אבטחת מידע

זבולון

2014

חוק הגנת הפרטיות

"האחריות לאבטחת מידע מוטלת על בעלי מאגר המידע, על המחזיקים בו או על מנהליו". הגופים המוזכרים בחוק זה, בין היתר הרשויות המקומיות, חייבים למנות ממונה על אבטחת מידע, אשר יופקד על אבטחת המידע במאגרים המוחזקים ברשותן.

הגדרות

- **מאגר מידע** מוגדר בחוק הגנת הפרטיות, כ: "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב".

- **"מידע"** מוגדר בחוק הגנת הפרטיות, כ: "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".

- **"מידע רגיש"** מוגדר: "נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו" וכל מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש.

"למעט - (1) אוסף לשימוש אישי שאינו למטרת עסק; או (2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר אפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף".

הסיכונים

- **פגיעה בפרטיות בשל עיבוד מידע שלא על פי הוראות החוק, בשל חשיפה למידע אישי או שימוש לא מורשה במידע אישי (שמנוהל על ידו), עלולה לגרום לחשיפה להליכי אכיפה אזרחים ואף לחיוב לתשלום פיצוי ללא הוכחת נזק, כן יתכנו הליכי אכיפה על ידי הרשם העלולים להסתיים במקרים מסוימים גם בהטלתה של אחריות פלילית.**

חובות הרשות

- לבחון את הצרכים, להגדיר ולאשר את מדיניות אבטחת המידע במועצה.
- לקבוע תדירות לבחינת המדיניות שנקבעה בתחום אבטחת המידע. ולבחון בהתאם את מצב אבטחת המידע במועצה.
- להקים ולהטמיע תהליך ניהול אבטחת מידע בארגון.
- לוודא שמטרות, יעדים ותוכניות אבטחת מידע מוגדרות וממומשות.
- לספק משאבים מספקים לפיתוח, הטמעה, תפעול ובקרה של אבטחת מידע בארגון.
- להגדיר תפקידים ותחומי אחריות באבטחת מידע.
- להגדיר דרכי הוצאת מידע ממוחשב מהמועצה (הדפסה, צריבה,e-mail, disk on key).
- להגדיר סיסמאות מורכבות בכניסה לרשת ונהלי החלפת סיסמאות בהתאם.
- נעילת מחשבים אישיים במשרדים לאחר פרק זמן ללא שימוש.
- הדרכת עובדים- העלאת רמת המודעות לאבטחת וניהול המידע בארגון.
- שיתוף העובדים בשמירה הפיזית והלוגית על המידע הרגיש.

מנהל אבטחת מידע

- סעיף 17 לחוק הגנת הפרטיות, קובע כי על המועצה למנות מנהל אבטחת מידע בעל כישורים וניסיון בתחום אבטחת מידע.
- יש להקפיד שהאחראי על אבטחת המידע לא יעסוק בתחומים ביצועיים ותפעוליים של מערכות המידע אשר עלולים לגרום לניגוד עניינים עם נושאי אבטחת מידע.

- בין תפקידיו - אחראי על יישום מדיניות אבטחת המידע.
- אחראי על בקרת אבטחת המידע בארגון.
- אחראי על החדרה והטמעה של פתרונות אבטחת מידע בכל הרמות (תשתית וייישומים, נהלי אבטחת מידע) בארגון.
- אחראי להנחות מקצועית את הארגון בהובלת נושאי אבטחת מידע.

מנהל מאגר מידע

מנהל המאגר אחראי לאבטחת המידע במאגר שעליו הופקד, ומוטל עליו: לנקוט צעדים בתחום ההגנה הפיסית; לקבוע סדרי ניהול המאגר וסדרי הגישה למידע שבו; לקבוע הוראות תפעול של המערכת תוך אבטחת המידע; לנקוט אמצעי אבטחה סבירים לשמירה על המידע ולשם תיקון ליקויים.

מחשבים מנותקי רשת (ניידים)

- *יש לקבוע נהלים לאבטחת המידע ולהגנת הפרטיות למחשבים מנותקי רשת; לרבות טלפונים חכמים וכוננים נתיקים, ובכלל זה יש לקבוע את דרכי ההגנה על המידע הנאגר במחשבים אלה, כדי לצמצם את הסיכון שבגנבת הציוד - חשיפת המידע השמור בו ונגישות לרשת.*

נהלים

- *על המועצה לקבוע סדרי ניהול וכן נוהלי עבודה בתחום אבטחת המידע והגנת הפרטיות.*
- *על המועצה להכין נהלים במגוון תחומים ובהם נושאים הקשורים לניהול, הכנסה, תפעול, תחזוקה, והוצאה של מידע בארגון, כולל מערכות המכילות זיכרון נייד כדוגמת מחשבים ניידים, טלפונים חכמים ועוד. נהלים אלה ייגזרו ממדיניות אבטחת המידע ומצרכי אבטחת המידע בארגון.*
- *יש לאשר את הנהלים עם כתיבתם או את השינויים המהותיים בהם ולפעול להטמעתם.*
- *יש להעביר את הנהלים תהליך של בדיקה ועדכון בהתאם לצורך, בעת שינוי משמעותי בסביבה הטכנולוגית או לאחר אירוע אבטחת מידע, ולכל הפחות אחת לתקופה שתקבע בהם.*

רישום מאגר מידע

- חוק הגנת הפרטיות קובע שכל מאגר מידע המקיים את אחד מתנאי חוק זה חייב ברישום אצל רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע.
- חובת תשלום אגרה תקופתית בגין מאגר מידע הרשום בפנקס.
- מאגרי המידע של המועצה שיש לרשמם כוללים, בין השאר, מאגרי מידע בתחומי השירות הפסיכולוגי החינוכי, הרווחה, הארנונה-גביה, אוכלוסין ועוד.

