חוק שירות מידע פיננסי עוסק במתן שירות מידע פיננסי שהוא שירות מקוון במסגרתו בעל רישיון או אישור למתן שירות מידע פיננסי (להלן: "**בעל רישיון או אישור למתן שירות מידע פיננסי**") אוסף מידע פיננסי על אודות הלקוח שנמצא בידי גופים פיננסיים מהם מקבל הלקוח שירות פיננסי (להלן: "**מקורות מידע**"), ונותן על בסיסו שירות ללקוח. איסוף כאמור של המידע הפיננסי נעשה מכוח גישה של בעל רישיון למערכת מקוונת שדרכה מחויב מקור מידע לתת גישה למידע הפיננסי (להלן: "**מערכת הממשק למידע פיננסי**").

מידע פיננסי, הוא מידע על אודות הפעילות הפיננסית של הלקוח שמתנהלת אצל מקורות המידע כדוגמת: תנועות (זיכויים וחיובים) בחשבון העובר ושב של הלקוח ועלות ניהול החשבון של הלקוח (דמי ניהול חשבון); מידע על אודות האשראי של הלקוח, ובכלל זה סך האשראי שהלקוח נטל והריביות שהוא משלם בגינו; מידע על החסכונות של הלקוח, ובכלל זה היקף החיסכון של הלקוח וריביות שהוא מקבל בעדו; מידע על תיק ניירות הערך שמחזיק הלקוח והעמלות שהוא משלם עבור פעולות קנייה ומכירה של ניירות ערך וכיוצא בזה.

במסגרת שירות מידע פיננסי יכול בעל רישיון להציע ללקוחות שירותים שונים. לדוגמה, ריכוז מידע פיננסי ממקורות מידע פיננסי שונים; השוואת עלויות; העברת מידע לגופים פיננסיים לשם קבלת הצעות להתקשרות עבור הלקוח לשירותים פיננסיים שאותם הלקוח צורך או מבקש לצרוך (כלומר, הצעות מחיר מתחרות) או לשם סיוע בהתקשרות עמם; וכן ייעוץ בדבר התנהלותו הכלכלית של הלקוח. נדגיש כי לא מדובר ברשימה סגורה של שימושים שיכול בעל רישיון לעשות במידע הפיננסי, ובלבד שהשימוש נוגע להתנהלותו הכלכלית של הלקוח, לטובת הלקוח ובהסכמתו המפורשת.

חוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, התשפ"ג-2023 (להלן: "**חוק הסדרת העיסוק בשירותי תשלום**"), אשר נחקק ביוני 2023 ויכנס לתוקף ביוני 2024, מתווסף לחוק שירות מידע פיננסי, ומסמיך את רשות ניירות ערך (להלן: "**הרשות**") להעניק רישיון או אישור למתן שירות ייזום בסיסי, לתאגיד העומד בדרישות הקבועות בחוק הסדרת העיסוק בשירותי תשלום, ולפקח על בעל רישיון או אישור כאמור.

שני החוקים האמורים, הן חוק שירות מידע פיננסי והן חוק הסדרת העיסוק בשירותי תשלום, מבוססים על עקרונות האסדרה האירופאית כפי שהיא באה לידי ביטוי בדירקטיבת ה-PSD2[1], המסדירה את שירותי המידע הפיננסי והייזום הבסיסי, לצד הסדרת שירותי תשלום נוספים שהוראה זו אינה עוסקת בהם.

שירות ייזום בסיסי הוא שירות נוסף במסגרת תחום הבנקאות הפתוחה, שבמסגרתו בעל רישיון או אישור למתן שירות ייזום בסיסי, כותב את פרטי הוראת התשלום בחשבון הלקוח, לבקשת הלקוח, כאשר לאחר מכן וטרם ביצוע ההוראה, הלקוח נדרש לאשר באופן מקוון את הוראת התשלום מול מנהל חשבון התשלום שלו (לדוגמא: כתיבה של הוראת תשלום בחשבון הבנק של הלקוח על ידי בעל הרישיון שמאושרת לאחר מכן על ידי הלקוח מול הבנק באופן מקוון).

ייזום בסיסי בא להקל על הלקוח בכך שהוראת התשלום נכתבת עבורו, וכיוון שהשירות מקוון יש בו כדי למנוע טעויות בכתיבת ההוראה העלולות לנבוע מהקלדה שגויה של הלקוח. שירות ייזום בסיסי יאפשר ביצוע קל ונוח של העברות בנקאיות, באופן שיאפשר לייצר חלופה תחרותית לשימוש בכרטיסי אשראי לצורך ביצוע תשלומים לבתי עסק.

ייזום בסיסי יכול להיעשות גם כן באמצעות אותה מערכת ממשק, שדרכה נאסף מידע פיננסי ומשכך, שירותי המידע הפיננסי משיקים לשירות ייזום בסיסי במידה רבה והם עשויים להתבצע על ידי אותן חברות. יצוין כי גם באיחוד האירופאי ובבריטניה שירותים אלו מוסדרים כיום יחדיו, ואף חלקם מתבססים[2] על תקן טכנולוגי זהה.

בהמשך לחקיקת חוק הסדרת העיסוק בשירותי תשלום, נוספו להוראה הוראות בדבר אופן מתן אישור לשירות ייזום בסיסי עבור בעל רישיון שירות מידע פיננסי, וכן הוחלו על בעל רישיון או אישור למתן שירות ייזום בסיסי את דרישות האמצעים הטכנולוגיים ואבטחת המידע הקבועים בהוראה לעניין בעלי רישיון שירות מידע פיננסי, וזאת לנוכח ההשקה בין השירותים כאמור לעיל, והעובדה כי הם מתבצעים באמצעות אותה מערכת ממשק ועל בסיס תקן טכנולוגי זהה.

[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] שירות ייזום תשלומים (***Payment initiation***) ושירות מידע פיננסי (***Account information service***) מתבססים על הוראות ה-European Banking Authority שסמכותה נגזרת מהאסדרה האירופאית (דירקטיבת ה-PSD2), וכנגזרת מכך על תקני ברלין או תקנים מקבילים.

פרק א': כללי

1. בהוראה זו:

"**אתר הדיווח**" – אתר האינטרנט של הרשות, שבו מתבצע הדיווח האלקטרוני לרשות, כמוגדר בתקנות ניירות ערך (חתימה ודיווח אלקטרוני), התשס"ג-2003;

"**בעל רישיון**" – בעל רישיון שירות מידע פיננסי או יוזם בסיסי;

"**בעל רישיון שירות מידע פיננסי**" - בעל רישיון למתן שירות מידע פיננסי לפי חוק שירות מידע פיננסי;

"**יוזם בסיסי**" - בעל רישיון ייזום בסיסי או אישור מאת הרשות למתן שירות ייזום בסיסי לפי חוק הסדרת העיסוק בשירותי תשלום;

"**בנקאות פתוחה**" – כהגדרתה בנוהל בנקאי תקין מס' 368;

"**הוראת תשלום**", "**חשבון תשלום**", "**משלם**", "**שירות ייזום בסיסי**" **ו-**"**שירותי תשלום**" **-** כהגדרתם בחוק הסדרת העיסוק בשירותי תשלום;

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

"**חוק הסדרת העיסוק בשירותי תשלום**" – חוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, התשפ"ג-2023;

"**יום עסקים**" – יום שבו רוב התאגידים הבנקאיים בישראל פתוחים לביצוע עסקאות עם הציבור;

"**כללי הגשת בקשת רישיון למתן שירות מידע פיננסי**" - כללי הגשת בקשת רישיון למתן שירות מידע פיננסי, התשפ"ב-2022 אשר פורסמו ברשומות ביום 26.5.2022;

"**כללי הגשת בקשת רישיון למתן שירות ייזום בסיסי**" – כללי הגשת בקשת רישיון שירותי תשלום או שירות ייזום בסיסי, התשפ"ד-2024 אשר פורסמו ברשומות ביום 26.5.2024;

"**מבקש**" – תאגיד המבקש לקבל רישיון למתן שירות מידע פיננסי;

"**מדד**" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה;

"**מידע רגיש**" –מידע פיננסי וכל מידע שחלה עליו חובת הסודיות לפי חוק שירות מידע פיננסי;

"**מנהל חשבון תשלום**" – כהגדרתו בנוהל בנקאי תקין מס' 368;

"**מערכת הממשק**" –מערכת ממשק למידע פיננסי כהגדרתה בחוק שירות מידע פיננסי וכן מערכת ממשק למתן הוראות תשלום כהגדרתה בחוק הסדרת העיסוק בשירותי תשלום;

