



משרד ראש הממשלה
ארכיון המדינה

אבן פינה

מבוא לניהול אלקטרוני של רשומות

גרסה 2.0

אפריל, 2021

תוכן עניינים

מבוא לניהול אלקטרוני של רשומות..... 3

1. מבוא 3

2. קהל יעד 4

3. תכולה..... שגיאה! הסימניה אינה מוגדרת.

4. סקירה כללית – ניהול אלקטרוני של רשומות 4

5. שלבים למימוש מערכת ל-”ניהול אלקטרוני של רשומות” 16

6. עקרונות למימוש מערכת ל-”ניהול ושימור אלקטרוני של רשומות” 19

7. ביבליוגרפיה 25

מבוא לניהול אלקטרוני של רשומות

1. מבוא

- 1.1 מסמך זה הינו מבוא הסוקר את הסוגיות המרכזיות הכלולות תחת נושא ניהול הרשומות האלקטרוניות ומתמקד בעיקר בנושא ניהול הרשומות בסביבה משרדית.
- 1.2 המסמך מתבסס על התקן הבין-לאומי בתחום ניהול הרשומות ועל ידע ופרסומים בתחום של ארגון ה-ICA וידע שנוצר במדינות אירופה ובעיקר בארכיון הבריטי.
- 1.3 מטרת המסמך להקנות מושגים עיקריים ולהציג בקצרה סוגיות, בעיות, תועלות, עקרונות ותהליכים עיקריים בניהול רשומות אלקטרוניות
- 1.4 נדגיש כי מסמך זה מתייחס לנושא ניהול הרשומות האלקטרוניות ולא לנושא ניהול המסמכים האלקטרוניים (ראה סעיף 4.6).

2. קהל יעד

- 2.1 גורמים האחראים על קביעת הנהלים והנחיות במשרדי הממשלה ובמוסדות המדינה (סמנכ"לים, מנהלי רשומות במשרד וכו').
- 2.2 מובילי פרויקט בארגונים לעיל בנושא ניהול רשומות או ניהול ידע או נושאים קשורים.
- 2.3 אנשי הטכנולוגיה ומערכות המידע במשרדים ובגופים לעיל האחראים על תכנון, בחינה מחדש, עיצוב ויישום של מערכות לניהול אלקטרוני של רשומות, בין אם המערכות הנבחרות הן תוכנות מדף ובין אם הן יישומים שמפותחים במיוחד לצורכי הארגון. בכלל זה הועדה המרכזית לענייני תקשוב במשרדי ממשלה ומנמ"רים.
- 2.4 גורמים האחראים על קביעת סטנדרטים ולקהילת ניהול הרשומות בכלל.
- 2.5 ארכיונאים העוסקים בניהול רשומות.
- 2.6 יועצים וספקי תוכנה ומוצרים בתחום ניהול אלקטרוני של רשומות וניהול תוכן (ECM).

3. תכולת הנוהל

- 3.1 סקירה כללית – ניהול אלקטרוני של רשומות: מהי רשומה, מהי רשומה אלקטרונית, מהו ניהול רשומות, תהליכי ניהול רשומות במשרד, מאפיינים, הנעשה בעולם, המצב בישראל וכו'.
- 3.2 שלבים למימוש מערכת ל- "ניהול אלקטרוני של רשומות"- מדיניות לפיתוח מערכות "ניהול אלקטרוני של רשומות" בארגון.
- 3.3 עקרונות למימוש מערכת ל- "ניהול ושימור אלקטרוני של רשומות"- דרישות ממערכת לניהול אלקטרוני של רשומות - עקרונות, תהליכים לזיהוי וניהול רשומות.

4. סקירה כללית – ניהול אלקטרוני של רשומות

משרדי הממשלה ומוסדות המדינה השונים, בארץ ובעולם מייצרים ומטפלים במידע רב שיש לארגנו ולהפיצו, אך מתקשים להתמודד עם כמויות גדולות של מידע.

ניתן להתמודד עם בעיית הטיפול במידע ע"י שימוש במערכת לניהול אלקטרוני של רשומות (ראה להלן הגדרה בסעיף 4.3) המאפשרת לשמור מידע מהימן ונגיש הנדרש לארגון. הדברים עולים מפרסומים ותקנים בתחום מן העולם הרחב.

נציין כי לא כל המידע בארגון הופך לרשומה (לדוגמה מידע אישי וטיוטות ראשוניות – על-פי-רוב לא ייחשבו "רשומה"), אלא רק כאשר המידע נדרש לארגון ומשמש כעדות לפעילות.

4.1 מהי רשומה?

רשומה (רשומה ארכיונית) הינה מידע רשום, ללא קשר לפורמט או למצע עליו הוא מאוחסן, שנוצר, התקבל, נשמר, על ידי תאגיד או אנשים במהלך ביצוע פעילות משפטית, מנהלית או עסקית, ומשמש כעדות ומידע על פעילות התאגיד או האנשים.

4.2 מהו מסמך אלקטרוני?

מידע המאוחסן על מצע מגנטי כדוגמת מסמך שנכתב במעבד תמלילים, גיליון אלקטרוני, דואר אלקטרוני, גרפים, תמונות, מסמכי מולטימדיה או סוגים נוספים של מסמכים משרדיים.

4.3 מהי רשומה אלקטרונית?

מידע רשום המאוחסן על מצע מגנטי שהוצהר כרשומה ארגונית ואין יותר אפשרות לשנותו אלא בתנאים מבוקרים. בנוסף מתבצעים עליו תהליכי בקרה המבטיחים את המקוריות (אותנטיות) שלו לאורך זמן. הרשומה האלקטרונית לעיתים מקורה בחומר שנוצר בסביבה אלקטרונית ונועד למלא את כל "תפקודיו" בסביבה אלקטרונית, ולעיתים מקורה בחומר שערב דיגיטיזציה ממדיית המקור (נייר, קלטת וכו') למדיה דיגיטאלית.

רשומה אלקטרונית יכולה לכלול פורמטים כגון מסמכים, תמונות, הודעות דואר אלקטרוני, קטעי שמע, קטעים אור-קוליים וכו'.

הרשומה האלקטרונית כוללת מטה דאטה (להרחבה בנושא ראה מסמך "ניהול מטה דאטה"- אפ-005) המחזיק מידע על היווצרותה ועל תהליכים שונים "שעברו" עליה.

אין הכוונה במונח רשומה אלקטרונית למונח המשמש בטכנולוגית המידע לתאר את הפריטים היוצרים יחד קובץ או טבלה. **נדגיש כי המטה דאטה הינו חלק בלתי נפרד מהרשומה וללא מטה דאטה אין זכות קיום לרשומה.**

4.4 מהי רשומה אלקטרונית מסורתית?

רשומה אלקטרונית מסורתית הינה רשומה אלקטרונית עצמאית המחזיקה מטה-דאטה ומפנה לחומר המתויק באופן פיזי ולא באופן אלקטרוני, כגון מדף המכיל קלטות אור קוליות או תיקים המכילים מסמכי נייר ועוד. מערכות לניהול אלקטרוני של רשומות תומכות בניהול משולב של רשומות מסורתיות (פיזיות) ורשומות אלקטרוניות בתיק אחד.

4.5 מהו ניהול אלקטרוני של רשומות?

ניהול אלקטרוני של רשומות הינו מימוש שיטתי של כלל הפעולות על רשומות אלקטרוניות בארגון: יצירה, הערכה, סיווג, תחזוקה, הנגשה, איחזור, ביעור ו/או העברה לארכוב. הניהול כולל את כל הפעולות הנדרשות כדי לשמור על שלמות, מהימנות, מקוריות, וההקשר שבו נוצרו הרשומות ושימושן בארגון. כל זה כדי לשמור את הרשומות ולהפוך את התוכן הגלום בהן לזמין ותומך בפעילות השוטפת, המנהלית והמשפטית של הארגון.

מערכות לניהול אלקטרוני של רשומות תומכות בניהול של מסמכים ורשומות אלקטרוניות.

ניהול אלקטרוני של רשומות כולל בתוכו גם ניהול של רשומות אלקטרוניות וגם ניהול רשומות אלקטרוניות מסורתיות (פיזיות) המחזיקות מטה-דאטה המפנה לחומרים שאינם מאוחסנים על מצע דיגיטאלי, כדוגמת מסמך נייר, קלטת אודיו קולית ועוד.

כפי שהודגש במבוא, השימוש בביטוי ניהול אלקטרוני של רשומות או ניהול רשומות אלקטרוניות במסמך זה ובמסמכים אחרים שיופצו במסגרת פרויקט "אבן פינה" מתייחס לאותה סוגיה אלא אם צוין במפורש אחרת.

4.6 מהו ההבדל בין ניהול אלקטרוני של מסמכים לבין ניהול אלקטרוני של רשומות?

א. מערכות לניהול מסמכים: מהוות אמצעי לקליטה, אחסון, ניהול ושיתוף מסמכים ומאפשרות גישה קלה למסמך. מערכות אלה אינן מתייחסות לכלל ההיבטים המשפטיים, ההנחיות והתקנות בנושא. ולמסמכים השמורים בה אין ערך של מקור.

