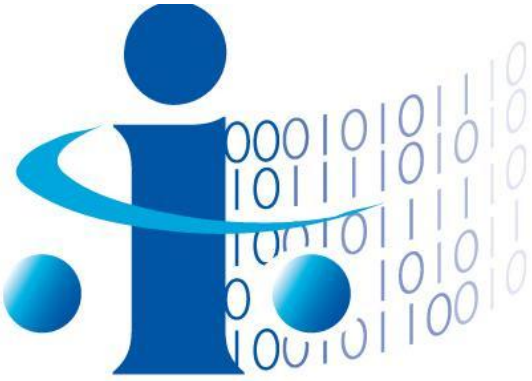


הרשות למשפט, טכנולוגיה ומידע

סיכום פיקוח

בחינת עבודת הועדה להעברות מידע בין גופים ציבוריים

ומינוי ממונה אבטחת מידע בגופים ציבוריים וכשירותו

על פי חוק הגנת הפרטיות, התשמ"א-1981

תוכן עניינים

א. מבוא 3

ב. כללי 4

מסגרת הפיקוח 4

העברת מידע בין גופים ציבוריים – רקע משפטי 5

ג. הועדה להעברת מידע וסדרי עבודתה 7

רקע משפטי 7

עיקרי הממצאים 8

מינוי ועדה 8

תדירות התכנסות הועדות 8

עמידה בהוראות התקנות ומילוי טפסים 9

פרוטוקולים של ועדות להעברת מידע 10

משמעות והמלצות 11

תפקידי הועדה 11

הנחיית הגופים בעניין מילוי הוראות החוק והתקנות 13

עדכון הטפסים ופיתוח מערכת מידע רוחבית לניהול הוועדות 14

ד. פרסום רשימת הגופים אליהם מועבר מידע דרך קבע 15

רקע משפטי 15

עיקרי הממצאים 15

משמעות והמלצות 16

ה. מינוי ממונה אבטחת מידע, כשירותו וסמכויותיו 17

רקע משפטי 17

נושא הבחינה 17

עיקרי הממצאים 18

האם ישנו ממונה על אבטחת מידע בארגון? 19

מהי הכשרתו של הממונה? 20

למי כפוף הממונה בתוך הארגון? 21

האם נוסף על היותו ממונה אבטחת מידע הוא ממלא תפקיד נוסף? 22

האם כפופים לממונה אנשים נוספים לצורך מילוי תפקידו זה ואם כן כמה? 23

משמעות והמלצות 24

ממונה אבטחת המידע - כללי 24

אחריותו של הממונה 24

הכשרתו של ממונה אבטחת המידע 25

ו. נספח א' – הנחיית המשנה ליועמ"ש – העברות מידע בין גופים ציבוריים 26

ז. נספח ב': אחריות בעל המאגר והממונה לאבטחת המידע 32

קביעת אחריות לאבטחת מידע 32

הגדרת הכישורים הנדרשים מהממונה 32

ח. נספח ג': רשימת הגופים המפוקחים 35

א. מבוא

דו"ח פיקוח זה מסכם פעולת פיקוח רוחבית אשר נעשתה על ידי הרשות למשפט, טכנולוגיה ומידע בשנים 2010-2011 בקרב מדגם של גופים ציבוריים במדינת ישראל, לבחינת סוגיות הקשורות בהעברות מידע בין גופים ציבוריים ותפקידו של הממונה על אבטחת מידע הממונה מכוח סעיף 17ב' לחוק הגנת הפרטיות, התשמ"א-1981 בהם.

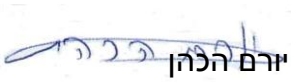
בעריכת הפיקוח וכתיבת הדו"ח השתתפו עובדי רמו"ט הבאים:

- עו"ד רבקי דב"ש מנהלת מחלקת רישום ופיקוח
- עו"ד עמית אשכנזי, מנהל המחלקה המשפטית
- מר יצחק (צחי) ספיר, מפקח
- גב' מריה ג'מאל, מתמחה
- מר אלעד קפלן, מתמחה

דו"ח זה מפרט את התשתית המשפטית לתהליכי העברות מידע ואבטחת מידע בגופים ציבוריים, את התשתית העובדתית שנאספה במהלך הפיקוח, ואת התובנות שגובשו ברמו"ט בעקבות דו"ח זה, בין היתר על בסיס נסיון נוסף שנצבר ברמו"ט בהקשר לנושאים אלה.

הדו"ח ממליץ על תהליכי שינוי רבים שיש לבצע על בסיס המסקנות שגובשו, רובם בשיתוף של גורמים נוספים בשירות המדינה.

נוסחו של דו"ח זה אושר על ידי הח"מ, ורמו"ט תקדם את ההצעות המפורטות בו במסגרת תוכנית העבודה שלה לשנת 2013.



יורם הכהן
רשם מאגרי מידע
ראש הרשות למשפט, טכנולוגיה ומידע

ב. כללי

מסגרת הפיקוח

מכוח תפקידם הציבורי, ובין היתר לצורך מתן שירות איכותי ויעיל לאזרח, מחזיקים גופים ציבוריים במידע אישי רב, שחוק הגנת הפרטיות, התשמ"א-1981 (להלן – **החוק**) חל עליו. מקור המידע האישי יכול להיות האזרח עצמו, מידע המועבר מגופים ציבוריים אחרים ואף מידע אישי המתקבל מגופים פרטיים המחויבים למסור מידע על פי דין. היקף המידע המועבר, בדרך כלל, הינו על חלקים נרחבים מהאוכלוסייה, ולעתים על כולה.

בהתאם לחוק, חובת הגוף הציבורי להקפיד כי לא ייעשה שימוש במידע המצוי בידו למעט למטרות לשמן נמסר או התקבל. בהתאם לכך קיימת גם חובה להגן על המידע האמור מפני שימושים לא מורשים בתוך הגוף הציבורי ומחוץ לו. החוק קובע חובה למנות ממונה על אבטחת מידע בכל גוף ציבורי, ופרק ד' לחוק קובע בהתאם הוראות מיוחדות לעניין העברות מידע בין גופים ציבורים. מכוחו נקבעו תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבורים), התשמ"ו-1986 (להלן – **התקנות**).

במהלך שנות העבודה 2010-2011 ביצעה מחלקת רישום ופיקוח ברשות למשפט טכנולוגיה ומידע (להלן – **רמו"ט**), בשיתוף עם המחלקה המשפטית של רמו"ט, פיקוח במסגרת סמכויות הפיקוח של רשם מאגרי מידע הקבועות בחוק (להלן – **הרשם**), לבדיקת קיום הוראות החוק הנ"ל במדגם של גופים ציבוריים.

במסגרת הפיקוח פנתה רמו"ט ל-34 גופים ציבוריים שנבחרו מתוך חמש הקבוצות המוגדרות בסעיף 23(ג) לחוק: מוסדות מדינה, משרדי ממשלה, רשויות מקומיות, תאגידים סטטוטוריים וגופים ציבוריים שנקבעו בצו. מתוך 34 גופים ציבוריים הנ"ל התקבלה התייחסות מ-30 גופים, שנים מהם (הכנסת והביטוח הלאומי) העבירו את המידע באיחור ניכר ולאחר פניות חוזרות ונשנות. ארבעת הגופים המפוקחים שלא השיבו, למרות פניות בכתב ובעל פה הם:

א. משרד הבריאות.

ב. אוניברסיטת תל אביב.

ג. בית חולים אברבנאל.