- ***נמצא כי מאגרי המידע של המועצה אינם רשומים כנדרש.***
- ***יש לבצע מיפוי של כל מאגרי המידע במועצה ולרשום אותם אצל הרשם בהתאם להוראות החוק.***

העברת מידע

- **חובה להקים בכל גוף ציבורי ועדה שתפקידה לדון בבקשות למסירת מידע שהגיש גוף ציבורי ולהחליט אם ובאיזו מידה להיעתר להן, וכן לבחון אם לאשר בקשות של אותו גוף ציבורי לקבלת מידע מגוף ציבורי אחר.**
- יש להסדיר את כל נושא העברת המידע ומתן מענה במועצה.
- יש לקבוע כללים ברורים לגבי מסירת מידע על ידי עובדים-מי מוסר, מה מוסרים וכו',
- יש להסדיר את כל מתן המענה לפניות כאלו ואחרות.
- יש לקחת בחשבון כי ישנו מידע אשר ישנן מגבלות על פי דין למוסרו. במצב הקיים, יתכנו מצבים בהם עובדים אינם מודעים למגבלות ואיסורים לגבי מסירת מידע.

אבטחת מידע עובדים

- יש לקבוע נהלים לגבי בדיקת עובדים המגויסים למועצה.
- יש לקבוע הנחיות ברורות ביחס למשרות רגישות, וכן קריטריונים לנגישות למידע.
- בחוזה הנחתם עם עובדים בתפקידים בהם ישנה חשיבות לסודיות יש לכלול הצהרת סודיות .
- לגבי עובדים להם יש נגישות למידע רגיש או למידע בעל סיכון גבוה, יש להגדיר פעולות נוספות המיועדות למנוע את זליגת המידע.
- יש לקבוע חסימת הרשאות הגישה למידע (בין אם למערכות מידע ובין אם לאמצעים פיזיים), לעובדים (כולל עובדים חיצוניים למועצה) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק.

מיקור חוץ

- בדיקה ראשונית לגבי עצם הוצאת הפעילות למיקור חוץ, בחירת הקבלן, תנאי ההתקשרות, אבטחת מידע ובקרה, קבלת עובדים ועוד.
- בעת שימוש במיקור חוץ החובות והאחריות המוטלים מכוח החוק על בעל מאגר מידע, מנהל מאגר והמחזיק בו ממשיכים לחול על כל אחד מהם כאילו הוא מבצע את הפעולות בעצמו.
- על המזמין להגדיר מפורשות את המטרות המותרות לשימוש ואת סוג בעלי התפקידים המועסקים על ידי הקבלן שיהיו מורשים בגישה למידע.
- לבצע מעקב ובקרה שוטפים על קיום הוראות החוק על ידי הקבלן.

עיקרי הממצאים

- **לא נקבעה מדיניות אבטחת מידע במועצה.**
- **לא מונה ממונה על אבטחת מידע (אחראי על ניהול אבטחת מידע).**
- **לא נקבעו נוהלי אבטחת מידע (לגבי מידע ממוחשב ושאינו).**
- **המועצה לא הקפידה על חובת הרישום של כלל מאגרי המידע שלה ברשות למשפט, טכנולוגיה ומידע (להלן רמו"ט), כנדרש בחוק.**
- **לא נקבעו מנהלים למאגרי המידע.**
- **לא נקבעו כללים לאבטחת המידע במחשבים מנותקי הרשת ובאמצעים הנתיקים האחרים שנעשה בהם שימוש.**
- **אין תכנית שיקום מאסון והמשכיות עסקית.**
- **אין הוראות ונהלים תקפים ומחייבים לאבטחת רשומות מכל הסוגים.**
- **נמצא כי אין הקפדה שמידע אישי הנוגע למצבם הכלכלי או האישי של תושבים יוחזק נעול. דבר זה אינו עולה בקנה אחד עם הדרישות הבסיסיות להגנה על מידע רגיש הנוגע לתושבים.**
- **בהסכמים בין המועצה לקבלני מיקור חוץ (מגע"ר, חברה לאוטומציה) המשתמשים/פועלים במאגרי המידע שלה, לא נקבעו כללים בדבר מורשה הגישה למאגרים (כפי שנדרש בחוק הגנת הפרטיות) והעובדים לא חתמו על הצהרת סודיות. <u>הערה זו רלוונטית לכל התקשרות עם קבלן מיקור חוץ, שעובד עבור המועצה ויש לו זיקה למידע שלה.</u>**
- **לא הוקמו ועדות למסירת מידע.**
- המועצה לא קיימה פעולות הדרכה והסברה לעובדים בתחום אבטחת המידע. רשומות על גבי אמצעים מגנטיים, אופטיים או על גבי ניירת.

המלצות

- לקיים תהליך למידה והטמעה של הכללים והחוקים בתחום אבטחת המידע, כתכנית עבודה רב שנתית בכל מחלקה בנפרד ובמועצה בכלל.
- להגדיר מדיניות אבטחת מידע במחלקות בפרט ובמועצה בכלל.
- למנות ממונה על אבטחת מידע כמתחייב מחוק הגנת הפרטיות.
- לרשום ולנהל את כל מאגרי המידע שברשותה (כנדרש בחוק).
- להקים ועדות להעברת מידע .
- להגדיר נהלים ייעודיים בנושא העברת מידע בין גופים ציבוריים כפי שנקבע בתקנות הגנת הפרטיות.

- לקיים פעולות בקרה בעניין אבטחת המידע והגנת הפרטיות, כדי לזהות פעולות חריגות או ניסיונות של גורמים בלתי מורשים לעשות פעולות כאלה, זאת ועוד בהתאם להוראות החוק ותוצאות סקר הסיכונים.