ב. מערכות לניהול רשומות: מיועדות לספק לארגון עדות מהימנה על פעילויות, מדיניות, החלטות, נהלים, ומטרות הארגון, כאשר התוכן נדרש לארגון ומשמש כעדות לפעילותו. בנוסף לכך מערכות אלה מספקות מידע בהיר ומנחה לגבי מה נדרש לשמור ומה אפשר לבער. מערכות אלה גם מאפשרות לנהל גם מסמכים וגם רשומות אלקטרוניות.

4.7 הבדלים עיקריים בין רשומות נייר לרשומות אלקטרוניות

מחזור החיים, התפקיד והמטרות של רשומות הנייר והרשומות האלקטרוניות הינם זהים. הן רשומות הנייר והן הרשומות האלקטרוניות מרכיבות את הזיכרון הארגוני המתעד את הפעולות בארגון.

רשומות הנייר עדיין הינן האמצעי השכיח לשמירת מידע. סביר להניח שבעתיד נשמור פחות מידע על רשומות נייר וננהל אותו כרשומות אלקטרוניות.

עיקר השוני בא לידי ביטוי באופן ניהול הרשומות הנובע מהשוני במצע עליו הן נמצאות:

4.7.1 רשומות אלקטרוניות שונות מהותית מעצם טבען מרשומות מסורתיות (פיזיות). ברשומות מסורתיות, כמו נייר, מוטבע התוכן על מצע פיזי והופך להיות חלק ממנו. כתוצאה מכך קשה לשנותו והמצע נשמר לעתים קרובות זמן רב.

4.7.2 רשומות אלקטרוניות, מעצם טיבן, הן אוסף של אותות חשמליים (מגנטיים) המאוחסנים על מצע פיזי (תקליטור, כונן קשיח). הרשומות האלקטרוניות מצד אחד אינן עומדות בפני עצמן (במנותק ממצע פיזי כלשהו) ויחד עם זה יכולות להתקיים בסביבות מיחשוב שונות מבלי לשנות את זהותן, תוכןן, עיצובן (פונטים, צבעים, דגשים שונים) ותכולתן.

4.7.3 בשל העובדה שלרשומות אלקטרוניות ישנם מאפיינים מיוחדים, נדרשים מספר אמצעים טכנולוגיים על מנת להציג את הרשומה (תוכנת הפעלה, יישום, חומרה, צג מחשב, מערכת שמע).

4.7.4 רשומות אלקטרוניות לעומת רשומות מסורתיות (דוגמת נייר) רגישות מאוד לשינויים טכנולוגיים. חומר השמור על מצע מגנטי כלשהו ובפורמט כלשהו, הופך בחלוף מספר שנים לבלתי ניתן לקריאה ולשימוש, וכתוצאה מכך הופך לחסר ערך.

4.7.5 שינויים בתוכן רשומות אלקטרוניות עשויים להתרחש מסיבות רבות, בין אם כתוצאה מתקלות טכניות ובין אם כתוצאה מפעולה של המשתמש בהן. גם שינויים בפורמט עלולים לגרום לשינויים בתוכן הרשומה. לכן, רשומות אלקטרוניות פגיעות ונתונות לשינויים יותר מאשר רשומות נייר (ראה סעיף **4.14** להלן), ועל כן נדרש לנהל אותן באופן קפדני ביותר, תחת תהליכי מעקב ובקרה ואבטחת מידע.

4.7.6 בדרך כלל כאשר יש רשומות נייר, ההקשר בין הרשומות והתוכן הנמצא על הנייר בהיר. פעולת התיוק של רשומות הנייר בתיק הפיזי יוצרת את ההקשר של הרשומה עם הפעולה שיצרה אותה ועם שאר הרשומות בתיק. לעומת זאת, על מנת להציג את התוכן ברשומות אלקטרוניות ואת ההקשר שלהן, נדרשים אמצעים טכנולוגיים שונים. הדברים אמורים גם לגבי הצגת הקשר לפעולה

שיצרה את הרשומה וגם לגבי הצגת הקשר שבין הרשומה לרשומות אחרות

4.7.7 מטה דאטה – ה"מטה דאטה", כפי שמוגדר בהמשך, קיים גם ברשומות הנייר אולם הוא הופך לקריטי ברשומות אלקטרוניות. המטה דאטה הינו האמצעי המרכזי הקושר את הרשומה להקשר שלה, לפעולה שיצרה אותה ולרשומות קשורות אחרות ומחזיק מידע טכנולוגי על הרשומה האלקטרונית, ומשמר אותה לאורך זמן.

מטה דאטה הינו חלק בלתי נפרד מהרשומה וללא מטה דאטה אין זכות קיום לרשומה (הרשומה חסרת משמעות).

4.7.8 מערכות טכנולוגיות מאפשרות לשלוט באופן יעיל יותר בגישה לרשומות לעומת מערכות מסורתיות. האמצעים הטכנולוגיים מאפשרים לנעול, למנוע, להגביל שימוש במידע לגורמים מורשים.

4.7.9 לאור האמור לעיל, במקרים שבהם תוכן המסמך האלקטרוני הוא בעל חשיבות לארגון ועשוי לשמש כעדות לפעילות הארגון, המלצת ארכיון המדינה היא להפוך את המסמך האלקטרוני לרשומה, מוקדם ככל האפשר בחיי המסמך.

4.8 מדוע רשומות נוצרות?

רשומה נוצרת על ידי ארגון כאשר התוכן נדרש לארגון ומשמש כעדות לפעילותו, לרוב בנסיבות הבאות או כתוצאה מאחת או יותר מן הסיבות האלו:

4.8.1 אירוע, החלטה או פעולה - בעלי חשיבות ארגונית, משפטית, מחקרית או היסטורית.

4.8.2 עמידה בחוקים, תקנות ורגולציות רלוונטיות לארגון.

4.8.3 מעקב ובקרה אחר החלטות, פעולות ופרויקטים בעלי חשיבות ארגונית, משפטית, מחקרית או היסטורית.

4.8.4 ביצוע פעולה כעדות לאופן שבו נעשתה.

4.9 מתי רשומה אלקטרונית נוצרת (מתי מסמך הופך לרשומה)?

רשומה אלקטרונית יכולה להיווצר בשלבים שונים במהלך עבודת הארגון על פי החלטת הארגון. כאשר ארגון משתמש במערכת ממוחשבת לניהול רשומות הוא יכול להחליט על יצירת רשומה אלקטרונית באחד משני המצבים העיקריים האלה:

4.9.1 מסמכים אלקטרוניים מוכרזים כרשומות אלקטרוניות (ראה סעיף 4.13 להלן) פרק זמן מסוים לאחר היווצרותם על פי החלטת הארגון, לרוב כאשר נוצר הצורך לנהל את התוכן באופן מבוקר ומוגן משינויים. הדברים אמורים גם כאשר במשרד מנהלים מסמכים אלקטרוניים ורשומות אלקטרוניות במערכת אחת וגם כאשר מנהלים אותם בשתי מערכות נפרדות.

4.9.2 בהתאם להחלטה ארגונית שכל המסמכים אלקטרוניים הנוצרים במערכת מסוימת הופכים מיד ברגע היווצרותם לרשומות.

4.9.3 בהמרת חומר ארכיוני פיסי לדיגיטלי ע"י סריקה וניהולן במערכת ממוחשבת לניהול רשומות

4.10 מהי רשומה נאותה?

ניהול תקין של רשומות, המאפשר לספק עדות ומידע על פעילות תאגיד או אנשים, מחייב שהרשומה תהיה:

4.10.1 **מהימנה (Reliability)** – ניתן לבטוח ברשומה שהיא אמינה, מדויקת ומייצגת בצורה נאמנה את פעילויות הארגון, שבעקבותיהם נוצרה הרשומה. ניתן להסתמך עליה לשם ביצוע פעולות עוקבות.

4.10.2 **מקורית (Authenticity)** – הגנה על הרשומה (פרטי התוכן, היוצר/השולח, ההקשר, זמן היצירה וכו') מפני שינויים לא מורשים, כך שתישמר כפי שהייתה בעת הכרזתה כרשומה ותמשיך ותשמש כעדות לפעילות שיצרה אותה. כל שינוי ברשומה מתועד באמצעות כלי מעקב ובקרה.

4.10.3 **שלמה (Integrity)** – שמירת כל המידע המבטא את פעילות הארגון, בהתאם לדרישות הארגון. לדוגמא: מסר דואר אלקטרוני המכיל תוכן וקובץ מצורף, מספר גרסאות של מסמך, מסמכים מקושרים וכו'.