"**מקור מידע**" – כהגדרתו בחוק שירות מידע פיננסי, וכן לעניין שירות ייזום בסיסי – מנהל חשבון תשלום;

"**נוהל בנקאי תקין מס' 368**" – נוהל בנקאי תקין מס' 368 של בנק ישראל העוסק ביישום תקן של בנקאות פתוחה בישראל;

"**סוג השירות**" – אחד או יותר משלושה אלו: (1) איסוף מידע פיננסי והעברתו לאחר; (2) איסוף מידע פיננסי, ושימוש בו באופן מקוון, בידי מי שאסף את המידע; (3) שימוש, באופן מקוון, במידע פיננסי שנאסף בידי אחר והועבר לעושה השימוש, כאמור בפסקה (1);

"**סטנדרט**" - תקן לבנקאות פתוחה בישראל, המפורט בנספח א' לנוהל בנקאי תקין מס' 368, לרבות גרסאות מעודכנות, וכולל בין היתר: ארכיטקטורה, אבטחת מידע והגנת הסייבר, הגדרת תהליכים עסקיים, תהליכי הזדהות של בעל רישיון אצל מקור המידע, תהליכי קבלת הסכמת לקוח וביטול ההסכמה, כללים לרמת שירות, הגדרת השירותים ומבנה הפניה והתשובה לכל שירות, אופן ניהול הגרסאות והשירותים שיינתנו על ידי מקור המידע בסביבות הפיתוח;

"**סרטיפיקט**" - תעודה דיגיטלית שהונפקה לבעל רישיון על ידי ממשל זמין - בנקאות פתוחה באישור הרשות, לצורך פעילות בעל רישיון בבנקאות פתוחה מול מקורות המידע;

"**ערוץ מקוון**" – כתובת אתר אינטרנט או יישומון (אפליקציה);

"**פורטל מפתחים**" – כהגדרתו בנוהל בנקאי תקין מס' 368;

"**רשם מאגרי המידע**" - כהגדרתו בסעיף 7 לחוק הגנת הפרטיות;

"**שכבת התעבורה**" - ערוץ מאובטח מעל רשת האינטרנט המאפשר העברת מסרים בין מקור מידע לבין בעל רישיון.

"**תעודה דיגיטלית**" – אישור אלקטרוני שמקשר את הזהות של בעל התעודה לצמד מפתחות הצפנה (אחד פרטי ואחד ציבורי) שבאמצעותם ניתן להצפין ולחתום דיגיטאלית מידע;

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

פרק ב': הגשת בקשה לקבלת רישיון למתן שירותי מידע פיננסי

2. גוף המבקש לקבל רישיון למתן שירות מידע פיננסי יגיש בקשה בהתאם לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

3. מבקש אשר הגיש בקשה לקבלת רישיון או אישור למתן שירות מידע פיננסי ובקשתו טרם נענתה, יוכל להגיש בקשה לקבלת סרטיפיקט לסביבת הטסט.

4. הרשות תנפיק למבקש סרטיפיקט לסביבת הטסט לאחר שבחנה את עמידתו בדרישות המהימנות; תשלום אגרת בקשת רישיון; ובחינה ראשונית של האמצעים הטכנולוגיים של המבקש כאמור בסעיף 2(6) לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

5. בחינת הרשות את בקשת המבקש כאמור תעשה בשים לב למכלול בקשתו לקבלת רישיון ובהתאם לסיכונים הנשקפים מפעילותו בסביבת הטסט של מקורות המידע. לעניין חוות דעת המבקר המצורפת לבקשת הרישיון, הרשות תבחן, בין היתר, את התייחסות חוות הדעת לרמת אבטחת המידע של המבקש בסביבת הטסט.

6. קבלת סרטיפיקט לסביבת הטסט לא מעידה על עמידה במלוא דרישות קבלת הרישיון. מבקש שבקשתו לקבלת רישיון סורבה יבוטל הסרטיפיקט שלו לסביבת הטסט.

7. מבקש שבקשתו לקבלת רישיון אושרה על ידי הרשות, יוכל להגיש בקשה להנפקת סרטיפיקט אשר תנפיק לו הרשות, כאמור בפרק ה'.

פרק ב'1: הגשת בקשת אישור למתן שירות ייזום בסיסי

7א. בעל רישיון שירות מידע פיננסי המבקש אישור למתן שירות ייזום בסיסי, יגיש בקשה לאישור שתכלול את הפרטים האמורים בסעיפים הבאים בכללי הגשת בקשת רישיון למתן שירות ייזום בסיסי, בהתאמות הנדרשות לעניין שירות ייזום בסיסי:

א. סעיף 2(4) שעניינו בפירוט המבנה הארגוני ושירותי מיקור חוץ;

ב. סעיף 2(5) שעניינו בפירוט אודות אמצעים טכנולוגיים;

ג. סעיף 2(6) שעניינו בפירוט תכנית עסקית;

ד. סעיף 2(8) שעניינו בפירוט בדבר עמידה בדרישות הון עצמי;

ה. סעיף 2(9) שעניינו בפירוט בדבר עמידה בדרישות ביטוח או פיקדון;

ו. סעיף 2(11) שעניינו בפירוט הסדרי ממשל תאגידי ומנגנוני הבקרה הפנימית.

7ב. הוראות סעיפים 3 עד 6 בעניין סרטיפיקט לסביבת הטסט יחולו בשינויים המחויבים גם על מבקש רישיון או אישור למתן שירות ייזום בסיסי, ולעניין בחינת האמצעים הטכנולוגיים לפי סעיף 4 - זו תיעשה כאמור בסעיף 2(5) לכללי הגשת בקשת רישיון למתן שירות ייזום בסיסי.

7ג. יוזם בסיסי שבקשתו למתן שירות ייזום בסיסי אושרה על ידי הרשות, יוכל להגיש בקשה להנפקת סרטיפיקט אשר תנפיק לו הרשות, כאמור בפרק ה', ובלבד שיפעל בהתאם לסטנדרט ויעמוד בחובות הקבועות בחוק הסדרת העיסוק בשירותי תשלום וההוראות מכוחו.

פרק ב'2: תחולת הוראות על מתן שירות ייזום בסיסי

7ד. לעניין מתן שירות ייזום בסיסי, סעיפים 11-14 ופרקים ג', ד', ד'1 ו-ח' להוראה זו לא יחולו.

פרק ג': דרישות ביטוח או פיקדון

8. על בעל רישיון שירות מידע פיננסי לעמוד בדרישה לביטוח או לבטוחה מסוג פיקדון, כפי שיפורט להלן:

א. בעל רישיון שירות מידע פיננסי ביטח את אחריותו כלפי הלקוחות בהתאם לאמור בפרק ח' להוראה לחברות תשלומים, בעלי רישיון ייזום בסיסי ובעלי רישיון שירות מידע פיננסי בנושא הון עצמי, ביטוח או בטוחה אחרת.

ב. בעל רישיון שירות מידע פיננסי הפקיד פיקדון בסכום מספק לדעת דירקטוריון בעל הרישיון לכיסוי חבותו של בעל הרישיון בשל מעשה או מחדל רשלני כלפי לקוח בהתאם לאמור פרק ח' להוראה לחברות תשלומים, בעלי רישיון ייזום בסיסי ובעלי רישיון שירות מידע פיננסי בנושא הון עצמי, ביטוח או בטוחה אחרת.

פרק ד': שמירת מידע פיננסי הנדרש לשם הליך משפטי, הליך ביקורת פנימית או פיקוח לפי דין

9. שמירת מידע פיננסי הנדרש לשם הליך משפטי, הליך ביקורת פנימית או פיקוח לפי דין תתאפשר לבעל רישיון שירות מידע פיננסי למשך תקופה של שבע שנים מיום סיום מתן השירות ללקוח. מידע כאמור:

א. ישמר במאגר מידע נפרד מכל מאגר מידע אחר;

ב. המידע ישמש רק לשם הליך משפטי, הליך ביקורת פנימית או פיקוח לפי דין, הנוגעים לשירות שנתן בעל רישיון שירות מידע פיננסי ללקוחותיו;

ג. בעל רישיון שירות מידע פיננסי יבטיח כי לא תתאפשר כל גישה למידע האמור, אלא אם כן נפתח הליך כאמור בסעיף 27(ג) לחוק שירות מידע פיננסי הנוגע ללקוח מסוים, והמידע דרוש לבעל רישיון שירות מידע פיננסי לשם ניהול ההליך; בין השאר, בעל

רישיון שירות מידע פיננסי יבטיח כי אמצעי הגישה למידע האמור יאובטחו על פי האמור בהוראות אלו, יוחזקו רק בידי גורמים מעטים בבעל הרישיון וכי הגישה למידע האמור תיעשה באישור הגורמים המורשים בבעל הרישיון ותדרוש הליך של אחזור הנתונים.

