רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

הוראה למבקשי ובעלי רישיון למתן שירות מידע פיננסי

הוראה לפי סעיפים 4, 5, 27(ג)(1), 35, 36 לחוק שירות מידע פיננסי, התשפ"ב-2021

דברי הסבר

חוק שירותי מידע פיננסי, התשפ"ב - 2021 (להלן: "**החוק**") אשר נחקק בחודש נובמבר 2021, הסמיך את רשות ניירות ערך (להלן: "**הרשות**") להעניק רישיונות למתן שירות מידע פיננסי לתאגידים העומדים בדרישות הקבועות בחוק, ולפקח על בעלי רישיונות כאמור בהתאם לעקרונות שנקבעו בחוק.

החוק עוסק במתן שירות מידע פיננסי שהוא שירות מקוון במסגרתו בעל רישיון למתן שירות מידע פיננסי (להלן: "**בעל רישיון**", "**בעל רישיון 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.

<u>מטרת ההוראה</u>

במסגרת החוק, הוסמכה הרשות לקבוע הוראות למבקשי רישיון ובעלי רישיון למתן שירות מידע פיננסי בעניינים שונים המוסדרים בחוק, וזאת על מנת להבטיח את עמידת בעלי הרישיון בדרישות החוק ופיקוח יעיל על פעילותם. בפרט הוסמכה הרשות לקבוע עבור בעלי רישיון הוראות בתחומים של אבטחת מידע והגנת פרטיות הלקוחות, תחומים העומדים במרכזו של החוק העוסק בשירותים הניתנים על בסיס מידע פיננסי רגיש של לקוחות. לאור האמור מטרת ההוראה היא לקבוע כללים בנושא הגשת בקשה לרישיון והפרטים והמסמכים שמבקש רישיון נדרש לצרף לה. כמו כן, ההוראה קובעת את דרישות אבטחת המידע, ניהול סיכונים והגנת סייבר, בהן נדרש בעל רישיון לעמוד לצורך

פעילותו. עוד קובעת ההוראה את דרישות הביטוח או הפיקדון להן נדרש בעל רישיון כחלק מדרישות הרישיון. לבסוף, ההוראה קובעת את הדיווחים שבעל רישיון חייב לדווח לרשות, על מנת לאפשר פיקוח יעיל על פעילותו ועמידתו בדרישות החוק.

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;

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

"**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 החוק;

"**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. תאגיד המבקש לקבל רישיון למתן שירות מידע פיננסי יגיש בקשה באתר הדיווח שתכלול את הפרטים הבאים:

א. פרטי המבקש – לרבות מענו הרשום, מספר הטלפון, כתובת דואר אלקטרוני, שמו ומספרו הרשום ברשם החברות, פרטי איש קשר מטעמו ודרכי ההתקשרות עמו, והכל כפי שמפורט בטופס הבקשה באתר הדיווח.

ב. לצורך בחינת מהימנות המבקש ובעל שליטה בו - פרטי כל נושא משרה בכירה במבקש, פרטי בעל השליטה במבקש ופרטי כל נושא משרה בכירה בבעל השליטה (במידה והוא תאגיד) – לרבות שמו המלא, מספר תעודת זהות או מספרו הרשום ברשם החברות, תאריך הלידה שלו ותפקידו במבקש או בבעל השליטה והכל כפי שמפורט בטופס הבקשה באתר הדיווח. על הגורמים האמורים למלא תצהיר שיצורף לבקשה.

ג. זהות הממונה על אבטחת המידע והגנת הסייבר והממונה על ניהול סיכונים במבקש.

ד. סוג השירות שהוא מבקש לתת.

ה. פרטי הערוץ המקוון באמצעותו בכוונת המבקש לפעול במתן שירות מידע פיננסי, אם ישנו, וכן כל שם מסחרי שתחתיו יספק המבקש את שירותיו, אם הוא שונה משמו הרשום ברשם החברות.