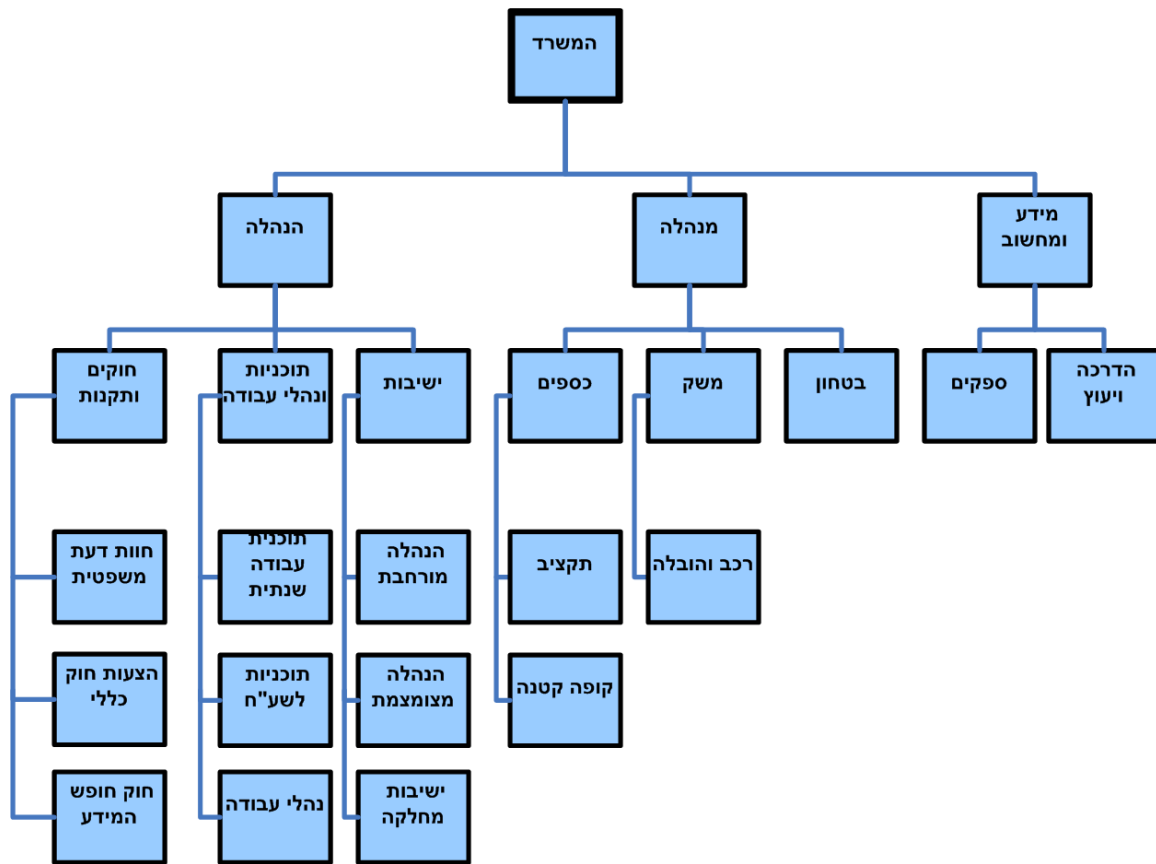
4.10.4 **נגישה (Useability)** – ניתן לאתר הרשומה ולגשת אליה ע"י שימוש בתוכנות ובחומרה סטנדרטיים (כלים שאינם יחודיים למערך המחשוב בארגון מסוים) ולהציג את תוכן הרשומה בהתאם לדרישות הארגון.

4.10.5 **הקשר** – בכדי שניתן יהיה להבין את משמעות הרשומה, נדרש לשמור את ההקשר בין הרשומות לפעולות הארגון שיצרו אותן, וכן את הקשרים בין

הרשומות, קרי: מי יצר את הרשומה, מתי נוצרה, באיזה תהליך היא נוצרה וכו'.

רשומה יכולה להיות מורכבת ממספר פריטי תוכן, שיחד יוצרים רשומה שלמה אחת, כאשר ללא אחד המרכיבים משמעות הרשומה עלולה להיות מוטעית או לא מובנת. לדוגמא: מסר דואר אלקטרוני יהיה מובן רק כאשר הרשומה מכילה את צרופותיו. דוגמא נוספת: מסמך שמכיל קיצור דרך למסמך אחר אשר מכיל תוכן חיוני להבנת המשמעות הכוללת.

4.11 אלו ישויות / מרכיבים עיקריים במערכת מחייבים ניהול מטה דאטה?



4.11.1 **ענף תיוק (class)** - ענפים בעץ התיוק המבטאים את הנושאים הראשיים בהם עוסק הארגון ו/או הפונקציות הארגוניות הראשיות (בהתאם למבנה המשרד ופעילותו). לכל ענף תיוק נידרש להגדיר שדות מטה דאטה, כדוגמת: שם הענף, תאריך יצירה, שם היוצר וכיו"ב.

לרוב תחת כל ענף תיוק יוגדרו תיקים.

4.11.2 **תיק (folder)** – תחת כל ענף יוגדרו תיקים המתארים את ההקשר, הנושא או הפונקציה שמייצג התיק. לכל תיק נידרש להגדיר שדות מטה דאטה, כדוגמת: שם הענף, תאריך יצירה, שם היוצר וכיו"ב

התיק יורש את רכיבי המטה דאטה מהרמה ההיררכית מעליו, בתוספת לרכיבי מטה דאטה הייחודיים לתיק.

4.11.3 רשומה (record) - ראו הגדרה בסעיפים 4.3 ו-4.4.

לכל רשומה נידרש להגדיר רכיבי מטה דאטה הכוללים מידע על יצירת הרשומה, תוכן הפעילות/האירוע היוצרים, האנשים המעורבים ביצירתה. בנוסף, המטה דאטה יכלול מידע טכני על הרשומה.

הרשומה יורשת את רכיבי המטה דאטה מהרמה ההיררכית מעליה, ומהגדרות מטה דאטה לסוג הרשומה ומהגדרות מטה דאטה לסוג התהליך העסקי שיוצר אותה.

4.11.4 מסמך (document) - ראו הגדרה בסעיף 4.2.

לכל מסמך נידרש להגדיר רכיבי מטה דאטה הכוללים מידע על יצירת המסמך, תוכן הפעילות/ האירוע היוצרים, האנשים המעורבים ביצירתו. בנוסף, המטה דאטה יכלול מידע טכני על המסמך.

המסמך יורש את רכיבי המטה דאטה מהרמה ההיררכית מעליו, ואת הגדרות המטה דאטה לסוג המסמך והגדרות המטה דאטה לסוג התהליך העסקי שיוצר אותו.

4.12 תועלות מניהול תקין של רשומות

ניהול נכון של רשומות במערכות מחשב הינו בסיס טוב לתפקוד הארגון, מכיוון שהוא תומך בפעילות הארגון ומספק בסיס למתן שירות טוב.

4.12.1 יעילות – הרשומה הינה חלק מהזיכרון הארגוני.

ניהול רשומות מאפשר הפיכת התוכן לזמין במהירות, כשנדרש לקבלת החלטות ולפעילות שוטפת. כמו כן שימוש בכלים לסילוק/ביעור של רשומות לא פעילות לפי תקופות שמירה מאפשר להתמקד בעיקר.

4.12.2 אחריות – יצירת רשומה שלמה ומוסמכת מאפשרת להציג ולהדגים את אחריות הארגון ופעילותו.

4.12.3 תאימות – הרשומה נגישה, מובנת ומאוחסנת בפורמט מתאים למשתמשים ברשומה.

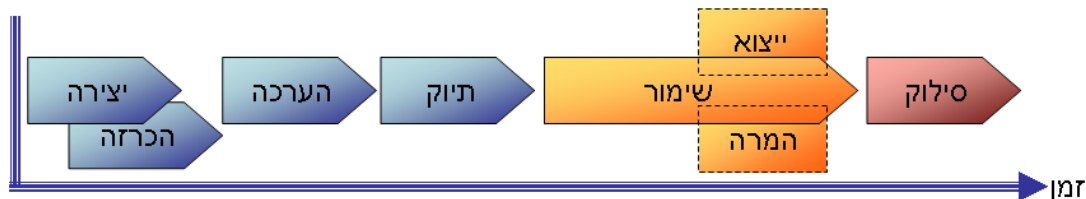
4.12.4 הקטנת סיכונים שעלולים לנבוע מתקלות, פעולות בזדון או בשוגג או ביעור שלא בהתאם לתקופות השמירה של רשומות, דהיינו, פעולות שעלולות לגרום לאובדן רשומות.

ומניעת גישה לא מורשית לרשומות ובכך להבטיח שמירה של התוכן מסיבות מסחריות, ביטחוניות, צנעת הפרט וכו'.

4.12.5 **נגישות** - הרשומה נגישה בו זמנית למספר רב של אנשים, ניתן לאתרה עפ"י קריטריונים שונים לגישה.

4.13 תהליכי ניהול הרשומה

מקובל להציג את התהליכים העוברים על הרשומה בארגון במחזור חיים המתואר להלן.