ד. מועצה מקומית דלית אל כרמל / עיר כרמל.

הפיקוח התמקד בשלושה נושאים:

א. הועדה להעברת מידע וסדרי עבודתה – שעל הקמתה ופעולתה חלה תקנה 3א לתקנות (להלן – **הועדה**).

ב. פרסום רשימת הגופים אליהם מועבר מידע דרך קבע – תקנה 7(ו) לתקנות.

ג. מינוי ממונה אבטחת מידע – שחובת מינויו קבועה בסעיף 17ב(א)(2) לחוק (להלן – **הממונה**).

ממצאי הפיקוח מלמדים על ציות חלקי להוראות החוק ומחייבים בחינה של יעילות ההסדר המשפטי הקיים בתחום העברות מידע בין גופים ציבורים ואמצעים לשיפור הציות לו. בכל אחד מהפרקים נציג את הרקע המשפטי, את נושאי הפיקוח, את הממצאים, ונציע הסדרים מתקנים, בהתאם לממצאי הפיקוח והניסיון המצטבר ברמו"ט בעניין הסדרת הגנת הפרטיות בהעברת מידע אישי.

העברת מידע בין גופים ציבוריים – רקע משפטי

הזכות לפרטיות היא זכות יסוד חוקתית המעוגנת בסעיף 7 לחוק יסוד: כבוד האדם וחירותו (להלן – **חוק היסוד**) ומוגנת בו. החוק קדם לחוק היסוד והוא עיגן בחקיקה עוד בשנת 1981 את הזכות לפרטיות, לרבות את הזכות לפרטיות במידע.

מיד עם כניסת החוק לתוקף התברר כי מעורר מגבלה תפקודית בממשלה על זרועותיה השונות, בשל חסימת האפשרות, לכאורה, להעביר מידע בין גופים ציבוריים. ב-1982 מינה היועץ המשפטי דאז, מר יצחק זמיר את "הועדה לעניין העברת ידיעות בין גופים ציבוריים", בראשותו של עו"ד חיים קלוגמן (להלן - **ועדת קלוגמן**).

ועדת קלוגמן נתבקשה להביע דעתה בשאלות הבאות –

א. באיזו מידה ובאילו עניינים רצוי לאפשר לגוף ציבורי מסוים, או גופים ציבוריים בדרך כלל, להעביר מידע לגופים ציבוריים אחרים?

ב. ככל שרצוי לאפשר העברת מידע כאמור, מה אמורים להיות ההסדרים הראויים בעניין זה?

ג. מהם האמצעים הראויים כדי להפחית את הסכנה של שימוש לרעה באפשרות של העברת מידע כאמור?

הוועדה שוכנעה כי בהעברת מידע בין גופים ציבוריים יש כדי לשרת את האינטרס הציבורי הלגיטימי, בין היתר ליעילות המנגנון הציבורי, לאחידות המידע המצוי בידי הרשויות, לחסכון בכספי ציבור ומניעת הטרדתו של היחיד בבקשות למסירת מידע חוזרות ונשנות. הוועדה הגישה שורה של המלצות המאפשרות העברת מידע, אך לוותה אותם בתנאים מגבילים שנועדו להגן על פרטיות המידע המצוי במאגרי הגופים הציבוריים.

בעקבות מסקנות ועדת קלוגמן, הוסף בשנת 1985 פרק ד' לחוק, אשר מסדיר את נושא מסירת מידע או ידיעות מאת גופים ציבוריים. הכלל, כפי הקבוע בסעיף 23ב לחוק, הוא כי **מסירת מידע מאת גוף ציבורי <u>אסורה</u> למעט במקרים הבאים:**

א. המידע פורסם לרבים או הועמד לעיון הרבים על פי סמכות כדין (סעיף 23ב(א) לחוק);

ב. האדם אשר המידע מתייחס אליו נתן הסכמתו למסירה (סעיף 23ב(א) לחוק);

ג. מסירת המידע או קבלתה נעשתה על ידי רשות בטחון לשם מילוי תפקידה, ובלבד שמסירת המידע או קבלתה לא נאסרה בחיקוק (סעיף 23ב(ב) לחוק);

ד. **מסירת המידע היא בין גופים ציבוריים ועמדת בדרישות סעיף 23ג לחוק.**

בבג"צ 8070/98 האגודה לזכויות האזרח נגד משרד הפנים ואח'[1] דן בית המשפט העליון בחוקיות ההסדר הקיים בחוק ובתקנות, לעניין העברת המידע בפורמט ממוחשב ממרשם האוכלוסין במשרד הפנים לגופים ציבוריים ופרטיים, שלא באמצעות שאילתות פרטניות, אלא בקובץ הכולל כמות נרחבת של רשומות או אף את כלל האוכלוסייה.

בעקבות קביעות שונות בפסק הדין בהקשר של העברות מידע בין גופים ציבוריים, פורסמה הנחייה ליועצים המשפטיים במשרדי הממשלה על ידי המשנה ליועץ המשפטי לממשלה (ייעוץ) ביום 16.03.2006, בנושא "העברת מידע בין גופים ציבורים" (להלן – **ההנחיה**). ההנחיה מצ"ב כנספח א' לדו"ח זה.

הרקע המשפטי הספציפי הנדרש להצגת ממצאי הפיקוח בנושאים השונים שנבחנו ולהבנתם יוצג להלן בפרקים הבאים.

[1] פ"ד נח(4) 842.

ג. הועדה להעברת מידע וסדרי עבודתה

רקע משפטי

תקנה 3א לתקנות קובעת כי בכל גוף ציבורי אשר מוסר מידע או מקבל מידע, ימנה המנכ"ל של אותו גוף ועדה להעברת מידע. יו"ר הוועדה יהיה המנכ"ל או סגנו או עובד בכיר הכפוף למנכ"ל ישירות. מספר חברי הוועדה לא יפחת משלושה, וחובה למנות בין חברי הוועדה את היועץ המשפטי של הגוף הציבורי או נציגו ועובד שתחום עיסוקו הוא ניהול מאגר מידע ואבטחתו.

לפי תקנות 3א(ד) ו-3א(ה) לתקנות ועל פי ההנחייה, תפקידה של הוועדה הוא כפול: ראשית, בחינה של בקשות למסירת מידע מאת הגוף הציבורי ובקשות לקבלת מידע של הגוף הציבורי מאת גוף ציבורי אחר. שנית, קביעת הוראות לעניין הגישה למאגרי המידע שברשות הגוף הציבורי, אשר יבטיחו את השמירה על המידע המצוי במאגרים.

לעניין העברות מידע, קובעות התקנות כי בקשה לקבלת מידע של גוף ציבורי, תוגש למשרד מוסר המידע על ידי המשרד מבקש המידע על גבי טופס א' המצוי בתוספת לתקנות (להלן – **טופס א'**). לפי ההנחיה, הטופס יוגש לועדה לאחר שבעלי התפקידים בועדת העברת המידע של המשרד מבקש המידע אישרו את הבקשה בחתימתם. על הועדה לבחון כי המידע המבוקש אכן נדרש, ובאופן בו הוא נתבקש, וכי מובטח שהגישה למידע תהיה מצומצמת ומפוקחת.