ו. פירוט האמצעים הטכנולוגיים שבידיו לצורך פעילות במתן שירות מידע פיננסי ומיומנותו בהפעלתם. לצורך בחינת עמידתו של המבקש בתנאי זה, על המבקש לכלול בבקשתו כל פרט מהותי בקשר עם קיומם של אמצעים טכנולוגיים מתאימים, לרבות את המידע ואת המסמכים הבאים:

1) חוות דעת של מבקר בדבר עמידת המבקש בדרישות הוראה זו. חוות דעת של מבקר תינתן בהתאם לאמור בסעיף זה להלן:

(א) חוות דעת של מבקר לפי כללים מקובלים, בדבר קיום הדרישות המנויות בהוראה זו הנוגעות להגנה על מידע וסייבר, ובכלל זה הדרישות לפי פרקים ה' עד ז', נאותות מערכות המידע של המבקש, מערכות הערוצים המקוונים, אמצעי האבטחה של המבקש ועמידה בתקני אבטחת מידע מקובלים בינלאומיים או לפי תורת ההגנה העדכנית, שפורסמה על ידי מערך הסייבר הלאומי[1];

[1] https://www.gov.il/he/departments/general/cyber_security_methodology_2

(ב) חוות הדעת תכלול גם התחייבות של המבקר לשמור את כל המסמכים ששימשו להכנת חוות דעתו לתקופה שלא תפחת משלוש שנים ממועד מתן חוות הדעת;

(ג) לעניין סעיף זה, "מבקר" הוא מי שמתקיימים בו כל אלה:

(1) יחיד בעל ניסיון של לפחות 3 שנים בביצוע ביקורות טכנולוגיות כאמור בסעיף זה;

(2) המבקר או התאגיד שבו הוא עובד או שותף אינם מצויים בניגוד עניינים או תלות בקשר עם חוות הדעת, למעט קבלת שכר עבור הכנת חוות הדעת[2];

(3) תושב ישראל;

(4) בעל תואר אקדמי רלוונטי ממוסד להשכלה גבוהה בישראל המוכר על ידי המועצה להשכלה גבוהה;

(5) בעל הסמכה בביקורת מערכות מידע או באבטחת מערכות מידע שהיא כדוגמת אחת מבין ההסמכות הבאות: CISA; CRISC או רואה חשבון מוסמך בישראל בעל התמחות במערכות מידע.

2) אישור כי האדם הממונה על אבטחת מידע והגנת סייבר במבקש, כאמור בסעיף 30(ג) הוא בעל ניסיון וידע בניהול רכיבי אבטחה שיש לו הסמכה כדוגמת אחת או יותר מההסמכות הבאות:

(1) CISSP

(2) CCSA

(3) CCNA

(4) CISO

(5) CISA

(6) CISM

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

[2] חזקה שמבקר נמצא בניגוד עניינים או שנפגעה אי-תלותו במבקש, אם במסגרת חוות הדעת שהוא מכין, עליו להתייחס לעניינים שיש לו או לתאגיד בו הוא עובד או שותף עניין אישי לרבות עניין כלכלי בהם.

3) פרטים בדבר אופן אחסון הערוצים המקוונים ומאגרי המידע של המבקש. יובהר כי אחסון המידע אצל ספק אינטרנט שאינו כפוף לדיני מדינת ישראל לא פוטר את המבקש מעמידה במכלול חובותיו מכוח הוראות הדין והוראה זו.

4) הייתה למבקש הרישיון הסמכה רלוונטית בתחום אבטחת המידע, כגון עמידה בתקני אבטחת מידע מוכרים, יצרף אסמכתא על כך לבקשתו.

ז. תכנית עסקית המעידה על יכולת המבקש לעמוד בהוראות הדין ובתנאי הוראה זו. התוכנית העסקית תציג פירוט של תהליכי העבודה הבאים:

1) השירותים המוצעים ודרכי מתן השירותים;

2) אופן קבלת המידע הפיננסי, שמירתו והעברתו לאחר או הצגתו ללקוח;

3) התשתיות המעורבות בתהליך, לרבות תשתיות מחשוב, טכנולוגיה, ציוד, ספקי משנה וכוח אדם.