4.13.1 **יצירה** - לכידת העדויות לפעילות הארגון לתוך מסמך או לתוך רשומה ולכידת מטה דאטה רלוונטי, בדרך כלל באמצעות יישומי משרד תקניים ו/או לכידת מסמך אלקטרוני אשר מאוחסן כקובץ. בהתאם לסטנדרטים ולנהלים בארגון.

4.13.2 **הכרזה** - חתימת (נעילת) המסמך (אין הכוונה לחתימה דיגיטלית) באופן שלא מאפשר לשנותו (תוכן, מטה דאטה וכו'). שינוי המתבצע לאחר ההכרזה יתועד ברשומה חדשה או בגרסאות נוספות של אותה רשומה.

4.13.3 **הערכה** - הערכת משך חיי הרשומה קרוב ככל הניתן לזמן היווצרותה.

4.13.4 **תיוק** - תיוק הרשומות עפ"י מפתח תיוק כלל ארגוני, המשקף מבנה היררכי של הפונקציות והפעולות הארגוניות.

4.13.5 **שמירה** - שמירת הרשומה לאורך התקופה המתחייבת עפ"י התקנות¹ ובהתאם לדרישות המשרד, תוך שמירה על מקוריות ומהימנות הרשומה.

4.13.6 **אחזור / נגישות** - יכולת אחזור של הרשומה בקלות והיכולת ל"פתוח" אותה ולעיין בתוכנה ובתוכן המטה דאטה הצמוד.

4.13.7 **סילוק** - מחיקה מבוקרת של הרשומות בתום תקופת השמירה שנקבעה להן.

¹ תקנות הארכיונים (ביעור חומר ארכיוני במוסדות המדינה וברשויות המקומיות), התשמ"ו – 1986, (להלן במסמך זה – תקנות הביעור), או בהנחיות.

בין אם ע"י העברתן לארכוב (במערך מחשוב אחר של המשרד או בארכיון המדינה) ובין אם ע"י ביעור ללא יכולת שחזור. לעיתים דורשים ממערכת לניהול רשומות לשמור עדות על כך שהייתה רשומה וסולקה/בוערה.

4.13.8 **המרה** - העברת הרשומות מפורמט אחד לאחר, כמתחייב משינויים טכנולוגיים.

4.13.9 **יצוא** - העברת רשומות לארכיון המדינה, מגנזה, ארכוב וכו'. דהיינו, העברת הרשומות והמטא דאטה שלהן בפורמט מתאים להעברה, יחד עם כל התיעוד הדרוש על הרשומות.

בניית עץ מידע המתאים למשרד, תיוק תקין, ושימוש נכון במטה דאטה (ראה סעיף 6.2.1 להלן) יאפשרו למשרד לבצע חיפוש ממוקד, נוח ויעיל. ככל שכמות המידע שנוצר במשרד גדלה, התיוק והמטה דאטה הופכים קריטיים לניהול המידע בארגון.

4.14 סיכונים ובעיות

4.14.1 שבירות הרשומה האלקטרונית.

4.14.1.1 המצע (המדיום) אינו חלק אינטגרלי מהרשומה.

4.14.1.2 נדרשים מספר אמצעים על מנת להציג את הרשומה (תוכנת הפעלה, יישום, חומרה, צג מחשב, מערכת שמע).

4.14.1.3 מושפעת משינויים טכנולוגיים מהירים: אורך חיי האמצעים הטכנולוגיים השונים המשרתים מערכת לניהול אלקטרוני של רשומות הינו קצר (כ- 3 שנים).

4.14.1.4 לדוגמא פתיחה של מסמך שנערך במעבד התמלילים "אינשטיין" (מעבד תמלילים שהיה מקובל בארץ בסוף המאה ה-20) תדרוש את התוכנה המיושנת אינשטיין ולעיתים גם מחשב ישן שיוכל להפעיל אותה.

4.14.2 רגישות לשינויים בתוכן, פורמט.

כאשר המידע אינו מאובטח ומהימן מבחינה מסחרית, ביטחונית, צנעת הפרט, הדבר עלול להשפיע על המידה בה ניתן לבטוח בשלמות ובאמינות הרשומה.

4.14.3 כאשר הקשר של הרשומה לפעולה שיצרה אותה, או הקשר בין הרשומות אינו מובן, המשמעות עלולה להיות מוטעית או לא מובנת ועלולה להשפיע על תהליך קבלת החלטות של הגופים הממשלתיים ועל המענה לפניות אזרחים.

נזכיר ונדגיש כי רשומה יכולה להיות מורכבת ממספר רכיבים אלקטרוניים שיחד יוצרים את הרשומה. לדוגמה דואר אלקטרוני אליו מצורף מסמך.

4.14.4 כאשר המידע אינו זמין במהירות הנדרשת לצורך קבלת החלטות ולפעילות השוטפת, עלול הדבר להשפיע על תהליך קבלת החלטות של הגופים הממשלתיים ועל המענה לפניות אזרחים.

4.14.5 נדגיש כי מידע היסטורי שאין דרישה חוקית ו/או ארגונית ו/או מחקרית לשמרו וממשיך להתקיים - מונע התמקדות בעיקר.

4.14.6 השינויים הטכנולוגיים הדינאמיים וההיקף הגדל והולך של יצירה אלקטרונית של רשומות במוסדות המדינה מחייבים בחינה מעת לעת של נוהלי הארגון והתאמתם לשינויים.

4.14.7 כתוצאה משידרוג טכנולוגיות עלול להיווצר שיבוש במסמכי העבר.

4.15 שימור אלקטרוני של רשומות

בעולם בו הטכנולוגיות והפורמטים משתנים במהירות, על הארגונים ובפרט על הגופים המופקדים על ניהול רשומות בארגונים וארכובן, להבטיח שרשומה תהיה "זהה", ככל הניתן למקור גם בחלוף מספר שנים, תהיה נגישה, ותשמר המקוריות שלה, כאשר המצע המגנטי מתיישן/מתבלה, מערכות ההפעלה, תוכנת ה-office והתוכנות ליצירה ולעיבוד של רשומות לבטח משתנות מספר פעמים.

פעולת השימור מחייבת תכנון, ניהול וניטור שוטפים לאורך זמן והיא כוללת שני היבטים:

4.15.1 תחזוקה שוטפת של אמצעי אחסון מוגנים וביצוע פעולות לשמירת שלמות הרשומות:

4.15.1.1 בחירת אמצעי אחסון מוגנים, אמינים בעלי אורך חיים ארוך.

4.15.1.2 ניהול אמצעי האחסון: ניטור ורענון והחלפת המצע המגנטי, לשם מזעור תקלות ותהליכי בלאי תוך הימנעות משיבושים ברשומות.

4.15.1.3 שדרוג הדרגתי של אמצעי האחסון הנובעים מתכנון ובעיות ביצועים תוך וידוא מניעה של שיבושים ברשומות.

4.15.1.4 ביצוע פעולות והגדרות בתחום האבטחה, הדחיסה או כל פעולות תחזוקה אחרת בתשתיות המיחשוב, ללא פגיעה ברשומות וללא פגיעה ביכולת לייצא אותן או להמיר אותן לפורמטים עדכניים בצורה תקינה.

4.15.1.5 יכולת הפקת דוחות: ניטור אמצעי האחסון, בדיקות שלמות,

ביצועים.

4.15.2 שימור תוכן הרשומה והמטה דאטה לאורך זמן בהתאם לצורך.

השימור מחייב:

4.15.2.1 בחירת סוגי פורמט יציבים לאורך זמן. הדברים אמורים הן לפורמטים לשימוש שוטף והן לפורמטים לשימור.

4.15.2.2 זיהוי סוגי הפורמט המשמשים בארגון ומאפייניהם והתאמתם לסוגי הפורמט המחייבים בארגון.

4.15.2.3 פיתוח תוכנית שימור, הכוללת מעקב אחר שינויים המתחוללים בעולם בסוגי הפורמטים המקובלים כסטנדרטיים ורלוונטיים לארגון, כדי שניתן יהיה לבצע פעולות שימור בחלוף הזמן.

4.15.2.4 המרה של תוכן הרשומות והמטה דאטה לפורמט חדש, כדי לשמור על נגישות לרשומה באמצעות טכנולוגיה סטנדרטית מתעדכנת. כל זאת תוך מניעת שיבוש רשומות העבר ושמירה על ההקשר, שלמות, מקוריות, מהימנות ושימושיות הרשומות.

4.15.3 מקובל להבחין בין שתי תקופות שימור טכנולוגי של חומר אלקטרוני:

4.15.3.1 שימור קצר טווח עד חמש שנים.

4.15.3.2 שימור לטווח ארוך מ – 5 שנים ועד לצמיתות. לדוגמה תיקי פרט שיש לשמורם ל - 75 שנה או 100 שנה.

נבחין בין שימור טכנולוגי של החומר (ראה סעיפים 4.15.1, 4.15.2) לבין תקופות השמירה שלו כפי שנקבעו בתקנות ובהנחיות. נדגיש כי אין בהכרח חפיפה בין השניים.