ד. בעל רישיון שירות מידע פיננסי ימחק את המידע בתום שבע שנים מיום סיום מתן השירות, למעט מידע הדרוש לשם ניהול הליך שנפתח כאמור בפסקה (ג) לפני תום התקופה האמורה. לצורך כך יקיים בעל רישיון שירות מידע פיננסי הליכי בקרה על מחיקת המידע האמור.

ה. כל הוראה ביחס לדרישות אבטחת המידע והגנת הפרטיות בהוראות אלו תחול גם לגבי מידע זה.

פרק ד'1: וידוא הסכמת הלקוח בגישה מתמשכת למידע פיננסי

9א. בעל רישיון שירות מידע פיננסי אשר קיבל גישה מתמשכת למידע פיננסי אודות לקוח לתקופה קצובה העולה על שישה חודשים, יוודא אחת לשישה חודשים, במהלך אותה תקופה, בהתאם להוראות סעיף 26(ב) לחוק שירות מידע פיננסי, כי הלקוח מודע לכך כי אפשרות הגישה למידע פיננסי עומדת בעינה, בהתאם להסכמתו. הווידוא יכלול פעולה אקטיבית מצד הלקוח המעידה על כך שהוא מודע לגישה למידע הפיננסי אודותיו על ידי בעל הרישיון כאמור. ווידוא כאמור ייעשה באחת מהדרכים הבאות:

א. ווידוא שימוש של הלקוח בשירותי המידע הפיננסי של בעל רישיון שירות מידע פיננסי, כגון: כניסת הלקוח לאפליקציה או לאתר האינטרנט; בשירות הניתן באמצעות שליחת הודעות דואר אלקטרוני ללקוח, קבלת חיווי תקופתי לכך שהלקוח פתח את הודעות הדואר האלקטרוני; פניה של הלקוח לבעל הרישיון כאמור בנוגע לשירות הניתן על ידי בעל הרישיון הכולל גישה למידע פיננסי של הלקוח.

ב. פנייה יזומה מצד בעל רישיון שירות מידע פיננסי ללקוח בו יתבקש הלקוח לאשר באופן אקטיבי כי הוא מודע לגישה שנתן לבעל הרישיון למידע פיננסי אודותיו למשך תקופה קצובה. בפנייה יצוין משך התקופה הקצובה, סלי המידע ומקורות המידע להם נתן הלקוח גישה לבעל הרישיון.

9ב. לא הצליח בעל רישיון שירות מידע פיננסי לוודא כי הלקוח מודע לאפשרות הגישה של בעל הרישיון כאמור למידע פיננסי אודותיו, יראו את הלקוח כאילו ביטל את הסכם ההתקשרות עם בעל הרישיון, כאמור בסעיף 28 לחוק שירות מידע פיננסי.

9ג. בעל רישיון שירות מידע פיננסי יתעד וישמור את הפעולות שנקט לצורך ווידוא כי הלקוח מודע לכך כי אפשרות הגישה של בעל הרישיון למידע פיננסי עומדת בעינה, וכן תיעוד לשימוש הלקוח או לאישור הלקוח בדבר מודעותו להמשך הגישה של בעל הרישיון למידע אודותיו, כאמור בסעיף 9א.

9ד. בשירות אשר עיקרו הוא העברת מידע פיננסי למייצג והלקוח אישר בפני בעל רישיון שירות מידע פיננסי כי ייפה את כוחו של המייצג לעניין מתן שירותים כרואה חשבון או יועץ מס, יכול בעל הרישיון כאמור לראות בפעולות שנעשו בהתאם לסעיף 9א על ידי המייצג כפעולות שנעשו על ידי הלקוח, ובלבד שבעת מתן האישור כאמור בסעיף 9 להוראה לבעלי רישיון למתן שירות מידע פיננסי בעניין העברת מידע לאחר, יאשר הלקוח כי הוא מייפה את כוחו של המייצג גם לעניין ווידוא הסכמתו להמשך העברת המידע הפיננסי לפי סעיף 26(ב) לחוק שירות מידע פיננסי.

פרק ה': אבטחת מידע והגנת פרטיות

<u>סימן א' - כללי</u>

10. אבטחת מידע והגנת פרטיות – כללי:

א. סטנדרט אבטחת המידע הקבוע בהוראות אלו יחול על כל מידע רגיש אצל בעל הרישיון.

ב. תקשורת של בעל רישיון המכילה מידע רגיש מול כל גורם, תיעשה בפרוטוקול סטנדרטי ובתעבורה מוצפנת על פי הטכנולוגיות העדכניות הקיימות בשוק.

ג. בעל רישיון מחויב לפעול בהתאם לסטנדרט בכל פניה או קבלת הודעות ממקור מידע הנעשית דרך מערכת הממשק של מקור המידע, ובכלל זה פניות או קבלת הודעות הנעשות בהתאם לסעיפים 28(ג)(2), 41(א)(2), 41(א)(3) ו- 45(ג) לחוק שירות מידע פיננסי יעשו בהתאם לסטנדרט, וכן בעת מתן שירות ייזום בסיסי.

ד. בעל רישיון לא ישתמש בפרטי הגישה של הלקוח אל חשבונו שנועדו לאמת את זהותו בפני מקור המידע, לשם מתן שירות ייזום בסיסי.

<u>סימן ב' - רישום ראשוני של הלקוח – הקמת חשבון משתמש בבעל רישיון שירות מידע פיננסי</u>

11. בעל רישיון שירות מידע פיננסי ירשום ויאמת את הפרטים שמוסר לו הלקוח באמצעות וידוא התאמת מספר הזיהוי שמסר לו לזה הרשום אצל מקור המידע, על מנת לאמת את הסכמת הלקוח לקבל שירות מידע פיננסי.

בעל רישיון שירות מידע פיננסי לא יבקש מלקוח את מספר כרטיס החיוב שלו, לצורך מתן הרשאת גישה למידע פיננסי. אין באמור כדי למנוע מבעל רישיון שירות מידע פיננסי לבקש מלקוח את מספר כרטיס החיוב שלו כדי לשלם עבור השירות הניתן על ידי בעל הרישיון.

12. לאחר רישום פרטי הלקוח מול בעל רישיון שירות מידע פיננסי, יפנה בעל הרישיון כאמור את הלקוח לערוץ המקוון של מקור המידע לשם מתן הסכמת הלקוח למתן הרשאת הגישה למידע פיננסי אודות הלקוח לבעל הרישיון.

13. לקוח המבקש לקבל שירות של בעל רישיון שירות מידע פיננסי, ינחה אותו בעל הרישיון כאמור להשלים בפעם הראשונה תהליך רישום ראשוני (enrollment) ביישומון (אפליקציה) או באתר האינטרנט של בעל הרישיון, בצירוף קבלת אמצעי אימות נוסף.

<u>סימן ג' - התחברות שוטפת של הלקוח לבעל רישיון שירות מידע פיננסי</u>

14. לאחר הרישום הראשוני והקמת חשבון משתמש בבעל רישיון שירות מידע פיננסי, ההתחברות השוטפת של הלקוח מול בעל הרישיון כאמור תעשה באמצעים הבאים:

א. באמצעות יישומון (אפליקציה) של בעל הרישיון שהותקן על מכשיר הטלפון הנייד של הלקוח: כניסה ליישומון (אפליקציה) תתבצע באמצעות אמצעי האימות שנמצא בשימוש בטלפון הנייד, כגון: קוד, סיסמה, טביעת אצבע, זיהוי פנים וכדומה.

ב. כניסת הלקוח לאתר אינטרנט של בעל הרישיון יחייב הכנסת אמצעי אימות נוסף מלבד סיסמה (Multi-Factor Authentication), כגון: זיהוי באמצעות קוד הנשלח ב- SMS או הקראת הקוד בשיחת טלפון.

<u>סימן ד' - שימוש בסרטיפיקט</u>

15. תהליך יצירת סרטיפיקט יתבצע אך ורק על ידי גורמים מורשים אצל בעל רישיון על פי תהליך הנפקת סרטיפיקט שפרסמה הרשות.

16. על בעל רישיון לדאוג שהסרטיפיקט בבעלותו עדכני ומכיל את הפרטים המתאימים, לפי הרישיון שניתן לו.

