מדריך לשיפור רמת אבטחת המידע במשרדי עורכי-דין[1]

לאחרונה זיהתה הרשות להגנת הפרטיות (להלן - **הרשות**) עלייה במספר אירועי אבטחת המידע ותקיפות סייבר אחרות הפוגעים בפרטיותם של תושבי מדינת ישראל[2] במגזר משרדי עורכי הדין. כידוע, משרדי עורכי הדין נושאים באחריות לאבטחת המידע במאגרים המנוהלים או מוחזקים בידיהם, בין אם הם בעל מאגר כמשמעותו בחוק הגנת הפרטיות, התשמ"א-1981 (להלן- **החוק**) ובין אם הם "מחזיק" במאגר כהגדרתו בחוק.[3] במסגרת הטיפול באירועים זוהו הפרות של החוק ושל תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 (להלן - **התקנות**) אשר מנוצלות באופן רוחבי על ידי תוקפים.

מטרתו של מסמך זה לסייע בשיפור רמת אבטחת המידע של משרדי עורכי-הדין ולוודא עמידתם בדרישות החוק והתקנות.

בנספח א' רוכזו מספר פעולות החשובות להעלאת רמת המוגנות והניתנות ליישום באופן פשוט ומידי.[4]

יובהר, כי במקרה של חשש לאירוע אבטחה חמור, כהגדרתו בתקנות, במשרדי עורכי-הדין, חלה חובה חוקית לדווח לרשות **באופן מידי**, באמצעות הטופס המקוון.[5]

---

[1] מדריך זה מתפרסם ככלי עזר למשרדי עורכי דין. האמור בו אינו ממצה את דרישות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז- 2017, ואינו פוטר את המשרדים מקיום כל הוראות חוק הגנת הפרטיות, התשמ"א- 1981 והתקנות שנקבעו מכוחו.

[2] בין התקיפות הנפוצות ביותר:
א DDOS -מתקפת מניעת שירות מבוזרת
ב Defacing - השחתת אתרים
ג Data Breach -דלף מידע

[3] "מחזיק לעניין מאגר מידע - מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש". הגדרה זו מתארת את החזקת המידע עבור אחרים, בעלי המאגר, אשר מבקשים להשתמש בשירותיו של המחזיק לשם אחסון המידע עבורם, או עיבודו עבורם בדרך אחרת. במרבית המקרים, משרד עורכי דין יהיה בעל מאגר המידע, למשל ביחס למידע על לקוחותיו היחידים, או על עובדי המשרד. אולם בנסיבות מסוימות ולגבי חלק מן המידע שהוא מחזיק במסגרת השירות המקצועי שהוא מספק, עשוי משרד עורכי הדין להיחשב כ"מחזיק" המאגר עבור לקוחותיו ; למשל ביחס לפרטי חייבים בגינם מספק המשרד שירותי גביה עבור לקוחותיו.

[4] למידע נוסף, ניתן לעיין בגילוי הדעת המקדים של ועדת האתיקה של לשכת עורכי הדין (את/1/22) מפברואר 2022, בדבר אבטחת המידע המצוי בידי עורכי דין
(https://www.israelbar.org.il/UpLoadFiles/ethics_committee_opinion_1-22_full.pdf)

[5] https://mojforms.justice.gov.il/mojaemprivacyprotectionauthority/databreachupdate.html

נספח א'