לפי ההנחייה, בקשה להעברת מידע מגוף ציבורי תיבדק על ידי הועדה להעברת מידע רק לאחר שמולא טופס א' כדין, קרי בחתימת כל בעלי התפקידים הרלוונטיים – מנהל מאגר המידע, ממונה אבטחת המידע והיועץ המשפטי בגוף מבקש המידע. כמפורט בהנחיה, בעת בדיקת הבקשות על בעלי התפקידים הרלוונטיים והועדה לבחון, בין השאר, אם הגוף המבקש את המידע הוא "גוף ציבורי" הרשאי לדרוש אותו על פי דין. כמו כן, על הוועדה לבחון את המידתיות והסבירות של הבקשה ואת התאמת רמת אבטחת המידע בגוף הציבורי מבקש המידע לאופי המידע המבוקש, אופי מורשי הגישה למידע המבוקש בגוף המבקש ואופי הטיפול במידע בו.

לאחר קבלת החלטה, על הועדה למלא טופס תשובה, המצוי בתוספת לתקנות, המאשר או דוחה את הבקשה (להלן – **טופס ב'**). לפי סעיף 23ד לחוק, על הגוף הציבורי המקבל מידע דרך קבע להודיע על כך לרשם, על גבי טופס ג' המצוי בתוספת לתקנות (להלן – **טופס ג'**).

על פי ההנחייה, על וועדת העברת המידע לקבוע קריטריונים בנוגע לכל מאגר מידע המצוי ברשות הגוף הציבורי, ובין היתר: מי הם בעלי התפקידים הזכאים לעיין במידע; אופן הגישה למאגר; צמצום המידע אליו קיימת גישה למינימום הנדרש; דרכי הבקרה; קבלת דיווח תקופתי על אופן יישום הוראות הוועדה.

את כללי הגישה יש לפרסם לפי הוראת סעיף 6 לחוק חופש המידע, הקובע בסעיף 6(א) כי רשות ציבורית תעמיד לעיון הציבור את ההנחיות המינהליות הכתובות שעל פיהן היא פועלת ושיש להן נגיעה או חשיבות לציבור.

עיקרי הממצאים

מינוי ועדה

הפיקוח העלה כי עד למועד ביצועו 12 הגופים המפורטים להלן **כלל לא מינו ועדה להעברת מידע**:

א. משרד התעשייה והמסחר

ב. המשרד לקליטת עליה

ג. עיריית חיפה

ד. מועצה אזורית משגב

ה. מועצה מקומית זיכרון יעקב

ו. מכבי שרותי בריאות

ז. קופת חולים לאומית

ח. הרשות למלחמה בסמים

ט. ארגון נכי צה"ל

י. עיריית ירושלים

יא. הרשות לשיקום האסיר

יב. בית חולים תל השומר-שיבא.

תדירות התכנסות הועדות

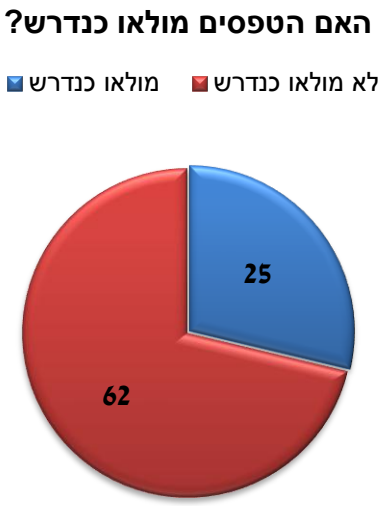
הגרף הבא מפרט, לגבי גופים בהם מונתה ועדה, את מספר הפעמים בהם התכנסה הועדה במהלך שנת 2009:



על אף הדרישה בתקנה 3א(ה) לתקנות, נמצא כי ב**אף אחד מהגופים לא נקבעו הוראות להרשאות עיון במידע מקרב עובדי אותו גוף, אופן הבקרה על הטיפול וזהותם של מורשי הגישה למידע**. על אף האמור בסעיף 23ד(ג), **הגופים אינם מעבירים לידי הרשם טפסי ג' המפרטים על קבלת מידע דרך קבע**.

מהפיקוח עולה כי **פחות מ-30% מהטפסים מולאו כנדרש וללא ליקויים** (25 טפסי א' מתוך 87 שנבדקו). חמור מכך, מהפיקוח עולה כי בתהליך אישור הבקשות על ידי הועדות בגופים השונים, **כמעט מחצית מהבקשות שהוגשו עם ליקויים מהותיים אושרו בכל זאת וללא סייגים** (30 טפסי א' מתוך 62 טפסים עם ליקויים). כמו כן, **ל-30 טפסי א' נוספים שהוגשו עם ליקויים לא צורפו טפסי ב' כלל**. רק 2 טפסי א' נדחו כנדרש בטופס ב' מחוסר סמכות ואי עמידה בדרישות החוק.

נמצא כי בקרב הגופים המפוקחים שורר בלבול וחוסר הבנה כיצד יש למלא את הטפסים המצויים בתקנות, וכיצד יש לבדוק אותם. נמצאו חוסר דיוק ונתונים חסרים בשדות מידע בהם יש לפרט את מטרת בקשת המידע, מקור הסמכות לקבלת המידע ומורשי הגישה למידע. אלה מעלים חשש להתייחסות רשלנית למילוי הטפסים וחוסר הבנה של מטרת החוק.



מעיון בטפסים עולים מספר סוגי ליקויים. להלן עיקרם -

א. חסרים פרטים בנוגע למידע המבוקש והמטרה לשמה נתבקש;

ב. אין פירוט של שדות המידע המבוקשים אלא הגדרה כללית בלבד;

ג. אין תאימות בין המידע המבוקש לבין המטרה לשמה נדרש לקבל את המידע (דוגמה: 2 טפסים בהם מטרת הבקשה היא אימות כתובות, בעוד שבנתונים המבוקשים לא מופיע שדה כתובת).

ד. ההתייחסות לנושא אבטחת המידע היא כללית ביותר ולא מספקת.

ה. חסר פירוט מקור הסמכות החוקית לקבלת המידע. להלן דוגמאות -

- ב-22 טפסים נזכר חוק מסוים מבלי שניתנה הפניה לסעיף המסמיך.
- ב-12 טפסים צוין מקור הסמכות כסעיף 23 או 23ג לחוק הגנת הפרטיות, המופיעים בפרק ד' לחוק ומגדירים מיהו "גוף ציבורי" ואת הסייגים לפיהם ניתן להעביר מידע, אך אינם מסמיכים את הגוף לקבל מידע;
- ב-11 טפסים צוין תפקיד הגוף בלבד (לדוגמה: "מכוח היותנו רשות מקומית");
- ב-2 טפסים צוינו כמקור סמכות הוראות פנימיות של הגוף המבקש.

ו. חסר מידע מדוייק לגבי מורשי הגישה למידע:

- ב-14 טפסים קיים חוסר התאמה בין אפיון תפקיד מורשה הגישה המבוקש למי שניגש למידע בפועל.
- ב-3 טפסים לא מצוין תפקידם של מורשי הגישה, אלא שמם בלבד.

ז. לא כל השדות מלאים כנדרש לאישור הבקשה;

ח. חסר תאריך הגשת הבקשה;

ט. טפסים ממולאים בכתב בלתי קריא;

י. ב-7 טפסים היו חסרות החתימות הנדרשות.