4.16 הנעשה בעולם (על קצה המזלג)

בעולם הרחב נעשתה עבודה רבה. הוקמו קבוצות עבודה שונות, נעשו מחקרים, נוסחו תקנים לניהול אלקטרוני של רשומות, ולניהול Meta Data (מאפייני רשומה, תיק), פותחו מסמכי דרישות פונקציונאליות ממערכות לניהול רשומות, נכתבו מדריכים ולומדות לשימור ודיגיטיזציה.

אולם כל מדינה מפתחת לעצמה את אסטרטגיית העבודה בתחום ניהול ושימור אלקטרוני של רשומות.

4.16.1 בשנת 2001 פורסם התקן הבין לאומי הראשון לניהול רשומות ISO 15489. התקן אומץ באוסטרליה, בריטניה ובמדינות נוספות. תקן זה מהווה מסגרת עבודה כללית הן לניהול רשומות מסורתיות (נייר, קלטות שמע, מיקרופילם וכו') והן לניהול אלקטרוני של רשומות.

5. שלבים למימוש מערכת ל- "ניהול אלקטרוני של רשומות"

בכל מקרה שבו הארגון החליט לפתוח במהלך של מעבר לניהול אלקטרוני של רשומות תהיה הכנת מדיניות ארגונית למימוש התהליך הכרחית להצלחת הטיפול בנושא.

בהתאם, המלצת הארכיון היא כי כל מוסד ממוסדות המדינה העובר לניהול מערכת אלקטרונית של רשומות יכין לעצמו מדיניות הכוללת מספר שלבים.

בעולם מקובלים השלבים הללו במימוש התהליכים:

5.1 **התארגנות** - שילוב הפרויקט בתוכנית העבודה של המשרד, הגדרת גבולות המערכת: תכולה, מטרה, יעדים, היקף ואוכלוסייה וקביעת אבני דרך.

5.2 **מיפוי ניהול המידע** - מיפוי ניהול המידע הקיים בארגון ומיפוי החוקים הרלוונטיים כדי שניתן יהיה לזהות ולהגדיר את התחומים הקיימים ואת התחומים בהם צריך לבצע חשיבה מחדש או שינוי של המדיניות הקיימת.

המיפוי יכלול נושאים כגון:

5.2.1 מיפוי מערכות קיימות – מערכות הרלוונטיות לניהול אלקטרוני של רשומות בארגון – ומיפוי התכנים בהן.

5.2.2 אלו מסמכים מוכרזים כרשומות ומתי, היכן הם נשמרים.

5.2.3 אלו רשומות אלקטרוניות המצביעות על חומר פיסי (מסמכי נייר, קלטות שמע, סרטים אור –קוליים וכו') מנוהלות ובאילו נושאים, והאם רשומות אלה מנוהלות יחד עם רשומות המצביעות על חומר אלקטרוני.

- 5.2.4 בחינת סוגי הפורמטים בשימוש – הן של חומר פיסי והן של חומר אלקטרוני.
- 5.2.5 בחינת שיטות התיוק והמטה דאטה.
- 5.2.6 בחינת מדיניות הזנת/לכידת מטה דאטה.
- 5.2.7 בחינת מדיניות האבטחה, הגישה וביצוע הפעולות על המידע ע"י העובדים השונים בארגון.
- 5.2.8 בחינת תקופות שמירה של הרשומות (לפי תקנות הביעור וההנחיות).
- 5.2.9 בחינת מדיניות שימור הרשומות.
- 5.2.10 בחינת מדיניות הביעור ומדיניות הסילוק/ העברת הרשומות (העברה לגניזה; לארכיון המדינה; או ביעור).
- 5.2.11 בחינת הקשר/השילוב של ארכיון קיים (פיזי או דיגיטלי), לרבות בחינת סוגיית דיגיטיזציה של חומר פיזי.
- 5.3 **ניתוח תהליכים עסקיים** - גם במקרה שקיימת מערכת ממוחשבת לניהול רשומות, חיוני / מומלץ לבצע ניתוח כולל, שיעסוק בין השאר, במיפוי ובזיהוי של תהליכים בארגון, מיפוי הגורמים המעורבים בתהליכים ותחומי אחריותם ועוד.
- 5.4 בחינת חלופות לכלים לניהול אלקטרוני של רשומות.
- 5.5 ככל שהארגון עושה שימוש בלעדי באמצעים דיגיטאליים לתיעוד פעילויות הארגון, המידע הדיגיטאלי שנוצר עשוי לשמש כעדות היחידה לפעילויות או החלטות הארגון, עיקרון זה מחייב את הארגון לזהות את כל התהליכים אשר יוצרים תוכן חשוב לארגון ולבצע פעולות ללכידה ולשמירה על הרשומות הרלוונטיות בהתאם למדיניות/חוק.
- 5.6 ניהול פרויקט – כמו כל פרויקט אירגוני, גם פרויקט מסוג זה מצריך מינוי מנהל פרויקט ותכנון ומעקב לכל אורך מחזור החיים.
- 5.7 ניהול שינויים ארגוניים - אוטומציה של תהליכים בארגון גורמת לשינוי מעבר לאופן ביצוע התהליכים ומשפיעה על התפקידים והאחריות של העובדים בארגון.
- בכל הטמעה של מערכת ממוחשבת נדרש להתייחס למרכיב האנושי ולפעול למיזעור התנגדויות.
- כישלונות בפתרונות או ביישום מערכות לניהול רשומות, נובעים לעיתים קרובות מליקויים בניהול השינוי הארגוני ולא דווקא מבעיות טכנולוגיות.
- 5.8 פיילוט – כשלב ראשון בתהליך מומלץ לעשות פיילוט ע"מ שניתן יהיה להתרשם ולהפיק לקחים מתפעול המערכת והתאמה לצרכי הארגון.

- 5.9 ניהול סיכונים - כמו בכל פרוייקט, חיוני למפות את הסיכונים ולהקטינם. מומלץ ללוות את ההחלטה אם למחשב את תהליכי ניהול רשומות בניתוח סיכונים. הניתוח יתייחס בין השאר גם לשאלה אם לא לממש או לממש באופן הדרגתי שיוגבל לנושאים מוגדרים מראש או ליחידות מוגדרות מראש בתוך הארגון.
- 5.10 כ"א לתפעול והטמעת המערכת. נדרשות פעולות הדרכה והטמעה בקרב העובדים בהפעלת המערכת.
- 5.11 נהלים – הארגון יוודא כתיבת נהלים והנחיות ברורות לצורך התפעול השוטף של מערכת ניהול הרשומות, באופן שיתנו מענה לאמור להלן בסעיף 6 - עקרונות למימוש מערכת ל-"ניהול ושימור אלקטרוני של רשומות".
- 5.12 שימור אלקטרוני - הארגון יפתח יכולות ניהוליות, טכנולוגית ואנושיות בארגון לתמיכה בתהליכי השימור של הרשומות ראה לעיל סעיף 4.15 שימור אלקטרוני של רשומות.
- 5.13 בקרת איכות - כמו בכל פרוייקט מחשוב, הארגון יתכנן ויבצע בדיקות קבלה למערכת.
- 5.14 ניהול תצורה - הארגון יוודא כי המערכת תואמת לא רק את היכולות הנדרשות לניהול רשומות אלא שהיא משתלבת בתפיסה הכוללת של מערכות המחשב של הארגון.
- 5.15 תרבות ארגונית - יצירת תרבות ארגונית המדגישה את הערך והחשיבות של ניהול הרשומות במערכת מחשב ושימור רשומות טוב היא חלק מן המהלך כולו וחיונית להטמעתו בארגון, הארגון יוודא שכל העובדים העוסקים ברשומות הארגון, ינהגו בהתאם לכך.
- במסגרת זאת, חיוני לקבל את מחוייבות המנכ"ל / סמנכ"ל לנושא.

6. עקרונות למימוש מערכת ל- "ניהול ושימור אלקטרוני של רשומות"



6.1 הבהקים

6.1.1 מערכת מסוג זה צריכה לדעת לטפל בכל סוגי המידע הנוצרים במערכות פנימיות או מגיעים ממערכות חיצוניות ומוגדרים כחלק ממערך ניהול הרשומות בארגון כמו: מסמכים, תמונות, הודעות דואר אלקטרוני, קטעים קולים, סרטים וכו'.

6.1.2 מערכת מסוג זה צריכה לנהל מסמכים ורשומות הן בעלות תוכן אלקטרוני והן בעלות תוכן מסורתי כגון: תיקים נייריים, קלטות שמע, קלטות אור-קוליות ועוד.

המערכת צריכה לתמוך באפשרות להכריז על כל מסמך כרשומה הן באופן ייזום או באופן אוטומטי בעת יצירת המסמך.

6.1.3 הרשומה במערכת חייבת להיות מנוהלת באופן שוטף, ולהישמר באופן מהימן, כעדות אמינה לפעילות הארגון ללא יכולת לשנותה. רשומה במערכת צריכה להיות מוגבלת/מנועה/נעולה בפני גישה של משתמשים שאינם מורשים. מומלץ לא לאפשר עדכון רשומות (לרבות מטה דאטה הכרוך ביצירת הרשומה ובהכרזה על הרשומה). כאשר צריך או ניתן לבצע שינויים המערכת נדרשת לתעד אותם באופן מלא. הנחיות אלו משרתות גם את תנאי תקנה 3א' לתקנות העדות, כפי שפורטו בסעי' 4.18 לעיל.