17. בעל רישיון ישתמש בסרטיפיקט רק בהתאם לרישיון שקיבל ולשימושים המותרים לפיו. בעל רישיון יעשה שימוש נאות במערכת הממשק מבחינת תקינות הבקשות וכמות הבקשות באופן שיהיה תואם לאופי השירות שביקש הלקוח; לעניין זה, בקשות – לרבות בקשות המוגשות במסגרת שירות ייזום בסיסי.

18. בעל רישיון מחויב להזדהות באופן מקוון באמצעות סרטיפיקט ייעודי בכל פניה למערכת הממשק של מקור המידע. בעל רישיון לא יעשה שימוש בסרטיפיקט אם אינו תקף או שהוא בסטטוס מושהה או מבוטל.

19. בעל רישיון יעביר את המסרים למקור המידע רק על פי הסטנדרט. על אף האמור ברישא סעיף זה ובסעיף 10(ג), דיווח למקור מידע כאמור בסעיף 31 לחוק שירות מידע פיננסי על אירוע אבטחה חמור יעשה בפורטל המפתחים.

19א. בעל רישיון ישמור את הבעלות על הדומיין (כתובת האתר), המוגדר בסרטיפיקט, לצורך קבלת הודעות ממקור המידע, כל עוד קיימות הסכמות בתוקף, שהוקמו עם הסרטיפיקט בו מוגדר אותו דומיין.

20. בעל רישיון יגיש בקשה לרשות להשהיית או ביטול הסרטיפיקט שלו, וזאת בשל חשש לאירוע אבטחת מידע העלול לגרום לשימוש לא נאות בסרטיפיקט. לאחר הגשת הבקשה, הסרטיפיקט

יושהה או יבוטל באופן אוטומטי. על בעל הרישיון לוודא שקיבל הודעה מהרשות על השהיית או ביטול הסרטיפיקט או יוודא את השהיית או ביטול הסרטיפיקט מול ממשל זמין.

הוסר החשש כאמור, יודיע על כך בעל הרישיון לרשות ויבקש כי השהיית הסרטיפיקט תבוטל - ביטול ההשהיה יבוצע אוטומטית; או כי יונפק לו סרטיפיקט חדש בהתאם להליכי הנפקת סרטיפיקט.

<u>סימן ה' - ביטול הסרטיפיקט בעקבות ביטול או התליית רישיון</u>

21. הותלה או בוטל רישיון למתן שירות מידע פיננסי לפי סעיף 7 לחוק שירות מידע פיננסי או הותלה או בוטל רישיון או אישור למתן שירות ייזום בסיסי לפי סעיף 7 או 17 לחוק הסדרת העיסוק בשירותי תשלום, לפי העניין, יבוטל הסרטיפיקט של אותו בעל רישיון.

22. התלה יושב ראש הרשות רישיון למתן שירות מידע פיננסי באופן מיידי, לפי סמכותו בסעיף 7(ד) לחוק שירות מידע פיננסי או שהתלה רישיון או אישור למתן שירות ייזום בסיסי לפי סעיף 7(ד) או 17(ג) לחוק הסדרת העיסוק בשירותי תשלום, לפי העניין, יבוטל הסרטיפיקט של בעל הרישיון באופן מיידי.

23. תמה תקופת התליית הרישיון של בעל הרישיון, תנפיק הרשות סרטיפיקט חדש לבעל הרישיון.

24. בעל רישיון שמעוניין להפסיק את מתן שירותי מידע פיננסי או את מתן שירות ייזום בסיסי, ידווח לרשות על הצורך בביטול הסרטיפיקט שלו.

25. בעל רישיון אינו רשאי לפנות למקור מידע באמצעות הסרטיפיקט שלו בבקשה לקבל מידע פיננסי או לתת שירות ייזום בסיסי באמצעות מערכת הממשק כל עוד הרישיון או האישור שלו מותלה או מבוטל.

<u>סימן ו' - יצירה, ניהול ושמירה של תעודות דיגיטליות, לרבות סרטיפיקט</u>

26. כל אחת מהתעודות הדיגיטליות, צריכות להיות משויכות לגורם אחראי אחד אצל בעל רישיון, אשר ישמש כבעל התעודה הדיגיטלית, והוא יהיה אחראי על כל מחזור החיים של התעודה הדיגיטלית.

27. בעל רישיון יעשה שימוש בטכנולוגיות עדכניות וידועות לשמירת תעודות דיגיטליות.

28. בעל רישיון יקבע ויטמיע נהלים ומנגנונים מתאימים להתקנה, אחסון ושמירה של תעודות דיגיטליות, בהתאם לסיכונים הכרוכים בפעילות בעל רישיון ולהיקף הפעילות. הנהלים והמנגנונים יתייחסו לעניינים הבאים:

א. הגנה על התעודות הדיגיטליות מפני פעולות או שימוש בלתי מורשים, הכוללים בין היתר: שינוי, החלפה, החדרה ומחיקה של התעודות הדיגיטליות.

ב. מניעת גילוי בלתי מורשה של התכנים הלא-ציבוריים של התעודות הדיגיטליות.

ג. מתן אינדיקציות למצב התפעולי של התעודות הדיגיטליות כדי להבטיח פעולה תקינה שלהם.

ד. איתור שגיאות בתפעול התעודות הדיגיטליות ומניעת זליגה של נתונים רגישים ופרמטרי אבטחה קריטיים כתוצאה משגיאות אלה.

ה. בקרה בזמן אמת על כל שינוי ופעולה המבוצעת על התעודות הדיגיטליות.

<u>סימן ז' - ניהול סיכונים</u>

29. על בעל רישיון לוודא כי מכלול הסיכונים הגלומים בשירותי מידע פיננסי או בשירות ייזום בסיסי, ובכלל זה סיכוני אבטחת מידע, סיכוני סייבר, סיכוני פגיעה בפרטיות, סיכונים תפעוליים, סיכוני מעילות והונאות, סיכונים משפטיים וסיכוני ציות, מנוהלים באופן שהולם את פעילות בעל רישיון, גודלה ומורכבותה ונוכח מידת וסוג הסיכונים הגלומים בפעילותו במתן שירות מידע פיננסי או במתן שירות ייזום בסיסי.

30. מבלי לפגוע בכלליות האמור בסעיף 29, על בעל רישיון:

א. לקבוע ולאשר מסגרת לניהול סיכונים, שתעוגן במדיניות אחת לשנה ולקבוע נהלים ליישום המדיניות בהתאם. מסמך המדיניות יכלול, בין היתר, התייחסות לנושאים הבאים:

1) מטרות השימוש במידע;

2) סוגי המידע השונים הכלולים במאגר המידע;

3) מיפוי תהליכים ומערכות שעליהם יבוצע תהליך של ניהול סיכונים בנושא אבטחת מידע ואופן ההתמודדות עימם;

4) תפיסת הגנת המידע- אבטחת המידע והגנת הפרטיות;

5) האמצעים שיש לנקוט והמשאבים שיש להקדיש לצורך הגנה על נכסי המידע;

6) עקרונות גיבוי, אחזור נתונים והמשכיות עסקית במצבים של תקלות והתממשות תרחישי איום;

7) מיקור חוץ;

8) פיתוח ושינויים במערכות מידע, לרבות שימוש בטכנולוגיות חדשות, ובטכניקות של פיתוח מאובטח.

ב. לגבש ולהטמיע מדיניות שתעגן את המסגרת לניהול בנקאות פתוחה. מדיניות זו תכלול בין היתר גם היבטים של ניהול הסיכונים, השירות ללקוח, אופן החיבור למקורות המידע ואופן העבודה בשכבת התעבורה.

ג. לוודא כי נקבעו תחומי אחריות ברורים והוקצו משאבים נאותים לניהול הסיכונים, לרבות באמצעות מינוי ממונה על אבטחת מידע והגנת סייבר בעל הכשרה וניסיון מתאימים אשר יהיה אחראי למכלול הנושאים הקשורים לניהול המידע והגנתו, כמפורט בהוראה זו, ובפרט האמור בסעיף 32 להלן.

ד. ליישם תהליכים לפיקוח על הטמעת המסגרת לניהול הסיכונים.

ה. ליישם אמצעי אבטחה – פיזיים ולוגיים – למניעה, גילוי, תיקון ותיעוד של חשיפות וסיכונים, דיווח עליהם, והכל בהתאם להערכת הסיכונים ותוך התייחסות גם להיבטים הבאים:

1) זיהוי ואימות (Identification & Authentication);

2) סודיות ופרטיות (Privacy);

3) שלמות ומהימנות של הנתונים (Integrity);

4) מניעת הכחשה (Non Repudiation).