פרוטוקולים של ועדות להעברת מידע

מבחינת הפרוטוקולים של הוועדות עולים ליקויים נוספים הנוגעים לתפקוד הועדה. מתוך 22 פרוטוקולים (של 12 גופים) שנבדקו נמצא כי:

א. ב-5 פרוטוקולים לא צוינה מיהות משתתפי ישיבת הועדה;

ב. ב-15 פרוטוקולים לא הייתה נוכחות מלאה של כל הועדה בישיבה;

ג. ב-15 פרוטוקולים, בהתייחסותם לבקשות העברות המידע, לא הפנו לתאריך הבקשה;

ד. ב-10 פרוטוקולים, בהתייחסותם לבקשות, לא פירטו את תוכן הבקשה באופן בהיר ומובן;

ה. ב-15 פרוטוקולים, בהתייחסותם לבקשות, לא הזכירו את מקור הסמכות לקבלת המידע;

ו. ב-10 פרוטוקולים בהן נדונו בקשות ואלה לא אושרו, או אושרו חלקית, רק לגבי 5 מתוך 10 בקשות תועד הדיון בגינו לא אושרה הבקשה, או סוייגה.

משמעות והמלצות

תפקידי הועדה

העובדה שמדגם הפיקוח העלה כי מחצית מהגופים המפוקחים לא מינו ועדה מעידה, לדעתנו, כי **הנחיית המשנה ליועץ המשפטי לממשלה (ייעוץ) לא הופנמה על ידי השירות הציבורי**, לרבות לא על ידי היועצים המשפטיים אשר היו אמורים לדאוג להקמתן של הוועדות ותפקודן השוטף. ייתכן שהדבר נובע מכך שהנחיה זו אינה מפורסמת בהליך הרגיל של הנחיות יועץ משפטי לממשלה.

לוועדה כאמור שני תפקידים מרכזיים: דיון ואישור של בקשות למסירת מידע וקבלתו, כאמור בתקנה 3א(ד). שנית, קביעת הוראות לעניין הרשאות והגבלות בעניין הגישה למאגרי מידע , בהתאם לסמכותה בתקנה 3א(ה). במסגרת פרסום הוראות, על הועדה לקבוע כי הגישה למידע במאגר תתאפשר רק לאותו עובד אשר קיים צורך לאפשר את גישתו למידע בהתאם להגדרת תפקידו. לצורך כך יש לקבוע הרשאות גישה, כאשר לכל עובד מוצמדת רמת הרשאה המתאימה לתפקידו ומאפשרת לו את היקף הגישה למידע על פי רמת הרשאתו. על הקצאת ההרשאות להתבסס על גישת "צריך לדעת", שמשמעותה: אם העובד לא צריך גישה למידע מסוים לצורך עבודתו, אזי לא תתאפשר לו הגישה לאותו מידע. **מהפיקוח עולה כי סמכותה של הוועדה לעניין קביעת הוראות להרשאות והגבלות לגישה למידע אינה מתבצעת בפועל והועדות מתמקדות באישור בקשות בלבד**.

לדעתנו הועדה נדרשת בראש ובראשונה לצורך קביעת המדיניות הארגונית וההוראות על פיהם יינתנו אישורים לבקשות. בהתאם לכך, **מוצע לשנות את התקנות, באופן השם דגש על הפעילות המהותית של הועדה** כך שיתקיימו ישיבות תקופתיות לקביעת הוראות וטיפול בבקשות מיוחדות להעברת מידע, בעוד בקשות רגילות יאושרו על ידי הדרג המקצועי המנוי בטפסי א' ו-ב'. בנוסף, מוצע כי בגופים ציבוריים המקבלים מעל 4 בקשות למסירת מידע בחודש, תוכל הועדה לקבוע קריטריונים ברורים ותנאי סף לזכאות לקבלת מידע, כך שהועדה תדון רק במקרים החריגים לכללים שנקבעו, וזאת במטרה לצמצם את ההליך הבירוקרטי. לצורך הכנסת הוועדות להליך עבודה סדור, **מומלץ לעדכן את התקנות ולקבוע כי על הועדה להיפגש לפחות פעמיים בשנה לצורך רענון ופרסום הוראות בתחומי אחריותה, וכן לאפשר לה קביעת קריטוריונים כאמור**.

נושא נוסף אשר יש לו השלכות רוחב על העברות מידע, ורלוונטי גם לעבודות הוועדה בפועל הוא **המימוש הטכנולוגי של העברות מידע**. הוועדה להעברת מידע אמורה לתת דעתה, במסגרת האישור, לסוגיות של אבטחת מידע מחד גיסא, ומידתיות העברת המידע מאידך גיסא. נראה כי לוועדות הדנות בבקשות, בפרט בגופים קטנים, חסר לעיתים מידע והבנה על אודות האופן שבו יועבר המידע, האופן יוחזק על ידי הגוף המקבל וייעשה בו שימוש. כן חסר להן לעיתים ידע מקיף ומספק בתחומים של אבטחת מידע ומערכות מידע, לצורך הערכת הסיכון הכרוך בהעברה. גם היכולת של וועדה המאשרת העברת מידע להעריך באופן ראוי את רמת אבטחת המידע של הגוף שאמור לקבל את המידע, לצורך אישור ההעברה, מוטלת בספק.

ההתרשמות שלנו היא כי במקרים רבים מועבר מידע עודף באופן בלתי מאובטח. לדעתנו **נדרש לשקול פיתוחים טכנולוגיים לשיפור המנגנונים המשמשים בפועל להעברת מידע בין גופים ציבוריים, בפרט בין צרכני מידע קטנים לספקי מידע גדולים** (כגון רשות האוכלוסין)**. פיתוחו של פרוטוקולי העברת מידע של השירות הציבורי המפנימים עקרונות של "עיצוב לפרטיות" (privacy by design) עשוי למזער את הסיכונים הנובעים מהעברות מידע אלה**. דוגמה לדרישה להסדר כזה נכללה בהחלטת הממשלה בעניין "סיוע בבדיקת ובמיצוי זכאות להטבות הנלוות לגמלאות שמשלם המוסד לביטוח לאומי"[2] ובהצעת חוק המדיניות הכלכלית לשנים 2011 ו-2012 (תיקוני חקיקה) , התשע"א-2010[3] לעניין העברות מידע מרשות המיסים לבדיקת זכאות להטבות בארנונה[4], ולעניין המסלקה הפנסיונית[5]. **גם בעניין זה תפנה רמו"ט אל הממונה על התקשוב הממשלתי לייזום ופיתוח של מסלקת העברת מידע כאמור.**

חשוב לציין כי נסיונה של רמו"ט מעיד כי לועדת העברת מידע אשר מתפקדת באופן נכון, ובפרט אם היא פועלת בגוף המעביר ו/או המקבל מידע רב, עשויה להיות השפעה רבה על כלל הגופים המקבלים או המעבירים מידע (וזאת בשל האופי הדו-צידי של התהליך, לפיו ארגון הפוגש ועדה מתפקדת ישפר את אופן הטיפול שלו כתוצאה מכך). תובנה זו התגבשה ברמו"ט לאור תוצאות תפקודה האפקטיבי של ועדת העברת המידע ברשות האוכלוסין וההגירה, אשר אחראית לאישור העברות מידע ממרשם האוכלוסין.

מומלץ, אם כן, למפות את ספקי המידע המרכזיים בשירות הציבורי, כמו גם את צרכני המידע העיקריים, סוגיהם ואופי המידע המבוקש על ידם, ולוודא כי ועדות העברת המידע בהם פועלות כראוי, וזאת לצורך יצירת מנגנון פיקוח אפקטיבי באמצעות אותם שחקנים גדולים.

