

הצעת הוראה לבעלי רישיון או אישור שירותי תשלום או ייזום בסיסי בעניין אמצעים טכנולוגיים ואבטחת מידע

עדכוני לקוחות

לאחרונה פורסמו להערות הציבור [הצעת כללי בקשת רישיון שירותי תשלום או שירות ייזום בסיסי](#) [1] של הרשות לניירות ערך ("הרשות"), [והצעת הוראה לבעלי רישיון או אישור שירותי תשלום או ייזום בסיסי בעניין אמצעים טכנולוגיים ואבטחת מידע \("ההוראה"\)](#).

ההוראה נועדה להסדיר את הדרישות שיחולו על בעלי רישיון מכוח חוק הסדרת העיסוק בשירותי תשלום וייזום תשלום, התשפ"ג – 2023 ("החוק") אשר יכנס לתוקף ביוני 2024, בעניין אמצעים טכנולוגיים, ניהול סיכונים טכנולוגיים מידע, אבטחת מידע, הגנת סייבר והמשכיות עסקית.

ההוראה המוצעת מתבססת הן על דרישות החוק והן על האסדרה האירופאית בעניין ניהול סיכונים טכנולוגיים מידע ואבטחת מידע שחלה על נותני שירותי תשלום או ייזום בסיסי.

טיוטת ההוראה עומדת על כך שפעילות שירותי תשלום וייזום בסיסי מתאפיינת בשימוש נרחב באמצעים אלקטרוניים ונעשית, לרוב, באופן מקוון, וכוללת בדרך כלל התקשרויות עם גופים שונים מהמגזר הפיננסי, כמו גם עם צדדים שלישיים. על כן, פעילות זו כוללת חשיפה לסיכונים טכנולוגיים מידע ואבטחת מידע, לרבות, חשיפה להתקפות סייבר. טיוטת ההוראה מחייבת את בעלי הרישיון לנהל את הסיכונים האמורים ולפעול לצמצומם.

לצורך כך, קובעת טיוטת ההוראה מודל הכולל שלושה מעגלי בקרה :

1. **מעגל הבקרה הראשון** כולל את בעלי התפקידים בחברה העוסקים בתחום טכנולוגיית המידע אשר אמונים על המערכות, התהליכים ופעילויות אבטחת המידע (כגון: יחידות טכנולוגיית המידע והתפעול).
2. **מעגל הבקרה השני** כולל את הממונה על אבטחת מידע והגנת סייבר.
3. **מעגל הבקרה השלישי** כולל מבקר חיצוני אשר יהיה אמון על ביצוע ביקורת עצמאית.

בנוסף, דירקטוריון בעל הרישיון נושא באחריות הכוללת בנושא סיכונים טכנולוגיים מידע וכחלק מאחריותו נדרש הדירקטוריון לאשר ולפקח אחר יישום דרישות ההוראה.

ההוראה המוצעת כוללת, בין היתר, דרישות בנושאים הבאים:

- ממשל תאגידי ודרישה לחלוקה ברורה של אחריות אצל בעל הרישיון, לרבות אחריות הדירקטוריון בנושא סיכונים טכנולוגיים מידע.
- גיבוש אסטרטגיית טכנולוגיית מידע בהלימה לאסטרטגיית העסקית הכוללת.

- חובת בעל רישיון לנהל ולהפחית את סיכוני טכנולוגיית המידע באמצעות ממונה אבטחת מידע עצמאי ולתחזק מיפוי עדכני של תהליכים עסקיים, תהליכים תומכים ונכסי מידע וסיווגם בהתבסס על שיקולי סודיות, אמינות וזמינות המידע. בהמשך לכך, על בעל רישיון להעריך את הסיכונים התפעוליים הקשורים לסיכוני טכנולוגיית מידע שמשפיעים עליו ולהחליט אילו אמצעים דרושים כדי לצמצם את הסיכונים שזוהו.
- יישום אמצעי אבטחת מידע אפקטיביים, לרבות הכנה ויישום של מדיניות אבטחת מידע, הטמעה ובדיקת אמצעי אבטחת מידע, והכנת תכנית הדרכות לכל עובדי בעל הרישיון וצדדים שלישיים.
- קביעת עקרונות לגבי ניהול פעולות טכנולוגיית מידע, ובכלל זה, יישום נוהלי תיעוד וניטור בעניין פעולות טכנולוגיית מידע חיוניות, תחזוקה ועדכון של רשימת נכסי טכנולוגיית מידע, ויישום של נהלים בעניין גיבוי ושחזור מידע.
- ניהול שינויים בתחום טכנולוגיית מידע, לרבות רכישה ופיתוח של מערכות מידע.
- ניהול המשכיות עסקית וגיבוי תכנית תגובה והתאוששות.
- ניהול יחסי בעל הרישיון והלקוחות, כולל דרישות לאפשר ללקוח להשבית פונקציות תשלום ספציפיות ומתן אפשרות, ללקוחות המעוניינים בכך, לקבל התראות לגבי ייזום עסקאות או ניסיונות כושלים לייזום עסקאות תשלום, וכן מתן תמיכה בנוגע לשאלות שעניינן אבטחת מידע והגנת הפרטיות.
- עמידה של בעל הרישיון בהוראות חוק הגנת הפרטיות, תשמ"א – 1981 והתקנות שחוקקו מכוחו. בהקשר זה, ההוראה כוללת דרישה כי תקשורת בעל רישיון מול כל גורם, המכילה מידע רגיש (כהגדרתו בחוק הגנת הפרטיות), תעשה בפרוטוקול סטנדרטי ובתעבורה מוצפנת על פי הטכנולוגיות העדכניות הקיימות בשוק. עוד נקבעו דרישות בעניין תהליך ניטור והגבלת הגישה למידע רגיש.

ההוראה קובעת כי בעל רישיון יקיים את ההוראה במלואה בשים לב למאפייניו הפרטניים (גודלו; המבנה הארגוני הפנימי; היקף, ומורכבת ומידת הסיכון המאפיינים את השירותים והמוצרים שבעל הרישיון נותן או מתכוון לתת). כמו כן, על בעל הרישיון לקחת בחשבון ולשקול לאמץ תקנים בין-לאומיים קיימים ושיטות עבודה מומלצות (best practice standards) בתחום טכנולוגיית מידע ואבטחת מידע למגזר הפיננסי.

ניתן להעביר הערות לטיטת ההוראה עד ליום 31.03.24, באמצעות כתובת הדוא"ל: seclaw@isa.gov.il.

משרדנו מלווה גופים פיננסיים שונים, ובכלל זאת נותני שירותי תשלום, בהיבטי הרגולציה השונים החלים על גופים פיננסיים בכלל ובתחום הסייבר והפרטיות בפרט. אנו מזמינים אתכם לפנות אלינו בכל שאלה ו/או התייעצות בנושא, ובפרט בראי כניסת החוק לתוקף ביוני 2024.

[1] להרחבה, ראו [עדכון הלקוחות](#) שלנו בנושא.

עדכון זה נועד לספק מידע כללי ותמציתי בלבד. הוא אינו מהווה ניתוח מלא או שלם של הסוגיות הנידונות, אינו מהווה חוות דעת משפטית או ייעוץ משפטי ואין להסתמך עליו.

אנשי קשר



אביטל חייטוביץ'
עורכת דין בכירה



עדו מלין
שותף



אסף הראל
שותף