

הנחיית רשם מאגרי המידע מס' 03/2018

תחולת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

על ארגונים המוסמכים לתקן ISO/IEC 27001

1. מכוח סמכותי בסעיף 20(ב) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017

"התקנות" אני מורה כי ארגונים שקיבלו הסמכה לתקן ISO/IEC 27001:2013(E)

"התקן" ומקיימים את הוראותיו לרבות את כל הבקורות הרלבנטיות המפורטות בנספח

A לתקן, באופן בו הן מפורשות ומפורטות בתקן ISO/IEC 27002:2013(E), יראו אותם

כמקיימים את הוראות התקנות במלואן ביחס למאגרים עליהם ניתנה ההסמכה לתקן

וכל עוד ההסמכה עומדת בתוקפה, אם ימלאו את כל הסעיפים והתנאים הבאים:

- תקנה 2 ;

- תקנה 3 ;

- תקנה 4 (א) – (ב), (ה) ;

- תקנה 5 (ב) – (ד) ;

- תקנה 9 (ב) (1) ;

- תקנה 10 (ד), (ה) ;

- תקנה 11 (ג), (ד) ;

- תקנה 12 ;

- תקנה 14 (ג) ;

- תקנה 18 (א) (2) ;

- תקנה 19 ;

הדרכות לעובדים לפי פריט 7.2.2. לנספח לתקן יקוימו בתדירות של לפחות אחת

לשנתיים ;

פריט 18.1.3 לנספח לתקן יקויים באופן בו הנתונים המפורטים בו ובפרשנותו

בתקן 27002 ישמרו למשך 24 חודשים ;

פריט 18.2 לנספח לתקן יקויים כך שהליכי הביקורת הנזכרים בו יבוצעו לכל

הפחות בתדירות של אחת ל – 24 חודשים.

2. תחילתה של ההוראה ביום תחילת התקנות והרשם עשוי לתקן את תנאיה מעת לעת,

בשים לב בין השאר לעדכונים ולשינויים בנוסח התקן.