ו. לנהל מעקב שוטף אחר ההתפתחויות הטכנולוגיות והסיכונים, ולהתאים את רמת האבטחה ובקרת הגישה למערכותיו על פי השינויים ברמת הסיכונים הנגזרים משינויים טכנולוגיים אלו.

ז. לפעול להפרדה מלאה של סביבת הייצור (Production) מסביבת הפיתוח (development) והבדיקות (Test).

ח. לבצע זיהוי אישי חד-ערכי של כל גורם בעל גישה למערכות המידע של בעל רישיון כתנאי מוקדם למתן הגישה; במקרים חריגים של ספקים ועובדים בהם לא ניתן לקיים את האמור לעיל, יישם בעל רישיון אמצעים חלופיים מתאימים.

ט. אחת לתקופה, בהתאם להערכת הסיכונים ולא יותר מ-18 חודשים, ליזום סקר בטיחות של מערך טכנולוגיית המידע של בעל רישיון. בסקר תוערך האפקטיביות של אמצעי ההגנה, בהתייחס להערכת הסיכונים, ויוצעו דרכים לתיקון הליקויים שיימצאו.

י. לוודא ולאמת (validate) את פרטי הוראת התשלום המועברת על ידו למנהל חשבון התשלום, בטרם העברתה למנהל חשבון התשלום. לשם כך, בעל הרישיון יתעד כל פעולה שנעשתה במסגרת שירות ייזום בסיסי לרבות מועד ביצוע הפעולה ופרטיה.

31. לצורך יישום האמור בסעיפים 29 - 30, ימנה בעל רישיון ממונה על ניהול סיכונים בעל הכשרה וניסיון מתאימים אשר יהיה אחראי על ניהול הסיכונים בבעל רישיון וידווח להנהלת בעל רישיון, ויכול שאדם זה ישמש גם כממונה על אבטחת מידע והגנת סייבר, כאמור בסעיף 30(ג).

<u>סימן ח' - ממונה על אבטחת מידע והגנת סייבר</u>

32. א. הממונה על אבטחת מידע והגנת סייבר שימונה לפי סעיף 30(ג) יהיה בעל ניסיון וידע בניהול רכיבי אבטחה שיש לו הסמכה כדוגמת אחת או יותר מההסמכות הבאות:

א. CISSP

ב. CISO

ג. CISA

ד. CISM

ה. בודקי ספקים שעמדו בהצלחה בבחינות הסיום לקורס בודקי תאימות סייבר לשרשרת אספקה ארגונית, מגופים המוכרים על ידי מערך הסייבר הלאומי.

ב. הממונה על אבטחת מידע והגנת סייבר יפעל כדלקמן:

1) יכין נוהל אבטחת מידע.

2) יבחן את הצורך בעדכון נוהל אבטחת המידע, לכל הפחות אחת לשנה או כאשר זיהה שינויים מהותיים במערכות המאגר ובתהליכי עיבוד מידע או בחשיפות לסיכונים ויעדכן את הנוהל בהתאם.

3) יכין תוכנית לבקרה שוטפת אחר העמידה בדרישות חוק שירות מידע פיננסי או חוק הסדרת העיסוק בשירותי תשלום, לפי העניין, וההוראות מכוחו ובדרישות חוק הגנת הפרטיות ותקנותיו, יבצע אותה ויודיע על ממצאיו להנהלת בעל רישיון אחת לתקופה כפי שיקבע במדיניות.

4) יעקוב אחר אופן יישום והטמעת מדיניות ונוהלי אבטחת מידע, המלצות סקרי אבטחת מידע והנחיות חוק שירות מידע פיננסי או חוק הסדרת העיסוק בשירותי תשלום, לפי העניין, הרלבנטיות.

5) יגדיר דרישות להגנה על המידע בכל מערכת חדשה שנקנתה או פותחה, ובעת שדרוג של מערכות מידע קיימות ויהיה מעורב ביישום תהליכי רכש או פיתוח של מערכות חדשות ובעת שדרוג מערכות קיימות.

6) במקרים בהם חשיפות בסיכון גבוה לא טופלו בתוך פרק זמן סביר מביצוע סקר אבטחת המידע, יבחן הממונה על אבטחת המידע את הסיבות לאי הטיפול בחשיפות אלו, ויעביר המלצותיו בנושא להנהלת בעל רישיון.

7) יתחקר אירועים חריגים ויעביר המלצותיו תוך פרק זמן סביר להנהלת בעל רישיון.

8) יבחן מעת לעת את תהליכי ניטור המידע שהוגדרו, תקינותם ואיכות האירועים שמתקבלים, ולכל הפחות אחת לשנה.

9) ינחה מקצועית את הארגון בנושאי אבטחת מידע והגנת הפרטיות.

10) יבחן באופן שוטף, את הליכי מחיקת המידע הפיננסי שבהחזקת בעל רישיון על פי ההוראות הקבועות בחוק שירות מידע פיננסי, ובכלל זה האם אין המידע שנשמר במאגר רב מהנדרש לצורך עמידה במטרות המאגר ודרישות חוק שירות מידע פיננסי והוראה זו.

<u>סימן ט' - הגנת הפרטיות</u>

33. בעל רישיון יעמוד בכל עת בהוראות הקבועות בחוק הגנת הפרטיות והתקנות מכוחו, ולעניין הוראות אלו, בעל רישיון המנהל מאגר מידע אשר חלה עליו רמת האבטחה הבסיסית כהגדרתה בתקנות הגנת הפרטיות – יעמוד בכל עת בדרישות החלות על מאגר מידע אשר חלה עליו רמת אבטחה בינונית לפחות.

על אף האמור בתקנה 10(ד) לתקנות הגנת הפרטיות, לעניין שירות ייזום בסיסי נתוני התיעוד של מנגנון הבקרה כאמור בתקנה 10(א) לתקנות הגנת הפרטיות, יישמרו למשך שבע שנים לפחות ממועד יצירתם.

פרק ו': שרשרת אספקה – מיקור חוץ

<u>סימן א' – מיקור חוץ</u>

34. בעל רישיון רשאי לבצע פעילויות ניהול, עיבוד ואחסון של המידע שלו או פיתוח מערכות, לרבות שירותי יעוץ, ידע ושירותים אחרים, על ידי גורמים מחוץ לבעל רישיון, בכפוף לכך שבעל הרישיון יבצע בעצמו את הפעילות המהותית הכרוכה במתן שירות מידע פיננסי או במתן שירות ייזום בסיסי.

35. על אף האמור בפרק זה, בעל רישיון לא יוכל להעביר את אחריותו לקיום כל חובותיו לפי חוק שירות מידע פיננסי או חוק הסדרת העיסוק בשירותי תשלום, לפי העניין, לגורמים אחרים ויראו כל פעולה שנעשתה במיקור חוץ, לרבות שירותי ענן כאמור בפרק ז', כפעילות שנעשתה על ידי בעל הרישיון והוא יישא באחריות המלאה לה; האמור בסעיף זה יחול גם על אחריות בעל רישיון בעת מתן שירות ייזום בסיסי.

36. התקשרות לצורך מיקור חוץ תיעשה בהסכם כתוב.

<u>סימן ב' – ספק מהותי</u>

בסימן זה, "**ספק מהותי**" - גורם חיצוני הנכלל בשרשרת האספקה של בעל רישיון אשר מספק שירותים שמהותיים לפעילותו בתחומים הקשורים לטכנולוגית המידע או חושפים אותו לסיכוני אבטחת מידע פוטנציאליים אשר בהתממשותם ניתן לתקוף את מערכות בעל הרישיון או לפגוע בפעילותו.

37. במיקור חוץ לספק מהותי, בעל רישיון יוודא את מהימנותו ואת חוסנו הכלכלי של הספק המהותי, ויבחן מראש את התאמת כישוריו ואת יכולתו לבצע את מטלותיו.

38. במיקור חוץ לספק מהותי, בעל רישיון –

א. יקבע עקרונות מפורטים להתחייבויותיהם של ספקים מהותיים כלפי בעל רישיון בהתייחס לניהול סיכוני אבטחת מידע.

ב. יעגן בהסכם ההתקשרות עם הספק המהותי התייחסות פרטנית לנושא ניהול סיכוני אבטחת מידע ויוודא כי הספק המהותי עומד בעקרונות שהוגדרו כאמור בסעיף קטן (א) לעיל.

ג. יערוך אחת לתקופה ולא יותר מ-20 חודשים:

1) מיפוי של הספקים המהותיים של בעל רישיון; בחינת הסכם ההתקשרות עימם; עמידתם בהתחייבויותיהם החוזיות; זאת, תוך התייחסות לצורך בשינויים הנדרשים מהספק המהותי כתוצאה מהתפתחויות ושינויים טכנולוגיים ושינויים בשירותים הניתנים.