---

[2] החלטה מס' 5155 של הממשלה מתאריך 14.10.2010 שם נקבע:
"(ג) ההסדר המוצע יעוצב בדרך טכנולוגית אשר תמזער את פוטנציאל הפגיעה בפרטיות הזכאים, שתגובש בתיאום עם הממונה על התקשוב הממשלתי.
(ד) ההסדר המוצע יכלול התייחסות לרמת אבטחת מידע הנדרשת בגוף הציבורי, שהולמת לרגישות המידע שיועבר ולהיקפו."
לעיון: http://www.pmo.gov.il/Secretary/GovDecisions/2012/Pages/des5155.aspx

[3] הצעות חוק 541, מיום 18 באוקטובר 2010.

[4] שם, עמ' 64-62

[5] שם, עמ' 69-65.

הנחיית הגופים בעניין מילוי הוראות החוק והתקנות

לצורך העמקת הפנמת הנחיית המשנה ליועץ המשפטי לממשלה, **רמו"ט תכתוב במהלך שנת 2013 הנחיית רשם מאגרי מידע אשר תבהיר את ההנחיה ותרחיב אותה בסוגיות הטכנולוגיות-משפטיות הייחודיות שבתחום התמחותה** של רמו"ט. בכך תעמיד רמו"ט לידי הוועדות כלי עבודה סדור לתפקוד הוועדה. במסגרת זו תיכלל התייחסות לנקודות הבאות:

א. חובות הועדה בעת בדיקת הבקשות לקבלת מידע. ההנחיות יבהירו את האופן הנכון לבחינת הנושאים המפורטים להלן:

- הצורך של הגוף המבקש במידע המבוקש והיקף המידע הנדרש נוכח עקרון המידתיות
- ההרשאה של הגוף הבודק למסור את המידע המבוקש;
- מיפוי האיומים והסיכונים הנובעים מסוג המידע המועבר לגוף המבקש, תוך שימת לב להבדלים באופיי הגוף המוסר והמקבל, ואת אופן ההתמודדות עם הבדלים אלה;
- הגדרה ברורה של מטרות השימוש המותרות על ידי הגוף המבקש;
- קביעת חובת אבטחת מידע כתנאי יסוד למסירתו, לרבות אופני מסירת המידע, הטמעתו למערכות המידע של הגוף המבקש ושימוש בו בפועל;
- בחינת ההבטים הפורמליים של עבודת הגוף המבקש, לרבות מינוי ממונה אבטחת מידע וועדה להעברת מידע;
- קביעת פרק הזמן במהלכו מותר לגוף המבקש לשמור את המידע.

ב. ציון מקור הסמכות לקבלת המידע גם בפרוטוקולים של הועדה, על מנת שיהיה ניתן לנהל מעקב אחר תקינות ההחלטות

ג. החובה למלא ולמסור את טופס ג' לרשם כנדרש בחוק ובתקנות.

ד. סוגי העברות מידע שגרתיות.

ה. פרסום המידע על אודות העברות המידע המאושרות לציבור כנדרש בחוק.

כמו כן הננו ממליצים על פיתוח יישום תוכנה לעבודתן של וועדות העברות מידע בשירות הציבורי, אשר יתבנתו ויסדירו את הליכי העבודה הנ"ל בין הוועדות השונות ברחבי בשירות הציבורי. על יישום זה לוודא:

א. כי הדרישות הפורמליות הנדרשות בעבודת הוועדה ומילוי הטפסים על ידה ייעשו כראוי

ב. כי תהליך בחינת ההבטים המהותיים של הבקשה נעשה ומתועד כראוי

ג. כי נעשית תקשורת תקינה בין וועדות העברת המידע השונות ברחבי השירות הציבורי

ד. כי ייעשה דיווח אוטומטי לרשם מאגרי מידע כנדרש בטופס ג

ה. כי המידע על אודות העברות המידע מפורסם לציבור באופן זמין ובהיר

רמו"ט תפנה לממונה על התקשוב הממשלתי לצורך ייזום פיתוח מערכת רוחבית כזו במסגרת מערכות ממשל זמין.

עדכון הטפסים ופיתוח מערכת מידע רוחבית לניהול הוועדות

הפיקוח העלה כשלים שונים במילוי הטפסים על ידי מגישי הבקשות והוועדות שדנו בהן. בבעיה זו מוצע לטפל בשני מישורים, משפטי וטכנולוגי.

בהקשר המשפטי, נדרש לעדכן את הטפסים כמפורט להלן:

א. יש להוסיף לטופס א' ולטופס ב' המצויים בתקנה שדה לציון התאריך בו נחתם המסמך.

ב. בטופס ב' יש להוסיף הפניה לטופס א' (לדוגמה: "בהמשך בקשתכם בטופס א' מיום...").

ג. מוצע לגבש טופס פרוטוקול אחיד לתיעוד דיוני וועדה, שיקל על הגופים בניהול ומעקב אחר ישיבות הועדה.

בהיבט הטכנולוגי, הטפסים אמורים להיות מוטמעים במסגרת מערכת מידע רוחבית כמתואר לעיל.

ד. פרסום רשימת הגופים אליהם מועבר מידע דרך קבע

רקע משפטי

בתקנה 7(ו) נקבע כי מנהל מאגר ינהל רשימה של כל מאגרי הגופים, פרטים וציבוריים כאחד, למעט מאגרי מידע המנויים בסעיף 13(ה) לחוק, שאליהם נמסר מידע דרך קבע ממאגר המידע של הגוף הציבורי וסוג המידע המועבר.

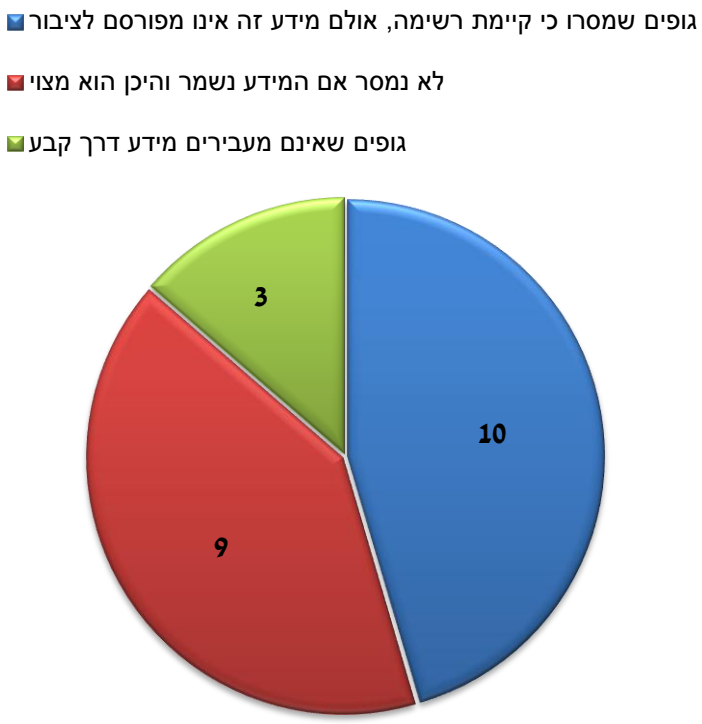
לפי הנחיית המשנה ליועמ"ש, על הרשימה לכלול את הגוף הציבורי אליו מועבר המידע, תדירות העברת המידע או עדכונו, אופן העברת המידע וכן סוג המידע המועבר. הרשימה תעמוד לעיון הציבור בהתאם להוראות סעיף 6(ב) לחוק חופש המידע, המסייג וקובע, כי במידה שאחד מהסייגים המנויים בסעיף 9 לחוק חופש המידע (כגון בטחון המדינה, פגיעה ביחסי חוץ וכד') מתקיים גם לגבי מידע מסוים המצוי ברשימה, אין לפרסם מידע זה.