ח. הצהרה בדבר האמצעים הכספיים של מבקש הרישיון, ובכלל זה מקורות מימון קיימים או עתידיים ומסמכים המאמתים את ההצהרה כאמור.

ט. על המבקש לכלול בבקשה אישור כי מתקיים בו אחד מאלה:

1) אישור כי הוא ביטח את אחריותו כלפי לקוחותיו כמפורט בסעיף 8(א) להלן. על האישור לכלול את פירוט תנאי הביטוח של המבקש לרבות שם המבטח, תקופת הביטוח, סכום הביטוח וסכום ההשתתפות העצמית, וכן אישור הדירקטוריון כי היקף הביטוח ותנאיו הם בהיקף ובתנאים הנדרשים להבטחת אחריותו של בעל הרישיון כאמור בסעיף 8(א) ונקבע בהתאם לשיקולים המנויים בסעיף 8(ג).

2) אישור על הפקדת פיקדון בסכום ובתנאים כמפורט בסעיף 8(ב). על אישור פרטי הפיקדון שהפקיד המבקש לכלול את סכום הפיקדון שהופקד וזהות הגוף בו הופקד; פרטי הנאמן לפיקדון כהגדרתו בסעיף 8(ב); אישור הנאמן שהפיקדון הופקד למשמרת אצל בנק או חבר בורסה וכי הוא מנוהל כפי שנדרש בסעיף 8(ב); וכן אישור הדירקטוריון כי סכום הפיקדון הוא בהתאם לנדרש להבטחת אחריותו של בעל הרישיון כאמור בסעיף 8(ב) ונקבע בהתאם לשיקולים המנויים בסעיף 8(ג).

י. אישור על רישום בפנקסי מאגרי המידע לפי חוק הגנת הפרטיות וכן הצהרה של המבקש בדבר עמידתו בהוראות חוק הגנת הפרטיות והתקנות מכוחו.

יא. תיאור עיסוקים נוספים של המבקש מלבד כוונתו לפעול במתן שירות מידע פיננסי, ככל שישנם. בפרט יתאר המבקש עיסוקים נוספים שלו הטעונים רישוי או רישום אחר.

יב. מפת סיכונים הכוללת הערכת סיכונים הטמונים בתהליכי העבודה השונים, ופירוט אופן ניהולם, גידורם והצעדים הנדרשים למזעורם (MITIGATION). מפת הסיכונים תתייחס לסיכוני אבטחת מידע, סיכוני הגנת פרטיות, סיכוני מעילות והונאות, סיכונים משפטיים וסיכוני ציות.

מבקש העושה שימוש בספקי משנה נדרש לפרט את אופן ניהול שרשרת המידע, הסיכונים הגלומים בכך ואופן ניהול וגידור אותם סיכונים, כאמור בפרק ה' להוראה זו.

יג. המבקש יצרף לבקשה מסמך ובו פירוט בנוגע למאגר המידע שבו יישמר המידע הפיננסי, לרבות:

1) תיאור כללי של פעולות האיסוף והשימוש במידע הפיננסי;

2) תיאור מטרות השימוש במידע הפיננסי;

3) סוגי המידע השונים הכלולים במאגר המידע בשים לב לרשימת סוגי המידע שבפרט 1(3) בתוספת הראשונה לתקנות הגנת הפרטיות;

4) פרטים על מיקום החזקת מאגר המידע;

5) פרטים בדבר ביצוע פעולות עיבוד מידע באמצעות אחר;

6) עבור עוסק ותיק כהגדרתו בסעיף 81 לחוק - אופן הפרדת פרטי הגישה של הלקוח אל חשבונו שנועדו לאמת את זהותו בפני מקור המידע, מהמידע הפיננסי המוחזק במאגר;

7) שמותיהם של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת המידע בו.

יד. אישור המבקש כי מתקיימים בו כל תנאי הכשירות הקבועים בהוראה זו וכן תצהיר של נושא משרה בכירה במבקש המאשר התקיימותם של תנאים אלו.