2) הערכת סיכונים הנגזרים מהשירותים הניתנים על ידי הספקים המהותיים בהתבסס גם על הבחינה כאמור בסעיף קטן (א) ותוצאות הסקרים כאמור בסעיף 30(ט).

39. הסכם ההתקשרות של בעל רישיון עם הספק המהותי -

א. במסגרת הסכם ההתקשרות של בעל רישיון עם הספק המהותי, הסכם ההתקשרות יתייחס מפורשות לפחות לנושאים הבאים:

1) הגדרת תחומי אחריות של כל אחד מהצדדים להסכם, לרבות קבלני משנה;

2) הסכם רמת השירות (SLA);

3) חובת הסודיות, אבטחת מידע, הגנת פרטיות ומצבי חירום;

4) הסדרים להפסקת ההסכם וליישוב מחלוקות, לרבות הסדרים שיאפשרו לבעל רישיון לתפעל ולתחזק את פעילות מיקור החוץ במקרים בהם הספק המהותי חדל מלספק את השירות;

5) התייחסות לקבלת מידע הנוגע למבדקים וביקורות של פעילות הספק המהותי.

ב. בעל רישיון ייקח בחשבון את הצורך בשילוב ההיבטים הבאים בהסכם ההתקשרות עם הספק המהותי, בהתאם להערכת הסיכונים:

1) הקשחת המערכות של הספק המהותי המותקנות ברשת בעל רישיון בהתאם לנהלי אבטחת המידע וניהול הסיכונים של בעל רישיון.

2) העברת קבצי לוג ממערכות הספק המהותי לפי בקשת בעל רישיון.

3) עריכת סקר פגיעויות ומבדקי חדירה אחת לתקופה בהתאם לבקשת בעל רישיון ובהתאם לניהול הסיכונים.

4) טיפול בממצאים שזוהו בסקר ובמבדקי החדירה תוך פרק זמן סביר לאחר זיהויים.

5) ביצוע בדיקות מהימנות לעובדי הספק המהותי המעורבים בפעילות בעל רישיון.

6) מינוי נאמן אבטחת מידע אצל הספק המהותי והגדרת סמכויותיו ותפקידיו.

7) הצגת רשימה של ספקי משנה אשר תומכים בשירותים הניתנים לבעל רישיון על ידי הספק המהותי מידי תקופה שתיקבע על ידי בעל רישיון.

8) קביעת הסדרים למחיקת נתונים של בעל רישיון המאוחסנים בחצרות הספק המהותי בסיום ההתקשרות בין הצדדים, לפי דרישת בעל רישיון וכן על פי חובות המחיקה החלות על בעל רישיון.

9) ביצוע הפרדת סביבות בחצרות הספק המהותי (פיתוח וייצור).

10) ביצוע הפרדת סביבות עבודה (tenants) של בעל רישיון במידה והספק המהותי מספק שירותים לנותני שירות/תאגידים נוספים.

11) דיווח לבעל רישיון על כל אירוע אבטחת מידע בקשר לפעילות בעל רישיון שהתרחש אצל הספק המהותי או אצל ספק המשנה שלו.

40. בעל רישיון יגדיר פעילויות בהתאם להערכת הסיכונים, עבורן נדרש הספק המהותי לאמצעי זיהוי חזקים (Multi-Factor Authentication) בפעילויות, כגון: גישה מרחוק למערכות בעל רישיון, פעילות תחזוקה במערכות בעל רישיון, וכדומה.

41. בעל רישיון יקבע מנגנוני אבטחה ובקרה בגישה מרחוק של הספק המהותי, בהתאם להערכת הסיכונים, כגון: מניעת גישה אלא אם אושרה על ידו; גישה מאובטחת מסביבת פעילות נפרדת מיתר סביבות העבודה של הספק המהותי; הפעלת מנגנון ניתוק התקשורת (Time-out) לאחר פרק זמן שבו לא בוצעה פעילות מצד הספק המהותי; הקלטת וניטור פעילות תחזוקה; וכדומה. כמו כן, גישה לסביבת הייצור של בעל רישיון לא תתאפשר, אלא אם אושרה על ידו.

42. בכל שינוי בבעלות של הספק המהותי, על בעל רישיון לבחון מחדש את ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם על ידי הבעלים החדשים.

פרק ז': מחשוב בענן

43. בטרם הפעלת שימוש במערכות מבוססות ענן, על בעל רישיון לבצע מיפוי והערכת סיכונים נאותים, במעורבות כלל הגורמים הרלוונטיים בבעל רישיון, ולפרט גם את הבקרות, הכלים והצעדים הנדרשים למזעור הסיכונים. הערכת הסיכונים תעודכן באופן שוטף במהלך תקופת

ההתקשרות, בין היתר, בהתאם לשינויים טכנולוגיים, משפטיים, רגולטוריים, עסקיים וארגוניים אצל בעל רישיון ואצל ספק שירותי הענן.

44. במחשוב ענן מהותי, לפני התקשרות עם ספק שירותי הענן, על בעל רישיון לבצע בדיקת נאותות (Due Diligence) לרבות בנוגע לחוסנו הכלכלי של הספק, יכולתו המקצועית וניסיונו לספק שירותים דומים. על בעל רישיון לבצע מעת לעת בדיקה כאמור, גם במהלך תקופת ההתקשרות.

45. בעל רישיון יגבש מדיניות לשימוש בטכנולוגיות מחשוב ענן אשר תתייחס בין היתר לסוגי היישומים והשירותים בטכנולוגיית מחשוב ענן, סמכויות ואחריות, בקרות, היבטים משפטיים, פיתוח, תחזוקה, ניטור, אבטחת מידע וכדומה.

46. בעל רישיון רשאי לאחסן מידע רגיש או נתוני לקוחות מחוץ לגבולות מדינת ישראל, אם וידא שספק שירותי הענן מקיים את רמת ההגנה בהתאם לדירקטיבה על הגנת המידע במדינות האיחוד האירופי (GDPR) והודיע על כך ללקוח.

47. אין בהוראה זו כדי לגרוע מהחובות החלות על בעל רישיון לפי כל החוקים והתקנות הרלוונטיים לשימוש בטכנולוגיות מחשוב ענן, ובכלל זאת, חוק הגנת הפרטיות ותקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א- 2001, וכן, הנחיית רשם מאגרי מידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי".

48. בעל רישיון יוודא עמידת ספק מחשוב הענן בתקני אבטחת מידע ואבטחה פיזית מקובלים והסמכות חיצוניות, הכוללים בין היתר התייחסות לזיהוי אימות, הרשאות גישה, בקרת פעילות ולוגים, סקרים ומבדקי הגנת סייבר.

49. גישה לנתונים בענן תבוצע באמצעות דרכי גישה מאובטחים כגון: כתובות מורשות בלבד, אימות חד חד ערכי (Multi-Factor Authentication), הצפנה וכדומה.

50. במקרים בהם נתוני בעל רישיון מאוחסנים במערכת שאינה לשימושו הבלעדי של בעל רישיון (Multi-tenant), יעשה שימוש בטכנולוגיות כגון הצפנה, מיסוך נתונים או טוקניזציה, במטרה למנוע חשיפה של מידע רגיש או נתוני לקוחות לגורמים שאינם מורשים.

51. בשירותי מחשוב ענן, מידע רגיש יוצפן, גם אם התשתית היא ייעודית.

52. בעל רישיון יוודא שיש לו אפשרות לבצע ניטור אירועי אבטחת מידע המתרחשים בענן.

53. במחשוב ענן, על בעל רישיון לוודא כי עבור כלל ערוצי הגישה מספק מחשוב הענן ואליו, קיימים אמצעים להגנת הסייבר ואבטחת מידע, שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפת בעל רישיון.

54. בעל רישיון יכלול בהסכם ההתקשרות עם ספק מחשוב הענן, בין היתר:

א. קיום אפשרות חד צדדית של בעל רישיון להפסיק את השימוש בשירותי ספק מחשוב הענן או לעבור לספק אחר תוך העברת נתוניו הרלוונטיים ממערכות הספק תוך זמן

קצר, מחיקתם במערכות הספק והתחייבות הספק שלא ניתן לאחזר מידע זה במערכותיו.

ב. התייחסות לקבלת מידע הנוגע למבדקים וביקורות על ספק שירותי הענן.

55. בכל שינוי בבעלות של ספק שירותי הענן, על בעל רישיון לבחון מחדש את ההתקשרות כדי להבטיח קיום ההתחייבויות כלפיו גם על ידי הבעלים החדשים.

