

דו"ח פיקוח רחב

ממצאי הליך פיקוח הרחב בקרב מגזר חברות אחסון ועיבוד מאגרי מידע בישראל

חשוון תשפ"א אוקטובר 2020

אתגרים ומאפיינים ייחודיים של מגזר חברות אחסון ועיבוד מאגרי מידע בישראל

עמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו

- רמת עמידה גבוהה
- רמת עמידה בינונית/חלקית
- רמת עמידה נמוכה

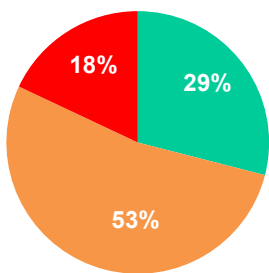


דרגות שירות שונות באמצעות שירותי SAAS – Software as a Service, PAAS - Platform as a Service IAAS - Infrastructure as a Service

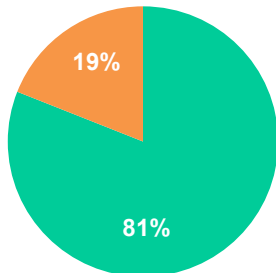
ניהול מידע של מספר לקוחות על אותה פלטפורמה, היקפי המידע, ומספרם הרב של האנשים עליהם מוחזק המידע, דורשים הקפדה מיוחדת על עמידה בהוראות החוק והתקנות.

החזקת המידע נעשית עבור אחרים, המהווים בעלים של המאגר ומבקשים להשתמש בשירותיו של המחזיק, כבעל היכולות הטכנולוגיות לאחסון ועיבוד המידע עבורם.

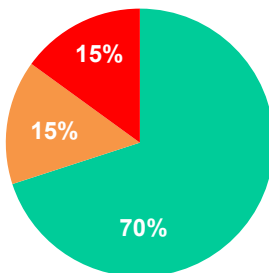
חברות המנהלות שירותי אחסון ועיבוד מאגרי מידע מחזיקות מאגרי מידע רבים הכוללים בין היתר מידע רגיש ומזוהה.



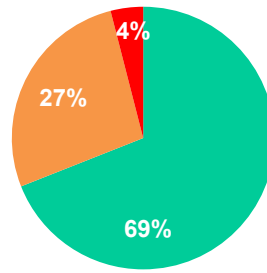
עיבוד מידע אישי במיקור חוץ



אבטחת מידע



ניהול מאגרי מידע



בקרה ארגונית וממשל תאגידי

עיקרי הנחיות לתיקון ליקויים

יש לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע מקום שנדרש כזה.

יש לבצע הדרכות לבעלי הרשאות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים.

יש לבצע ביקורת בנושא אבטחת מידע, סקר סיכונים ומבדק חדירות כנדרש בתקנות 5 ו-16 לתקנות אבטחת מידע.

יש לוודא קיום נהלי אבטחת מידע אשר כוללים את כל הנושאים המפורטים בתקנה 4 לתקנות, וכי נעשית בחינה של תוקפם מעת לעת כנדרש בתקנות.

יש להבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה אך ורק למי שהורשו לכך במפורש בהסכם בכתב בינם לבין בעליו של אותו מאגר.

על גופים המחזיקים ברשותם חמישה מאגרי מידע או יותר, למנות אדם בעל הכשרה מתאימה כממונה על אבטחת מידע, ולמסור לרשם מדי שנה רשימה של מאגרי המידע שברשותם.

יש לוודא שקיימת תכנית עבודה שנתית העומדת בדרישות התקנות, ולערך אחת ל-24 חודשים לפחות ביקורת פנימית או חיצונית בנושא אבטחת מידע על ידי גורם בעל הכשרה מתאימה שאינו ממונה האבטחה של המאגר, כדי לוודא עמידה בתקנות.

על הגופים המחזיקים בתקן ISO 27001 לפעול בהתאם להנחיית רשם מאגרי המידע 3/2018 – 'תחולת תקנות הגנת הפרטיות (אבטחת מידע) על ארגונים המוסמכים לתקן ISO/IEC 27001.

יש לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, וכן לוודא כי קיימת התאמה בין זהות מנהל המאגר במסמכי החברה, לבין הרשום אצל רשם מאגרי המידע.

על גופים המחזיקים ברשותם חמישה מאגרי מידע לפחות של בעלים שונים, למסור לרשם, מדי שנה, רשימה של מאגרי

המידע שברשותם, בציון שמות בעלי המאגרים, תצורה על כך שלגבי כל אחד מן המאגרים נקבעו הזכאים בגישה למאגר בהסכם בינו לבין הבעלים, ושמו של הממונה על אבטחת המידע.

בדיוור ישיר, בין אם עבור לקוחות ישירים של הגופים ובין אם כפלטפורמה למתן שירותי דיוור ישיר יש להקפיד על ציון הפרטים המנויים בסעיף 117 לחוק.

החובות החלות על בעל מאגר מידע יחולו גם על מנהל המאגר, ולמעט החובות הקבועות בתקנות 2 ו-15(א) – הן יחולו גם על מחזיק המאגר, בשינויים המחויבים ולפי העניין.

על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בה. יש לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, אשר יכלול את כל הוראות תקנה 15(א) לתקנות וכן התייחסות לחובותיו ואחריותו של הספק לרבות: דיווח אודות אירועי אבטחת מידע, מנגנוני אבטחת מידע, שמירת המידע לאחר סיום תקופת ההתקשרות וחובות צד שלישי בהעברת מידע לאחר.

יש לוודא כי כל צד שלישי אשר מספק שירותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.