הרשימה תעמוד לעיון הציבור באתר האינטרנט של הגוף הציבורי, ובאין אתר אינטרנט, במשרד הראשי ובמשרדים המחוזיים.

עיקרי הממצאים

נמצא כי ל- 25 גופים יש אתר אינטרנט **אולם רק 3 מפרסמים** באתר רשימה כמתחייב בחוק (משרד הפנים, משרד האוצר ומד"א).

להלן הנתונים לגבי שאר הגופים המפוקחים:



בבדיקת הרשימות נמצא כי הרשימות אינן מעודכנות, אינן כוללות את כל הגופים אליהם מועבר מידע והפרסום אינו מפרט לציבור, באופן ברור וגלוי, מהו המידע המועבר. להלן שתי דוגמאות:

א. הפרסום באתר משרד הפנים אינו עונה לדרישה בתקנה 7(ו).

- פורטו "קוד שרות", "שם שרות" ו"סוג שרות", שהינם קודים פנימיים של המשרד. על המשרד לספק מידע בהיר ומובן.
- חלק מהמידע שמפורסם אינו מעודכן (דוגמא: המידע אינו תואם את ההסכם עם התאגיד מקבל המידע).

ב. נמצא כי מד"א לא פרסם כי הוא מעביר מידע דרך קבע למאגר למניעת הונאות ביטוח.

משמעות והמלצות

לאור העובדה כי איסוף המידע למאגרי הגופים הציבוריים אינו מבוסס על הסכמתו של אדם אלא על חובה חוקית, מן הראוי כי מקום בו המידע מועבר בין הגופים הציבוריים – יקפידו אלה על חובת השקיפות הנדרשת ביחס להעברות המידע שנאסף על ידי הגוף הציבורי. מטרת חובת שקיפות זו לסייע בבקרה של הציבור על אודות השימוש שעושים הגופים במידע, וחיזוק ההגנה כי המידע מועבר באופן סביר ומידתי כנדרש מחוק היסוד ומחוק הגנת הפרטיות. עמדה זו גם מעוגנת בתקנות.

כמפורט בפרק הקודם, עמדתנו היא כי יש לקבוע מסגרת סדורה ומובנית לעמידת הגופים הציבוריים בחובה שנקבעה בתקנות ומפורטת בהנחייה, לרבות הנגשת המידע הזה באופן אלקטרוני לציבור. הנחיית רשם מאגרי מידע שתפורסם, תכלול התייחסות לנושא זה. בנוסף, אנו מציעים להקדיש אתר ייעודי לכך במסגרת מערכות ממשל זמין, אליו יוכלו כל הגופים מעבירי ומקבלי המידע לדווח את המידע שחובה לפרסם, ובו יוכל הציבור לדעת את התמונה המלאה. גם לעניין זה, רמו"ט תפנה בנושא זה לממונה על התקשוב הממשלתי.

ה. מינוי ממונה אבטחת מידע, כשירותו וסמכויותיו

רקע משפטי

לפי סעיף 17ב(א)(2) לחוק, גופים ציבוריים חייבים במינוי אדם בעל "הכשרה מתאימה" שיהיה ממונה על אבטחת המידע. בסעיף 7 לחוק מוגדרת "אבטחת מידע" כ"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין". על פי סעיף 17ב(ב) הממונה יהיה אחראי לאבטחת המידע במאגר של הרשות הציבורית, בנוסף על אחריותם של בעל מאגר המידע, מנהל מאגר המידע והמחזיק במאגר המידע לאבטחת המידע בו. לפי תקנה 2 לתקנות על הגוף הציבורי להודיע לרשם בכתב את שמו של הממונה.

לפי ההנחיה, אישור הוועדה להעברת מידע יינתן רק לאחר בחינה מדוקדקת של המורשים לאשר בקשות להעברת מידע (מנהל המאגר, הממונה והיועץ המשפטי), ובכך אישור זה יהווה מדרג נוסף בטרם תתאפשר העברת מידע בין גופים ציבוריים.

נושא הבחינה

בפניית רמו"ט נתבקשו הגופים הנבדקים לפרט:

א. למי כפוף הממונה על אבטחת המידע בתוך הארגון?
ב. מה תפקידו הראשי בארגון?
ג. מה הכשרתו המקצועית?

שאלות אלו נועדו לבחון את מידת התאמתם של הממונים לתפקידם בהתייחס לרקע המקצועי שלהם, למעמדם הארגוני בקשר למשאבים והסמכויות המוקצים להם וכן לשאלת ניגודי עניינים פוטנציאליים במהלך תפקודם.

עיקרי הממצאים

בפרק זה נציג ניתוח ויזואלי וכמותי של המענים על השאלונים שעסקו בממונה על אבטחת המידע. ניתוח זה מבחין בין גופים ציבוריים גדולים (דוגמת משרדי ממשלה גדולים, עיריות גדולות או תאגידים סטטוטורים גדולים) וגופים ציבוריים קטנים (כגון מועצות מקומיות, יחידות סמך ממשלתיות קטנות, אגפים במשרדים וכד').

ב- 4 גופים מונה ממונה אבטחת מידע רק לאחר קבלת השאלון של רמו"ט. ואלה הם: משרד הפנים, הרשות לשיקום האסיר, שירות התעסוקה, מועצה אזורית אבו בסמה. שני ארגונים (הכנסת והמוסד לביטוח לאומי) מסרו את תשובותיהם מאוחר מאוד, ועל כן אלה לא נכנסו לדו"ח.

לעניין מינויו של ממונה על אבטחת מידע, הרי שברובם המכריע של הארגונים הגדולים דווח על מינוי כאמור (18 מתוך 20 ארגונים). גם רב הארגונים הקטנים דווחו כי קיים ממונה כאמור, אך באחוז נמוך יותר (6 מתוך 8 ארגונים).