פרק ח': דיווחים

<u>סימן א' - כללי</u>

56. בעל רישיון שירות מידע פיננסי ידווח לרשות על אודות פעילותו, הן באופן תקופתי והן באופן שוטף, כקבוע בהוראות אלה.

57. כל מסמך או הצהרה שמגיש בעל רישיון שירות מידע פיננסי לרשות לפי פרק זה יוגש או יינתן על ידי נושא משרה בכירה בו המוסמך להגישו או לתתו ובאופן הקבוע בסעיף 4 לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

<u>סימן ב' – דיווחים שנתיים</u>

58. בעל רישיון שירות מידע פיננסי יגיש לרשות, לא יאוחר מיום 31 במרס של כל שנה, דיווח על הפרטים המפורטים בסעיף זה. הדיווח יתייחס ליום האחרון של השנה שקדמה למועד הגשת הדיווח (להלן גם: "**שנת הדיווח**"), זולת אם נאמר אחרת בסעיף זה.

א. אישור קיומו של ביטוח כאמור בסעיף 8(א) (אם בחר בעל הרישיון בחלופה זו) הכולל פירוט תנאי הביטוח של בעל הרישיון לרבות שם המבטח, תקופת הביטוח, סכום הביטוח וסכום ההשתתפות העצמית וכן אישור הדירקטוריון כי היקף הביטוח ותנאיו ברמה מספקת לשם כיסוי חבותו של בעל הרישיון בשל מעשה או מחדל רשלני כלפי לקוח; או אישור פרטי הפיקדון כאמור בסעיף 8(ב) (אם בחר בעל הרישיון בחלופה זו), ואישור מאת הנאמן לגבי זהות הגוף בו הופקד הפיקדון, וכי הוא מנוהל כפי שנדרש בסעיף 8(ב) וכן אישור הדירקטוריון כי היקף הפיקדון נקבע בהתאם לנדרש בסעיף 8(ב).

ב. חוות דעת עדכנית[3] של מבקר תוך הדגשת השינויים שחלו בעניינים המפורטים בסעיף 2(6)(א)(1) לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

ג. מפת סיכונים עדכנית תוך הדגשת השינויים שחלו בעניינים המפורטים בסעיף 2(12) לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

[3] בעל רישיון שקיבל רישיונו בין חודש יולי לחודש דצמבר של שנת הדיווח, רשאי שלא להגיש חוות דעת מבקר במסגרת הדיווח השנתי (הראשון) שלו כבעל רישיון בגין אותה שנת דיווח.

ד. מצבת עדכנית של נושאי משרה בכירה בבעל רישיון שירות מידע פיננסי, בבעל השליטה בבעל הרישיון ונושאי משרה בכירה בבעל השליטה (במידה והוא תאגיד) ופרטיהם כמפורט בסעיף 2(2) לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

<u>סימן ג' – דיווחים חודשיים</u>

59. בעל רישיון שירות מידע פיננסי ידווח לרשות בתום כל חודש ולא יאוחר מעשרה ימי עסקים לאחר מכן, בהתאם לטופס הרלוונטי באתר הדיווח, על אודות:

א. פעילותו בבנקאות הפתוחה, לרבות מספר הפניות שנעשו למקורות המידע, מספר לקוחות, מספר הסכמות הלקוח לאיסוף מידע ממקורות המידע שהתקבלו או בוטלו, מספר דיווחים אודות רמות השירות.

ב. מספר תלונות לקוחות לרבות לעניין פגם במידע כהגדרתו בסעיף 61(א) לחוק שירות מידע פיננסי, בעיות בחיבור למקורות המידע או כשלים מהותיים במתן שירות מידע פיננסי.

ג. מספר פניות שנדחו, מספר לקוחות שהצטרפו או עזבו.

<u>סימן ד' – דיווחים מיידים</u>

60. המועד להגשת דוח מיידי הוא עד תום יום העסקים הראשון לאחר המועד שבו נודע לבעל רישיון שירות מידע פיננסי לראשונה על קרות האירוע; לעניין זה, "נודע לבעל רישיון שירות מידע פיננסי לראשונה על קרות האירוע" – נודע לראשונה על התרחשות אירוע לאחד מאלה: יושב ראש הדירקטוריון של בעל הרישיון, המנהל הכללי שלו, מנהל העסקים הראשי שלו, נושא המשרה הבכיר ביותר בתחום הכספים בבעל הרישיון, מזכיר החברה, או ממלא תפקיד מהתפקידים האמורים בבעל הרישיון אף אם תואר משרתו שונה.

61. בדוח יצוינו היום שבו התרחש האירוע המדווח אם הוא ידוע לבעל רישיון שירות מידע פיננסי, והיום שבו נודע לבעל הרישיון לראשונה על קרות האירוע המדווח.

62. בעל רישיון שירות מידע פיננסי יעביר לרשות דיווח מיידי במקרים הבאים:

א. דיווח על שינוי פרטי בעל הרישיון, כפי שמסר אותם לרשות.

ב. התקבלה החלטה לכל שינוי מהותי בפרטי בקשת הרישיון כפי שהוגשה לרשות או בדיווח השנתי האחרון שלו לרשות כאמור בסעיף 58, אשר יש לו או עשויה להיות לו השפעה מהותית על בעל הרישיון או על לקוחותיו.

ג. אירע אירוע אשר יש לו או עשויה להיות לו השפעה מהותית על בעל הרישיון או על לקוחותיו.

ד. התקבלה החלטה לכל שינוי או עדכון בסוגי השירות הניתנים על ידי בעל רישיון לשירות מידע פיננסי או שינויים מהותיים באופי פעילותו של בעל רישיון העלולים להשפיע על סיכונים עסקיים ותפעוליים של בעל רישיון.

ה. אירע אירוע אבטחה חמור כמשמעותו בסעיף 31 לחוק שירות מידע פיננסי, יודיע בעל רישיון על כך באופן מיידי לרשות וכן ידווח על תוצאות התחקיר שערך ועל הצעדים שנקט בעקבות האירוע.

ו. דיווח על הודעה שמקור מידע מסר לבעל רישיון לפי סעיף 41(א)(2) לחוק שירות מידע פיננסי והנימוק שמסר לו לאי מתן הגישה למידע, וכן הודעה על הסרת מניעת הגישה שקיבל בעל רישיון ממקור מידע לפי סעיף 41(א)(3) לחוק שירות מידע פיננסי.

ז. אירוע של פגיעה בשלמות המידע, אירוע שנעשה בו שימוש במידע בלא הרשאה או בחריגה מהרשאה או שיש אינדיקציות לכך שמידע רגיש אודות לקוחות נחשף או דלף אל מחוץ לחצרות בעל רישיון או כל אירוע משמעותי אחר שהתרחש או כמעט והתרחש בעל השפעה מהותית על ניהול המידע והגנתו.

ח. נפגעו או הושבתו מערכות המכילות מידע רגיש ליותר מ-3 שעות, למעט השבתה יזומה, או הפסקה של שירותים מהותיים כתוצאה מהשבתה לא מתוכננת של פעילות המערכות הממוכנות למשך יום עסקים אחד או יותר.

ט. התממשות אירועים חריגים, לרבות ניסיונות מהותיים של חדירה ותקיפה, חדירה בפועל למערכות מחשב, קריסה של מערכות מרכזיות, הפעלת תוכנית להתמודדות עם אירועים חריגים וכיוצא באלה.

י. אירוע של שימוש ללא הרשאה בסרטיפיקט.

יא. הוגשה הודעה לחברת ביטוח בקשר עם אירוע ביטוח שהתרחש, בנוגע לביטוח אותו ערך בעל רישיון לפי סעיף 8(א), ידווח תוכן ההודעה ומועד הגשתה.

יב. חל שינוי בהיקף הכיסוי או בתחום הכיסוי של ביטוח שערך בעל רישיון לפי סעיף 8(א), ידווח פרטים בדבר השינוי, מועדו והסיבות לו.

יג. חל שינוי בפיקדון שהפקיד בעל הרישיון לפי סעיף 8(ב) או בפרטי הנאמן לפיקדון.

יד. הודעה לפי סעיף 20(א) לחוק שירות מידע פיננסי תוגש כדיווח מיידי.

טו. מונה אדם לנושא משרה בכירה בבעל רישיון או בבעל שליטה, יובאו לגביו הפרטים המנויים בסעיף 2(2) לכללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

טז. מונה אדם לממונה אבטחת מידע או לממונה על ניהול הסיכונים בחברה, יובאו לגביו הפרטים המנויים בסעיף 31 או 32 להוראה זו, בהתאמה.