3. כל מסמך או הצהרה שמגיש מבקש הרישיון לפי הוראות אלו, ייחתמו בידי המורשים לחתום בשם התאגיד, ויצוין בהם תאריך החתימה; בצד כל חתימה יצוין שם החותם ותפקידו בתאגיד. סגל הרשות רשאי לדרוש מהמבקש להעביר לידיו פרטים משלימים אם ימצא כי הדבר דרוש לצורך קבלת החלטה בבקשתו לרישיון מתן שירות מידע פיננסי.

4. חל שינוי בפרט מהפרטים שמסר המבקש לרשות בבקשתו או במסמכים שצורפו לה, ידווח על כך לרשות, בהקדם האפשרי מהמועד בו נודע לו על שינוי הפרט ויצרף את המסמכים הנוגעים לעניין.

5. תאגיד חוץ כהגדרתו בסעיף 18(א) לחוק, הרוצה להגיש בקשה לקבלת רישיון ובמסגרתה לבקש פטור מאחת הדרישות המצוינות בסעיף 18(ב) לחוק, יגיש בקשה מתאימה לרשות. במסגרת

בקשתו, יפרט המבקש מהו הדין הזר המסדיר את עיסוקו במתן שירות מידע פיננסי, באיזה רישיון או רישום זר הוא מחזיק ומיהו המאסדר הזר המפקח עליו. בנוסף יפרט המבקש מהן דרישות הרישיון מהן הוא מבקש לקבל פטור, ומהי האסדרה והפיקוח החלים עליו אשר נותנים מענה מספק בנוגע לעניינים המוסדרים בסעיפים מהם הוא מבקש לקבל פטור וכל מידע נוסף הנדרש לשם קבלת החלטה בבקשתו לפטור מהסעיפים האמורים. המבקש יצרף לבקשתו אסמכתאות לכל הנאמר בה, ובכלל זה אישור מהמאסדר הזר בנוגע לרישיון או הרישום בו הוא מחזיק או רשום.

6. גוף אשר הגיש בקשה לקבלת רישיון ובקשתו טרם נענתה, יוכל להגיש בקשה לקבלת סרטיפיקט לסביבת הטסט. 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(ה) לעיל. 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.

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 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.

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 לפי החוק 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 לפי החוק: 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 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.

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 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 ללקוחותיו;

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

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

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 של 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 למידע פיננסי 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 יעשו בהתאם לסטנדרט.

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

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

12. לאחר רישום פרטי הלקוח מול בעל רישיון, יפנה בעל הרישיון 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, ינחה אותו בעל רישיון 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 הרישיון</u>

14. לאחר הרישום הראשוני והקמת חשבון משתמש בבעל הרישיון, ההתחברות השוטפת של הלקוח מול בעל רישיון 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 למידע פיננסי מבחינת תקינות הבקשות וכמות הבקשות באופן שיהיה תואם לאופי השירות שביקש הלקוח.

18. בעל רישיון מחויב להזדהות באופן מקוון באמצעות סרטיפיקט ייעודי בכל פניה למערכת הממשק למידע פיננסי 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 על אירוע אבטחה חמור יעשה בפורטל המפתחים.

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 לפי סעיף 7 לחוק , יבוטל הסרטיפיקט של אותו בעל רישיון.

22. התלה יושב ראש הרשות רישיון באופן מיידי, לפי סמכותו בסעיף 7(ד) לחוק, 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, ידווח לרשות על הצורך בביטול הסרטיפיקט שלו.

25. בעל רישיון אינו רשאי לפנות למקור מידע באמצעות הסרטיפיקט שלו בבקשה לקבל מידע פיננסי באמצעות מערכת הממשק למידע פיננסי כל עוד הרישיון 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, 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.

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.

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. הממונה על אבטחת מידע והגנת סייבר שימונה לפי סעיף 30(ג) יפעל כדלקמן:

א. יכין נוהל אבטחת מידע.

ב. 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.