6.1.4 המערכת תלכוד את המידע באופן אוטומטי ככל הניתן, ותשלבו בשדות המטה דאטה של הרשומות. הניסיון מראה כי משתמשים אינם אוהבים שעבודתם השוטפת מופרעת ע"י משימות שאינן משרתות אותם. אין זה מעשי לצפות מהמשתמש להזין הרבה שדות מטה דאטה.

- 6.1.5 הרשומות והמסמכים במערכת חייבים להיות מתויקים עפ"י מפתח תיוק, המשקף את הפונקציות הארגוניות והנושאים בהם עוסק הארגון. מערכת התיוק תהיה היררכית (עם מינימום של שלוש רמות מתחת לרמה הראשית) ותייצג בצורה הטובה ביותר את פעולות הארגון ומבנהו.
- 6.1.6 רשומה תהיה נגישה ככל הנדרש, בהתאם לדרישות הארגון והחוק, וזאת רק עבור משתמשים מורשים. הנגישות משמעה שניתן יהיה לאתר, לאחזר ולהציג רשומות ע"י שימוש בכלים סטנדרטיים (תוכנה וחומרה סטנדרטיים להצגת הרשומה והשימוש בה).
- 6.1.7 הרשומה צריכה לשקף את פעילות הארגון, ולכן צריך לשמור את ההקשר בין הרשומה לפעילות שיצרה אותה וכן את הקשרים לרשומות אחרות. הדרך לכך היא באמצעות לכידת/הזנת מטה דאטה.
- 6.1.8 ביעור או העברה של רשומות ינוהל בצורה עקבית ומבוקרת. נקודת מפתח בניהול תקין של רשומות הינה ניהול תקופות השמירה שלהן, ביעורן והעברתן (לארכיון/מערכת/אחסון אחר) בעת הצורך.
- מערכות צריכות להיות מסוגלות לבער ו/או להעביר רשומות בדרך עקבית, מבוקרת ואחראית, בהתאם למדיניות הארגון ולדרישות החוק ובאופן שניתן יהיה "לגשת" אליהן במערכות אליהן יועברו (דוגמת ארכיון המדינה).
- 6.1.9 חיוני לזכור שהצורך בשמירה אלקטרונית של רשומות עשוי להיות מעבר לאורך החיים של המערכת בהן נוצרו/נאגרו והוא מחייב המרה של הרשומה בין פלטפורמות טכנולוגיות.

6.2 התהליכים שיש לנהל במערכת לניהול אלקטרוני של רשומות

תהליכי ניהול הרשומות שלהלן חיוניים ליצירת רשומות שלמות אותנטיות ושמישות שיותאמו לסטנדרטים ולנהלים בארגון.

6.2.1 יצירה

רשומה נוצרת כתוצאה מפעילות/אירוע/תהליך עסקי כאשר התוכן נדרש לארגון ומשמש כעדות לפעילותו.

תהליך היצירה מאגד בתוכו מספר פעולות המתבצעות ברצף או בו-זמנית ומפורטות להלן:

6.2.1.1 הכרזה: תהליך המגדיר כי תוכן המסמך ומספר ממאפייני המטה דאטה מוקפאים ובזה המסמך מוצהר כרשומה.

6.2.1.2 לכידת התוכן: התוכן (מסמך, תמונה ועוד) יכול להיות:

א. אלקטרוני: מצורף באופן אוטומטי מיישומי משרד תקניים ו/או באופן יזום כאשר מאוחסן כקובץ.

ב. מסורתי: הפניה לחומר המתויק באופן פיזי ולא באופן אלקטרוני.

6.2.1.3 לכידת מטה דאטה: באופן יזום (הקלדה) ו/או באופן אוטומטי המתאר את תוכן, מבנה ומאפייני הרשומה. מאפשר יצירה, רישום, תיוק, נגישות, אחזור, הבנת הקשר בין רשומות, שימור וביעור של רשומות לאורך זמן. המטה דאטה הוא אחד המרכיבים המבטיחים את שמירת הרשומה כמקורית לאורך זמן.

6.2.1.4 תיוק: תיוק הרשומה עפ"י מפתח תיוק המשקף את הנושאים בהם עוסק הארגון או את הפונקציות הארגוניות.

לדוגמא, בתיוק מבוסס נושאים, הרשומות הקשורות לתחומים נושאיים רחבים יקובצו יחד (לדוגמא: כוח אדם, פיצויים, משכורות וכו').

6.2.1.5 הקשר בין רשומות: קישור של רשומות בעלות מאפיינים ותכונות משותפים. לעיתים, אוסף של רשומות אלקטרוניות מציג באופן משותף סיפור של אירועים; סדרה של פעילויות משולבות הקשורות אחת בשנייה.

הקשר בין רשומות יכול להיווצר ע"י שרשור בין הרשומות ו/או באמצעות רכיבי המטה דאטה כגון: כותרת, נושא, תאריכים, מחבר וכו'.

כאשר קיימים קשרים בין רשומות המיובאות ממערכת אחרת, המערכת לניהול רשומות צריכה להיות מסוגלת לזהות, ללכוד, לתעד ולשמור את הקשרים האלה לאורך זמן.

כל שינוי בהקשר חייב להיות מתועד ולכלול פירוט והסברים.

6.2.2 אחזקה ושימור

6.2.2.1 הערכה: החלטה לגבי אורך תקופת השמירה של הרשומה. ישנן רשומות שיימצאו מתאימות לשמירה לצמיתות בעוד אחרות ישמרו לתקופות מוגבלות בזמן שייקבעו בתקנות הביעור או בהנחיות שמפרסם הגנז. ביצוע ההערכה, על ידי ארכיון המדינה ו/או בהנחייתו רצוי שיעשה קרוב ככל הניתן ליצירת הרשומה.

6.2.2.2 שינוי: משעה שהוכרזה כרשומה, יש לתעד כל שינוי המתבצע או ליצור גרסאות נוספות של אותה רשומה. אין לשנות רשומה

שנוצרה ונתקבעה.

מכאן, שהתוכן וגם המטה דאטה המתעדים החלטות או תהליכים קודמים אינו יכול להשתנות, אבל ניתן להוסיף בתנאים מסוימים מטה דאטה חדש. נדגיש שאין הכוונה לנעילה מוחלטת של המערכת, באופן שיימנעו תיקונים קלים לתיקון פעולות שנעשו בשגגה. הדרישה היא שהרשאה לשינויים תהיה מוגבלת, או תיאסר באופן מוחלט במצבים מסוימים, כגון מכח הסדר חקיקתי או כתוצאה ממנו.

ניתן לשנות מיקום של רשומה, מיון וקטלוג שלה, אם נדרש. אם נדרש לשכפלה או לחשוף אותה חלקית, הפעולה תבוצע בצורה מבוקרת ומתועדת, על ידי יצירת רשומה חדשה הקשורה לרשומת המקור.

6.2.2.3 שימוש בפורמטים מקובלים וסטנדרטים בשוק, ולא בפורמטים מיוחדים וייעודיים בכדי:

א) לצמצם את הרגישות לשינויים טכנולוגיים. חומר השמור על מצע מגנטי כלשהו ובפורמט כלשהו, הופך בחלוף מספר שנים לבלתי ניתן לקריאה ולשימוש, וכתוצאה מכך הופך לחסר ערך. להקל על הצפייה והשימוש ברשומה ע"י עובדי המשרד והאזרח. שימוש בפורמטים שאינם סטנדרטים יחייב את המשרד להשתמש ולתחזק כלים ייעודיים לצפייה ברשומותיו.

ב) לאפשר ייצוא הרשומות לארכיון המדינה או לגורמים אחרים. בכלל זה מערכת ארכוב המשמשת את הארגון לסילוק רשומות.

6.2.3 אחזור

6.2.3.1 יכולת אחזור של רשומה באופן מהיר ובקלות_ (בעתיד יוציא הארכיון מסמך הרחבה בנושא).

6.2.3.2 המערכת מסוגלת לחפש ולאחזר תיקיות ורשומות אלקטרוניות, על ידי חיפוש אחד המשלב מספר קריטריונים.

6.2.3.3 יכולת חיפוש פשוט או חיפוש "חופשי" על פי מילה או צירוף מילים. חיפוש ממוקד, המאפשר ירידה לעומק על פי חיתוך פרמטרים שונים, בכדי להגיע לתוצאה האופטימלית.

חיפוש בוליאני (או/גם) ומורפולוגי.

6.2.3.4 יכולת שילוב כלים לאיחזור טקסטואלי.

6.2.3.5 יכולת שילוב מילונים מבוקרים כדוגמת טזאורוס.