יז. חדל אדם להיות נושא משרה בכירה בבעל רישיון או בבעל שליטה או חדל להיות ממונה אבטחת מידע או ממונה על ניהול סיכונים בחברה, יודיע בעל הרישיון על כך לרשות.

יח. דיווח לפיו חל שינוי בהחזקות בעל שליטה בבעל רישיון כך שהוא חדל להיות בעל שליטה או אם הפך אדם לבעל שליטה בבעל רישיון ללא היתר שליטה.

63. על אף האמור בסעיף 60, דיווחים לפי סעיף 62(טו) ו- 62(טז) יוגשו עד תום 7 ימי עסקים לאחר המועד שנודע לבעל רישיון שירות מידע פיננסי לראשונה על קרות האירוע.

פרק ט': תחילה, הוראות מעבר ובחינה תקופתית

64. תחילתו של תיקון מספר 2 להוראה זו יומיים מיום פרסום הודעה על נתינתה ברשומות (להלן – יום התחילה).

65. על אף האמור בסעיף 7א, חברות שביום התחילה החזיקו ברישיון למתן שירות מידע פיננסי ובאישור למתן שירות ייזום תשלומים כהגדרתו בנוהל בנקאי תקין מס' 368 ערב יום התחילה, יגישו בקשה מקוצרת לאישור למתן שירות ייזום בסיסי אשר תכלול את הפרטים האמורים בסעיפים קטנים (א) ו-(ו) בלבד בסעיף 7א (פירוט המבנה הארגוני ושירותי מיקור חוץ ופירוט הסדרי ממשל תאגידי ומנגנוני בקרה פנימית).

66. על אף האמור בסעיף 64, לגבי חברות שביום התחילה החזיקו ברישיון למתן שירות מידע פיננסי - יחולו ההוראות הבאות, עד ליום 6.12.2024:

א. הגדרת "מערכת הממשק" תיקרא כמערכת ממשק למידע פיננסי כהגדרתה בחוק שירות מידע פיננסי וכן לעניין שירות ייזום בסיסי - ממשק טכנולוגי מאובטח ומקוון, המאפשר גישה לחשבון תשלום, לצורך שירות ייזום תשלומים לפי נוהל בנקאי תקין מס' 368;

ב. התיקון לפרק ג' בנושא דרישות ביטוח או פיקדון לא ייכנס לתוקף וייקראו הוראות פרק ג' כנוסחו ערב תיקון מספר 2 להוראה.[4]

---

[4] "פרק ג': דרישות ביטוח או פיקדון

8. על בעל רישיון לעמוד בדרישה לביטוח או לבטוחה מסוג פיקדון, כפי שיפורט להלן:

א. בעל רישיון ביטח את אחריותו כלפי הלקוחות; תחומי כיסוי הביטוח, היקפו ותנאיו יהיו ברמה מספקת לדעת דירקטוריון בעל הרישיון, לכיסוי חבותו של בעל הרישיון בשל מעשה או מחדל רשלני כלפי לקוח, ובהיקף שלא יפחת מ- 500,000 ₪. הביטוח ייעשה אצל מי שהוא בעל רישיון לפי חוק הפיקוח על עסקי ביטוח, התשמ"א – 1981.
הביטוח שנערך לפי סעיף זה, יכסה תביעות בשל אירועים שאירעו בתקופת הפוליסה, גם אם הוגשו בתוך שנה מתום תקופת הפוליסה.
דירקטוריון בעל הרישיון יבחן ויאשר פעם בשנה או בעת שינוי מהותי כי תחומי כיסוי הביטוח, היקפו ותנאיו עומדים בדרישות סעיף זה.

ב. בעל רישיון הפקיד פיקדון בסכום מספק לדעת דירקטוריון בעל הרישיון לכיסוי חבותו של בעל הרישיון בשל מעשה או מחדל רשלני כלפי לקוח ושלא יפחת מ 500,000 ₪. הפיקדון יופקד באיגרות חוב הנסחרות בבורסה שמנפיקה הממשלה ושאינן ניתנות להמרה לניירות ערך המקנים זכות השתתפות או חברות בתאגיד, או באיגרות חוב הנסחרות בבורסה המדורגות בדרגת השקעה גבוהה (להלן -הפיקדון).
הפיקדון יהיה בתוקף למשך שנה מיום שחדל בעל הרישיון לפעול במסגרת הרישיון.

67. בחינה ראשונה של תיקון מספר 2 להוראה זו לפי סעיף 36 לחוק עקרונות האסדרה, התשפ"ב–2021, תתבצע לכל המאוחר, בתום 10 שנים מיום תחילתו.

מועד פרסום ההוראה באתר הרשות: 15.3.2022
תאריך עדכון (מס' 1): 7.9.2022
תאריך עדכון (מס' 2): 4.6.2024

* * *

עדכונים

גרסה	פרטים	תאריך
הוראה מקורית		15.3.22
עדכון מס' 1	נוספו הגדרות, שונו סעיפים 2-5,[5] נוספו סעיפים 7א-7ב, תוקנו סעיפים 8, 10, 17, 29, 32-34, 57-59, 62, נוסף פרק ד'1 (סעיפים 9א-9ד) להוראה.	7.9.22

דירקטוריון בעל הרישיון יבחן ויאשר פעם בשנה או בעת שינוי מהותי כי סכום הפיקדון עומד בדרישות סעיף זה.
על הפיקדון להיות מופקד למשמרת אצל בנק או אצל חבר בורסה על שם עורך דין או רואה חשבון שישמש נאמן לפיקדון (להלן - הנאמן); הנאמן ינהל את הפיקדון לטובת לקוחות בעל הרישיון (להלן – חשבון הנאמנות); חשבון הנאמנות לא יהיה ניתן לשעבוד, למשיכה או לעיקול אלא בהוראת הנאמן ובהתקיים אחד מאלה:
1) ניתן פסק דין של בית משפט בתובענה של לקוח נגד בעל הרישיון בשל אחריותו כלפי לקוחותיו או אושר הסכם פשרה או פסק בורר בין צדדים כאמור על ידי בית המשפט; פסק דין, הסכם פשרה או פסק בורר כאמור יכללו, בין השאר, את פירוט הזכאים לתשלום והסכומים שלהם הם זכאים.
2) בעל רישיון נמצא בהליכי חדלות פירעון וסכום הפיקדון דרוש לשם ביצוע פסק דין או פסק בורר שאישר בית המשפט בתובענה בשל אחריותו כלפי לקוחותיו: בפסקה זו, "הליכי חדלות פירעון" – הליכי פירוק או כינוס נכסים לפי פקודת החברות [נוסח חדש], התשמ"ג-1983, או הליכים לפי סעיף 350 לחוק החברות.
ג. השיקולים שעל דירקטוריון בעל הרישיון לשקול בקובעו את היקף הביטוח או הפיקדון יהיו, בין השאר, כדלקמן:
1) פרופיל הסיכון של בעל הרישיון – מספר התביעות שהוגשו לקבלת כספים בשל אחריות בעל הרישיון כנותן שירות מידע פיננסי ומספר החשבונות מהם אסף בעל הרישיון מידע פיננסי.
2) סוג הפעילות של בעל הרישיון – האם בעל הרישיון מספק רק שירות מידע פיננסי או שירותים נוספים כגון שירות ייזום תשלומים, שירותי תשלום, או שירותים שאינם שירותים פיננסים.
3) היקף הפעילות של בעל הרישיון – מספר הלקוחות של בעל הרישיון.
ד. הסכומים לפי סעיף 8(א) או 8(ב) יעודכנו ב-1 בינואר של כל שנה (להלן - יום העדכון), לפי שיעור השינוי שחל במדד האחרון שפורסם לפני העדכון לעומת המדד הבסיסי, ויעוגל לסכום הקרוב שהוא כפולה של אלף שקלים חדשים; לעניין זה, "המדד הבסיסי" – המדד שפורסם לאחרונה לפני יום העדכון הקודם."

[5] בשל פרסומם במסגרת כללי הגשת בקשת רישיון למתן שירות מידע פיננסי.

עדכון מס׳ 2	נוספו הגדרות, תוקנו סעיפים 2-4, נוספו פרקים ב׳1-ב׳2 (סעיפים 7א-7ד) להוראה, תוקנו סעיפים 8-14, 17-19, נוסף סעיף 19א, תוקנו סעיפים 21-22, 24-25, 29-30, 32-35, 56-62, 64 ונוספו סעיפים 65-67.	4.6.24