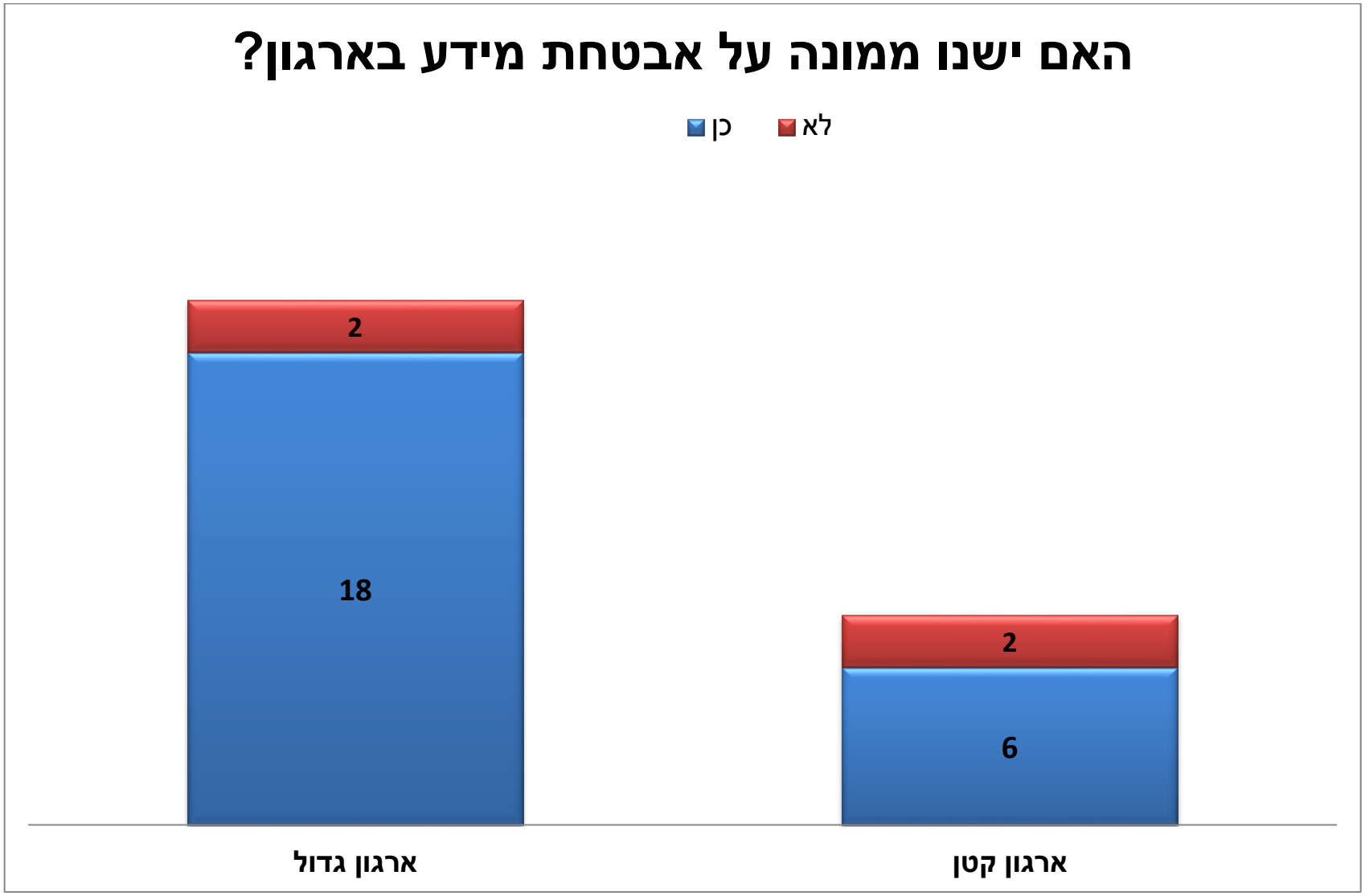
הכשרתם של ממוני אבטחת המידע בארגונים מגוונת, ורובם בעלי רקע כלשהו באבטחת מידע וטכנולוגיה (19 מתוך 24), ומיעוטם (5) חסר השכלה רלוונטית. חוסר ההשכלה הרלוונטית בולט בארגונים קטנים (3 מתוך 6).

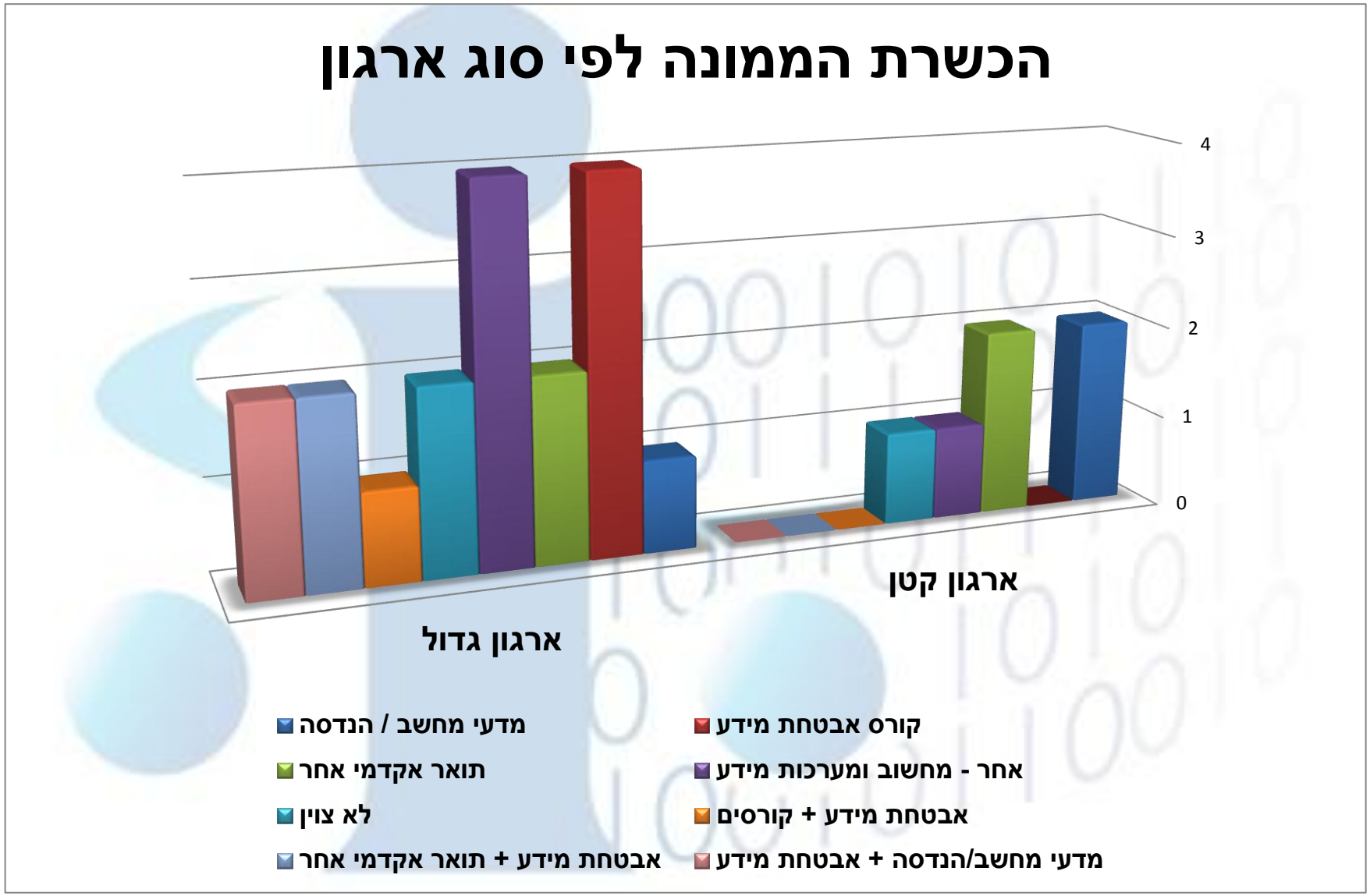
בדרך כלל ממונה אבטחת המידע כפוף למנכ"ל, לסמנכ"ל למנהל או למנהל אגף מערכות מידע. במקרים בודדים הכפיפות היא לקצין הבטחון.