6.2.4 ביעור

- 6.2.4.1 הקצאת תוכנית ביעור לתיקים ; אותה תוכנית ביעור תחול על כל סוגי התיקים : תיק פיזי , תיק אלקטרוני ותיק אלקטרוני מעורב (הקשור ביחד עם תיק פיזי).
- 6.2.4.2 אישור ביעור רשומות שנשמרו לתקופות השמירה וניתן לבערן בתום מועד תקופת השמירה, בהתאם להסדר הקבוע בתקנות הביעור ובתקנות בתי המשפט.
- 6.2.4.3 שמירת מטה דאטה מינימאלי לאחר הביעור, כעדות לקיום הקודם של התיק.
- 6.2.4.4 ישנן מערכות המפרידות בין ניהול המטה דאטה לבין ניהול הרשומות המחזיקות בתוכן הרשומה. חיוני לוודא שבעת ביעור רשומה מתיק כלשהו שהגיע למועד הביעור, לא יימחקו הרשומה עצמה והמטה דאטה שלה המקושרים לתיק אחר, שטרם הגיע מועד ביעורו (או מיועד לשימור לצמיתות).

6.2.5 מעקב ובקרה

- מערכת לניהול אלקטרוני של רשומות חייבת לנהל גישה לרשומות על בסיס הרשאות לפעולה, לבנות תחנות בקרה ולעקוב אחר שינויים ברשומות : מה קרה, מתי וע"י מי ; לתעד כניסות למערכת, ע"מ להוכיח שהפעולות בוצעו ע"י משתמשים מורשים. חובות אלו נובעות גם מתנאי תקנה 3א' לתקנות העדות, אשר פורטו בסעי' 4.18 לעיל.
- 6.2.5.1 הגישה לרשומות הארגון תתאפשר אך ורק באמצעות המערכת לניהול אלקטרוני של רשומות.
- 6.2.5.2 ע"מ לשמור על אותנטיות, מהימנות, שלמות ושימושיות, הרשומות המאוחסנות במערכת חייבות להיות מוגנות לכל אורך חייהן, כנגד גישה לא מותרת ושינוי במזיד או בשגגה, בתוכן, במבנה שלהן ובהקשרן.
- 6.2.5.3 המערכת צריכה לספק דוחות מעקב על הרשומות והניהול שלהן.
- 6.2.5.4 גישת המשתמשים לרשומות הארגון ופעולה בהן, תיעשה תחת ניהולו של "פרופיל משתמש" (מנוהל במסגרת מערך האבטחה של הארגון) מוגדר מראש.

6.2.6 יצוא/יבוא

כבר בשלב תכנון מערכת לניהול אלקטרוני של רשומות חיוני לקחת בחשבון את הדרישות הבאות, כחלק מדרישות הארגון.

6.2.6.1 נדרש לאפשר ייצוא רשומות לארגונים אחרים. הדבר נדרש במקרה של מיזוג או שינויים ארגונים, או במקרה של העברת רשומות ממערכת מקוונת לניהול רשומות למערכת שמירה או להפקדת חומר בארכיון. יצוא כזה דורש את שמירת הקשר בין הרשומה למטה דאטה שלה.

6.2.6.2 זמן שמירה של רשומות רבות יכול היות ארוך מאורך חיי המערכת המנהלת אותן, ולכן קרוב לודאי שיהיה צורך לייצא את הרשומות למערכת חדשה לניהול רשומות. יצוא כזה דורש את שמירת הקשר בין הרשומה למטה דאטה שלה.

6.2.6.3 יתכן צורך ביבוא של רשומות מתוך מערכות מחשוב אחרות בארגון, ובכלל זה מערכות משיקות המנוהלות בסביבות שונות. יבוא כזה דורש את שמירת הקשר בין הרשומה למטה דאטה שלה.

6.2.6.4 כדי לאפשר יבוא ויצוא של רשומות, חיוני להשתמש בפורמטים פתוחים ותקנים מקובלים. הדבר יקטין את העלות והקשיים בכל תהליך של יבוא/יצוא.

נספח - סקירה - ההסדרים החקיקתיים

מרכיב בלתי נפרד מסוגיית ניהול הרשומות במדינה הוא ההסדרה החקיקתית של התחום, על היבטיו השונים, באמצעות החוקים, התקנות וההנחיות המנהליות השונות (להלן בפרק זה: "כללים"). תחת מרכיב זה חוסות, זו בצד זו, מספר מערכות כללים, ובכללן: מערכת הכללים המטפלת בהיבטים הראייתיים של ניהול הרשומות האלקטרוני, מערכת הכללים המסדירה את הצדדים הארכיוניים של ניהול הרשומות האלקטרוני, ובצידן מערכות כללים ספציפיות החלות על כל משרד/מוסד בהתאם לתפקידיו ושטחי פעולתו, ומערכת החוקים הכללית החלה על כל אדם וגוף במדינת ישראל והנוגעת להגנה על זכויות הפרט והכלל בתחומי חופש המידע, הגנת הפרטיות וזכויות יוצרים וכיו"ב.

בפרק זה נתייחס לשורת הכללים המסדירים את ההיבטים הארכיוניים של עולם ניהול הרשומות בכלל, ובתוך כך עולם ניהול הרשומות האלקטרוני. בתחום זה ניתן למצוא, בין השאר, את ההוראות הקובעות את כללי השימוש, השימור, השמירה והביעור של הרשומות, ההוראות הקובעות את חובת הפקדת חומר ארכיוני בארכיון, והמגדירות את היקפיה, וכן הוראות הקובעות את התנאים שיאפשרו ביעור חומר ארכיוני קודם לתום תקופת השמירה שלו, באופן העולה בקנה אחד עם תקנות העדות (העתקים צילומיים), התשכ"ט - 1969.

6.2.7 חוק הארכיונים, התשט"ו-1955

חוק הארכיונים, התשט"ו - 1955 – קובע את המסגרת המשפטית והמנהלית לטיפול בחומר ארכיוני במדינת ישראל. בחוק מעוגנות, בין היתר, הגדרתו של חומר ארכיוני, דרכי השימוש והטיפול בחומר ארכיוני ושורת סמכויותיו של גנז המדינה - הן ביחס לחומר הארכיוני והן ביחס למוסדות המדינה². מן החוק משתמעם תפקידיו של ארכיון המדינה, כמי שאמון על ניהול המערכת הארכיונית במדינת ישראל ועל שימור לדורות של כלל החומרים – ממלכתיים ושאינם ממלכתיים - הנושאים משמעות לאומית, הסטורית, חברתית וכיו"ב.

מכח החוק תוקנה שורה של תקנות המיועדות להסדיר ולקבוע את פרטי השימוש והטיפול בחומר ארכיוני בעת הימצאו ברשות מוסדות המדינה, וכן את ההוראות החלות על חומר ארכיוני המיועד לשמירה לצמיתות מעת הפקדתו בארכיון המדינה. בצד קביעת ההסדרים ביחס לעיון בחומר ארכיוני, לתנאי ביעורו, לתקופת השמירה שלו ועוד, הוענקה לגנז הסמכות להנחות את

² במונח זה הכוונה לכלל המשרדים, המוסדות והגופים שהחוק חל עליהם, לרבות מוסדות המדינה המופיעים בצו הארכיונים (הכרזה על מוסדות מדינה), התשכ"ו - 1966, ולרבות הרשויות המקומיות.

מוסדות המדינה ולפקח עליהם בכל הנוגע ליישום הסדרים אלו, לרבות בנוגע לניהול רשומותיהם ממועד היווצרותן ועד למועד ביעורן או הפקדתן בארכיון.

התקדמות דברי החקיקה לעבר העידן האלקטרוני

המעבר של ארגונים ומוסדות מדינה לניהול רשומות אלקטרוני חייב התייחסות חקיקתית מתאימה - בהיבט הראייתי והארכיוני גם יחד. במסגרת זו נעשו עד כה מספר תיקוני תקנות שאיפשרו למוסדות מסוימים סריקת מסמכים וביעורם, קודם לתום תקופת השמירה הקבועה עבורם בתקנות הביעור או בהנחיות.

תקנות הארכיונים (שמירתם וביעורם של בתי דין ובתי משפט)

בשנת 2005 תוקנו תקנות הארכיונים (שמירתם וביעורם של בתי דין ובתי משפט), התשמ"ו-1986 (להלן – תקנות בתי המשפט) באופן שנועד לאפשר למערכת בתי המשפט, לבער כתבי בית דין שמוגשים כמסמכי נייר, בטרם חלפה "תקופת השמירה" הקבועה עבורם בתקנות הביעור/הנחיות, ובלבד שנסרקו ונתקיימו בסריקה תנאי תקנות העדות (העתקים צילומיים), תש"ל – 1969 (להלן – תקנות העדות) הנוגעים לענין.