ג. יכין תוכנית לבקרה שוטפת אחר העמידה בדרישות החוק וההוראות מכוחו ובדרישות חוק הגנת הפרטיות ותקנותיו, יבצע אותה ויודיע על ממצאיו להנהלת בעל רישיון אחת לתקופה כפי שיקבע במדיניות.

ד. יעקוב אחר אופן יישום והטמעת מדיניות ונוהלי אבטחת מידע, המלצות סקרי אבטחת מידע והנחיות החוק הרלבנטיות.

ה. 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.

ו. 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.

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

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

ט. ינחה מקצועית את הארגון בנושאי אבטחת מידע והגנת הפרטיות.

י. יבחן באופן שוטף, את הליכי מחיקת המידע הפיננסי שבהחזקת בעל רישיון על פי ההוראות הקבועות בחוק, ובכלל זה האם אין המידע שנשמר במאגר רב מהנדרש לצורך עמידה במטרות המאגר ודרישות החוק 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.

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 בצע בעצמו את הפעילות המהותית הכרוכה במתן שירות מידע פיננסי.

35. על אף האמור בפרק זה, בעל רישיון לא יוכל להעביר את אחריותו לקיום כל חובותיו על פי החוק 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.

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 ידווח לרשות על אודות פעילותו, הן באופן תקופתי והן באופן שוטף, כקבוע בהוראות אלה.

57. כל מסמך או הצהרה שמגיש בעל הרישיון לרשות לפי פרק זה יוגש או יינתן על ידי נושא משרה בכירה בו המוסמך להגישו או לתתו ובאופן הקבוע בסעיף 3 לעיל.

<u>סימן ב' – דיווחים שנתיים</u>

58. בעל רישיון ידווח אחת לשנה ולא יאוחר מחודש מתום שנת הדיווח שלו, את הפרטים הבאים:

א. הכנסות החברה ממתן השירותים בישראל לשנת הדיווח.

ב. 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 בהתחשב בשיקולים המנויים בסעיף 8(ג) ; 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 לשיקולים המנויים בסעיף 8(ג).

ג. חוות דעת עדכנית של מבקר תוך הדגשת השינויים שחלו בעניינים המפורטים בסעיף 2(ו)(1) לעיל.

ד. מפת סיכונים עדכנית תוך הדגשת השינויים שחלו בעניינים המפורטים בסעיף 2(יב) לעיל.

ה. מצבת עדכנית של נושאי משרה בכירה בבעל הרישיון, בבעל השליטה בבעל הרישיון ונושאי משרה בכירה בבעל השליטה (במידה והוא תאגיד) ופרטיהם כמפורט בסעיף 2(ב).

<u>סימן ג' – דיווחים חודשיים</u>

59. בעל רישיון 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, 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 הרישיון לראשונה על קרות האירוע; לעניין זה, "נודע לבעל הרישיון 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 הרישיון, והיום שבו נודע לבעל הרישיון לראשונה על קרות האירוע המדווח.

62. בעל רישיון יעביר לרשות דיווח מיידי במקרים הבאים:

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

ב. כל 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. כל שינוי או עדכון בסוגי שירותי המידע הפיננסי הניתנים 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, 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 והנימוק שמסר לו לאי מתן הגישה למידע, וכן הודעה על הסרת מניעת הגישה שקיבל בעל רישיון ממקור מידע לפי סעיף 41(א)(3) לחוק.

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 תוגש כדיווח מיידי.

טו. מונה אדם לנושא משרה בכירה בבעל רישיון או בבעל שליטה, יובאו לגביו הפרטים המנויים בסעיף 2(ב) להוראה זו.

טז. מונה אדם לממונה אבטחת מידע או לממונה על ניהול הסיכונים בחברה, יובאו לגביו הפרטים המנויים בסעיף 2(ו)(2) או 31 בהתאמה להוראה זו.

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 הרישיון לראשונה על קרות האירוע.

פרק ט': תחילה

64. תחילתה של הוראה זו ביום פרסום הודעה על נתינתה ברשומות.

מועד פרסום ההוראה באתר הרשות: 15.3.2022