הנושא	פעולת המניעה
סוגי המידע ואופן שמירתו ואחסונו	לוודא שהמשרד מכיר את התהליכים הממוחשבים בהם נאסף ונשמר מידע על לקוחות ועובדים. יש למפות את מערכות המידע המעורבות בתהליכי איסוף המידע ושמירתו ואת אמצעי אבטחת המידע המגינים על מידע זה.
תוכנות ואפליקציות בשימוש המשרד	לוודא שכל התוכנות והאפליקציות מורשות ברישיון ומקבלות תמיכה טכנית ועדכונים שוטפים. במקרים בהם משתמש המשרד בתוכנות להן לא נדרש רישוי ו/או חינמיות יש לוודא כי גם הן נתמכות ומקבלות מענה אבטחתי מתאים, כגון קבלת עדכונים וטלאי אבטחה באופן סדיר.
אתר האינטרנט של המשרד	אם למשרד יש אתר שיש בו אזור אישי או אפשרות ללקוחות להשאיר פרטים, יש לוודא שהגורם במשרד שאמון על תחזוקת האתר מיישם את אמצעי אבטחת המידע הנדרשים (הגבלת גישה גאוגרפית, הגנת DOS ניטור והצפנה של תעבורת הרשת בגישה לאתר, לבסיסי הנתונים ולגיבוי) לרבות עדכונים וטלאי אבטחה שוטפים לסביבת האתר.
מערכות הגנה	להתקין מערכות הגנה מנוהלות כגון (EDR) לתחנות הקצה ולסביבות ענן ככל ויש, למטרת ביצוע סריקות תדירות לאיתור פעילות חריגה או הפעלת נוזקות ווירוסים.
מערכת ניטור	ככל והמשרד שכר שירותי ניטור קבוע כלשהם, יש לוודא כי קבצי התיעוד מכלל מערכות האבטחה מוגדרים לשמירה (וגיבוי) למשך 24 חודשים לפחות. בנוסף יש לוודא תקינות וזמינות מנגנון קבלת התראות בזמן אמת.
גיבוי ותיעוד	בחינה והתאמת הגדרות התיעוד (והגיבוי) של כלל מערכות האבטחה לרבות אלו המוטמעים מטעם מערכת ההפעלה. **המלצה!** שנו את הגדרות מיקום תיקיות ברירות המחדל של קבצי התיעוד לתיקיות מוסוות תחת שם גנרי עם בקרת גישה לתיקיות אלו ולברירת המחדל.
	יש לוודא כי נתוני התיעוד (לוגים) לכל המערכות כולל ממערכת הבקרה, נשמרים לתקופה של 24 חודשים.

מניעת גישה לא מורשית למידע	וידוא כי כל המידע הקיים במאגר/י המידע ומערכות המאגר מוצפן בשיטות הצפנה מקובלות ועדכניות.[6]
גיבוי קר	יש לבצע סריקת מערכות הגיבוי לבחינת תקינותן ואבטחתן. מומלץ להחזיק העתק גיבוי קר מחוץ למשרד ולבצע תרגילי שחזור מידע אחת לרבעון בכדי לוודא תקינות.
חיבור מאובטח מרחוק	הדקו את מדיניות החיבור מרחוק של עובדים או ספקים לממשקי הניהול כך שיוגדרו לכתובות IP מוגדרות מראש, בתעבורה מאובטחת ומוצפנת ב- VPN. הפעילו מנגנוני אימות דו-שלבי ותחת מדיניות סיסמאות מורכבות.
הרשאות	יש לנהל יומן מורשי גישה מתעדכן עם מדרג הרשאות מתאים לכל עובד על בסיס תפקידו ועם ההגדרות המינימליות ביותר הנחוצות לעבודתו. יש להקפיד במיוחד לנטר באופן קבוע ורציף חשבונות מנהלים או בעלי הרשאות רחבות וגבוהות.
סקר סיכונים	וידוא כי בוצע לאחרונה סקר סיכונים מקיף ועדכני למאגרי המידע ומערכותיהן.
מבדקי חדירות	וידוא כי בוצע לאחרונה מבדק חדירות אפליקטיבי ותשתיתי (רצוי שיותאם לתוצרי סקר הסיכונים).

[6] כאמור בתקנה 4(ג)(5) שקובעת, בין היתר, כי נוהל האבטחה צריך לכלול, התייחסות למנגנוני ההצפנה המקובלים להגנה על המידע השמור במאגר או במערכות המאגר;