6.2.8 תקנות העדות

במקביל, בשנת 2005 הוכנס תיקון לתקנות העדות, ונקבע הסדר שלפיו העתק סרוק של מסמך שמקורו בוער, יוכל לשמש ראיה לכאורה בהליכים משפטיים, בכפוף לעמידה בשורה של תנאים המבקשים להבטיח את שלמותה ומהימנותה של הרשומה הסרוקה, ואלו הם:

"3א (א) מסמך סרוק של מסמך שבוער מקורו, ישמש ראיה לכאורה בהליכים משפטיים אם נתקיימו בו התנאים האלה:

- (1) הסורק אישר שהמסמך נסרק מהמקור בשלמותו ונלווה לקובץ המחשב מידע המציין שהוא תוצר של סריקה ממוחשבת;
- (2) ננקטו אמצעים סבירים כדי להבטיח את שמירת קובץ המחשב בצורה נאמנה למקור;
- (3) ננקטו באופן סדיר אמצעי הגנה סבירים מפני חדירה לקובץ המחשב ומפני שיבוש בעבודת המחשב העלולים לפגום בנאמנות קובץ המחשב למקור;
- (4) אם חל מעבר מטכנולוגיה לטכנולוגיה, ננקטו אמצעים סבירים כדי להבטיח את נאמנות קובץ המחשב למקור;
- (5) תועדו הפעולות המפורטות בפקאות (1) עד (4);
- (6) "...

יזכר כאן כי שלמות הרשומה ומהימנותה הם, כפי שצוין בסעי' 4.10 לעיל, מאפיינים הכרחיים עבור כל "רשומה נאותה".

6.2.9 תקנות הביעור

תיקון דומה לתיקון שנעשה בתקנות בתי המשפט, הוכנס בשנת 2008 לתקנות הביעור. על פי תיקון זה יחידות/מוסדות שיופיעו בתוספת השניה לתקנות הביעור, יהיו רשאיות לבער תעודות שגרתיות ומסמכים נוספים לאחר סריקת המקור ושמירת ההעתק הסרוק בכפוף לעמידה בתנאים מסוימים, וביניהם: תנאי תקנות העדות ונהלים לביצוע סריקה שיקבע המוסד באישור הגנז.

להלן התייחסות קצרה ותמציתית למספר חוקים אשר להם השלכות על עולם ניהול הרשומות האלקטרוני ומימשיקים איתו.

על הארגונים העוברים לניהול רשומות אלקטרוני לבחון ולשקול את ההשפעות שיש לחוקים אלו על נושאי עבודתם וכן לבדוק קיומה של חקיקה ספציפית המסדירה/הנוגעת לשטחי פעולתם, ואשר עשויה להיות מושפעת ממהלך שכזה.

6.2.10 חוק הגנת הפרטיות, התשמ"א - 1981

החוק מסדיר את הזכות לפרטיות שעוגנה בזכות יסוד חוקתית בחוק יסוד: כבוד האדם וחירותו. החוק מגדיר מהי פגיעה בפרטיות באמצעות רשימה של פעולות המהוות פגיעה בפרטיות, ואף קובע כי הפגיעה בפרטיות מהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית.

פרק שלם בחוק מוקדש לטיפול בסוגיית ההגנה על הפרטיות במאגרי מידע ובמערך הדיור הישיר, והוא מיועד לספק כלים שיאפשרו הגנה מפני חדירה למידע ממוחשב ואכיפתה במסגרות אלו.

בפרק זה מוסדרת סוגיית מאגרי מידע, רישום, ניהולם והשימוש בהם. החוק מורה כי ניהול/החזקה במאגר מידע, העונה על התנאים הקבועים בחוק (ובכללם: מאגר שיש בו מידע רגיש, נתונים על אישיותו של אדם ועוד), מחייבים רישומו של כל מאגר בפנקס מאגרי המידע המנוהל על ידי רשם מאגרי המידע. ככלל, החוק אוסר על בעל מאגר מידע או עובד החשוף למאגר מידע לפרסם מידע מתוך המאגר; כן מטיל החוק אחריות על בעל מאגר מידע/מנהל/מחזיק בו לאבטחת המידע שבמאגר המידע. בחוק מוקמת יחידת פיקוח שבראשה עומד הרשם ובסמכותה לפקח על מאגרי המידע, רישוםם ואבטחת המידע בהם.

חוק זכות יוצרים, התשס"ח - 2007

חוק זכות יוצרים מסדיר את דיני הקניין הרוחני בישראל.

החוק קובע שורה ארוכה של עקרונות וכללים בתחום זכויות היוצרים, ובתוך כך קובע מהי זכות יוצרים, מהם שימושים מותרים ביצירה – שעשייתם אינה מהווה הפרת זכות יוצרים, למי הבעלות בזכות היוצרים, מהן תקופות ההגנה על זכויות יוצרים, למי הבעלות בזכות יוצרים, מהי זכות מוסרית ("קרדיט"), מהן העבירות בתחום ומה העונשים עליהן ועוד...

יצוין בקצרה כי מדינת ישראל תהא הבעלים הראשון בזכות היוצרים של יצירה שנוצרה או הוזמנה על ידה או על ידי עובד המדינה, אלא אם סוכס אחרת. תקופת ההגנה על זכויות היוצרים ביצירה שהמדינה היא בעלת זכות היוצרים בה תהא 50 שנים ממועד יצירתה.

6.2.11 חוק חופש המידע, התשנ"ח - 1998

החוק מעגן את זכותו של כל אזרח או תושב לקבל מידע מכל רשות ציבורית, כהגדרתה בחוק. החוק מסדיר את רשימת הגופים החייבים לספק מידע לפיו, קובע את דרכי הטיפול בבקשות לקבלת מידע שמוגשות לפיו, ואף קובע באלו מקרים ובאלו נסיבות תהיה הרשות פטורה מחובתה למסור מידע. בתוך כך ככלל, הרשות לא תמסור מידע אשר שגילוי מהווה פגיעה בפרטיות, כמשמעה בחוק הגנת הפרטיות הנ"ל.

החוק מטיל על הרשות חובה למסור כל מידע המצוי ברשותה (בכפוף לחריגים הקבועים בחוק), לרבות מידע כתוב, מצולם, ממוחשב וכו'. דרך קבלת המידע תהא בהתאם לסוג המידע וצורת החזקתו, והיא כוללת עיון, צפייה, קבלת פלט מחשב וכו'.

6.2.12 חוק חתימה אלקטרונית 2001

חוק חתימה אלקטרונית נועד להסדיר את מעמדם המשפטי של מסמכים שהם מסרים אלקטרוניים שנחתמו בחתימה אלקטרונית.

החוק קובע כי ככלל, ניתן למלא דרישה חוקית לחתימה על מסמך באמצעות חתימה אלקטרונית מאושרת, כן נקבע כי מסמכים שנחתמו בחתימה אלקטרונית מאובטחת יהיו קבילים כראיה לכאורה בהליכים משפטיים לצרכים מסוימים.

החוק מגדיר מהי חתימה אלקטרונית מאושרת ומהי חתימה אלקטרונית מאובטחת, ויוצר את המסגרות שמאפשרות יצירתן של חתימות אלקטרוניות מאושרות. על פי החוק "גורמים מאשרים" שעמדו בתנאי החוק ונרשמו במרשם שמנהל "רשם הגורמים המאשרים", רשאים להנפיק תעודה אלקטרונית, המהווה מסר אלקטרוני, המאשר כי אמצעי אימות חתימה מסוים הוא של אדם מסוים. חתימה אלקטרונית מאובטחת, כהגדרתה בחוק,

תהפוך לחתימה אלקטרונית מאושרת, במידה שגורם מאשר הנפיק עבורה תעודה אלקטרונית כאמור.

6.2.13 חוק המחשבים, התשנ"ה-1995

חוק המחשבים קובע מהן העבירות הפליליות ומהן העוולות הנזיקיות בתחום השימוש במחשבים. כמו כן החוק מסדיר את ההיבטים הראייתיים ואת עקרונות החיפוש והתפיסה לענין חומר מחשב.

החוק קובע, בין השאר, כי שיבוש פעולתו התקינה של מחשב או שיבוש חומר מחשב, וכן העברה או אחסון במחשב של מידע כוזב הן עבירות פליליות, שהעונש עליהן הוא מאסר. בנוסף נקבע, בין היתר, כי הפרעה שלא כדין לשימוש במחשב ומחיקת חומר מחשב מהוות עוולות נזיקיות.

חוק זה הכניס אף תיקון לפקודת הראיות, שבמסגרתו נקבעו התנאים לקבילותה של רשומה מוסדית.

7. ביבליוגרפיה

- | | |
|-----|--|
| 7.1 | התקן הבין לאומי הראשון לניהול רשומות ISO 15489 |
| 7.2 | התקן הבין לאומי הראשון למטה דאטה ISO_TS_23081-1_2006 |
| 7.3 | התקן הבין לאומי הראשון למטה דאטה ISO_TS_23081-2_2007 |
| 7.4 | דרישות לניהול אלקטרוני של רשומות - הארכיון הבריטי 2002 |
| 7.5 | ICA Overview-principles and Functional Requirements Module1 |
| 7.6 | ICA-Guidelines-principles and Functional Requirements Module 2 |