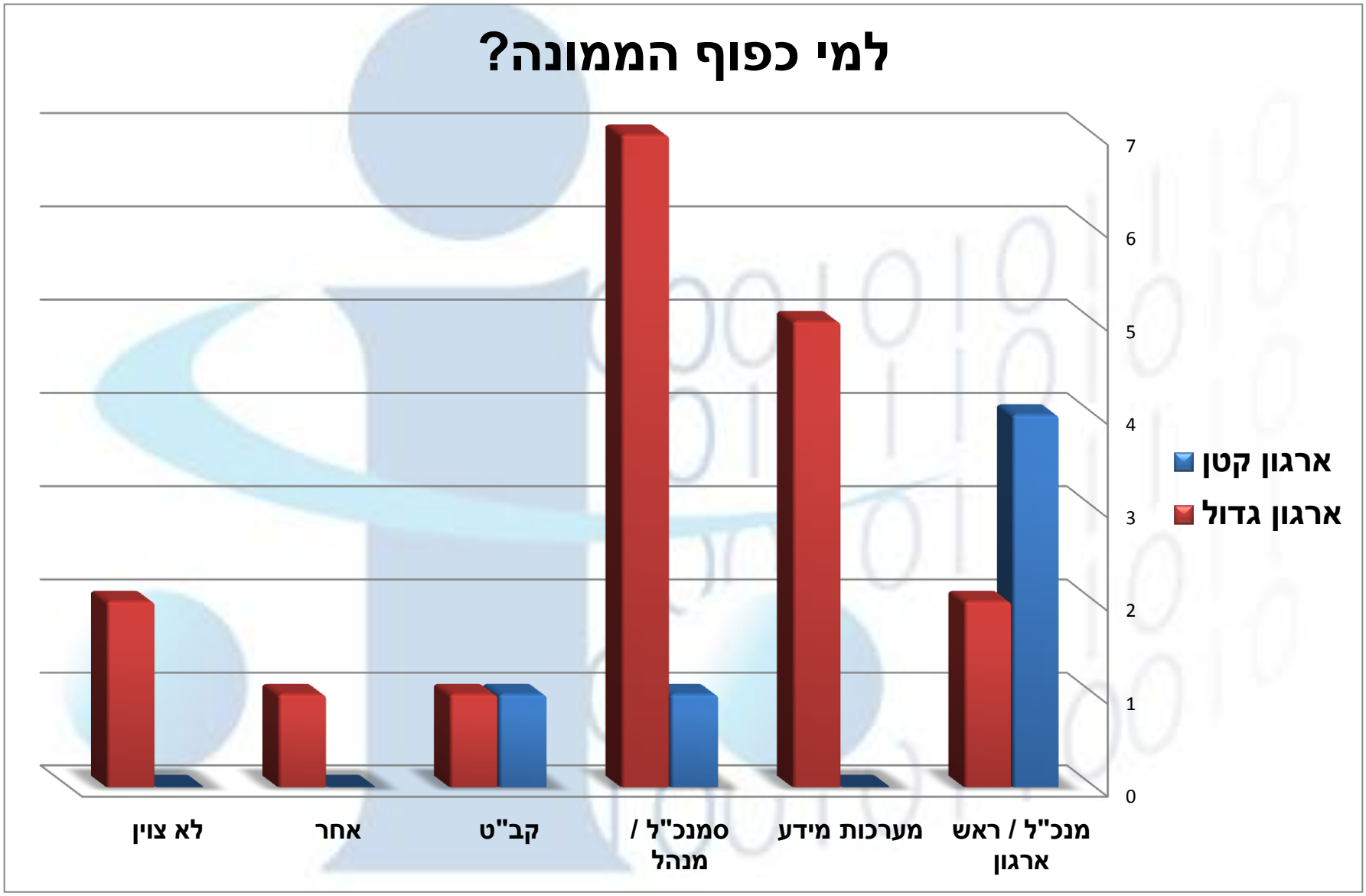
בכל הארגונים הקטנים, ממונה אבטחת המידע ממלא תפקיד נוסף. בארגונים גדולים, רוב הממונים ממלאים גם תפקיד נוסף (11 מתוך 15).

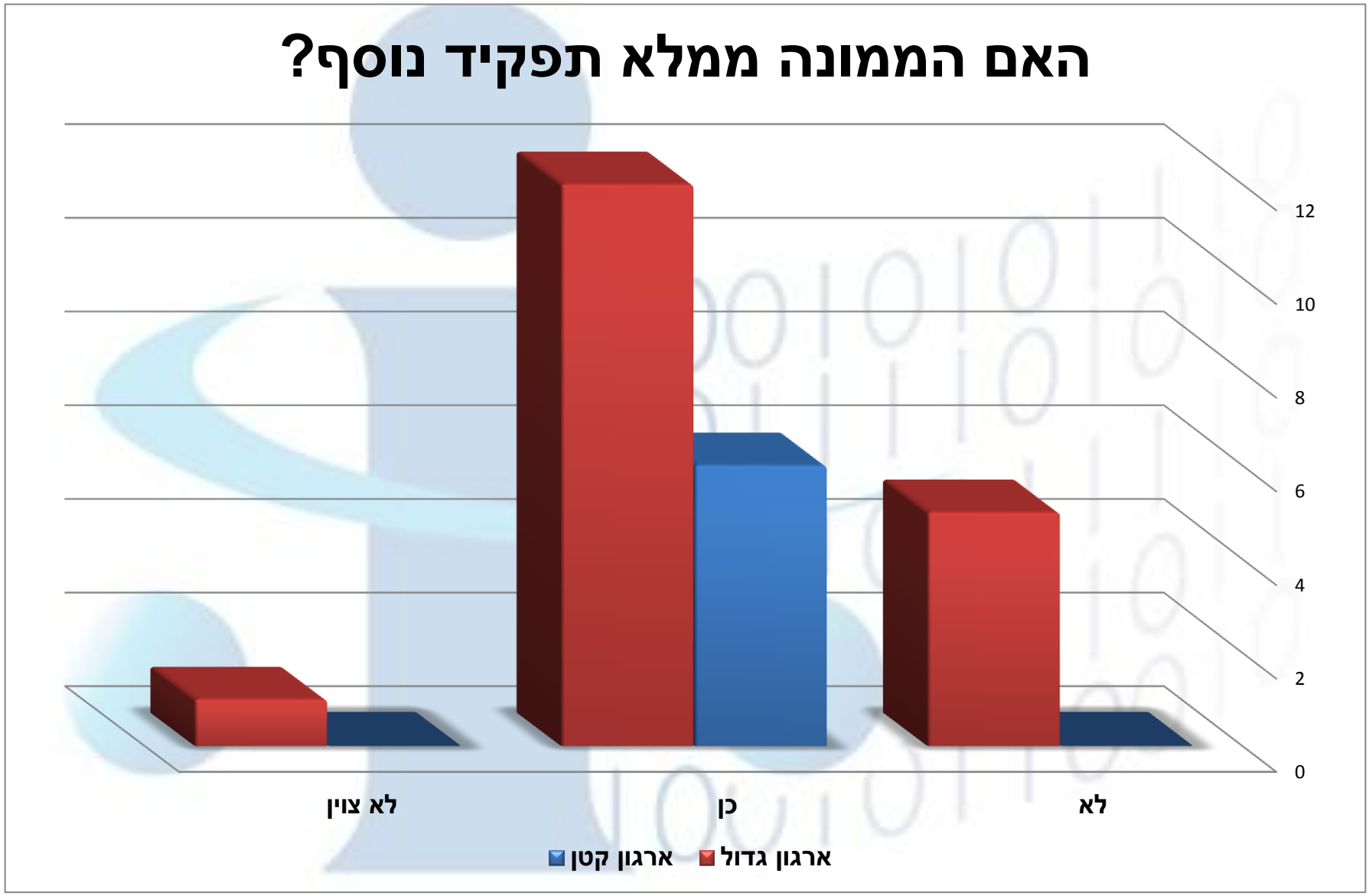
ברוב הארגונים, גדולים כקטנים, הממונה פועל לבדו, מבלי שיהיו לו כפיפים. במספר ארגונים גדולים יש מחלקות משמעותיות בנות 4-6 עובדים.

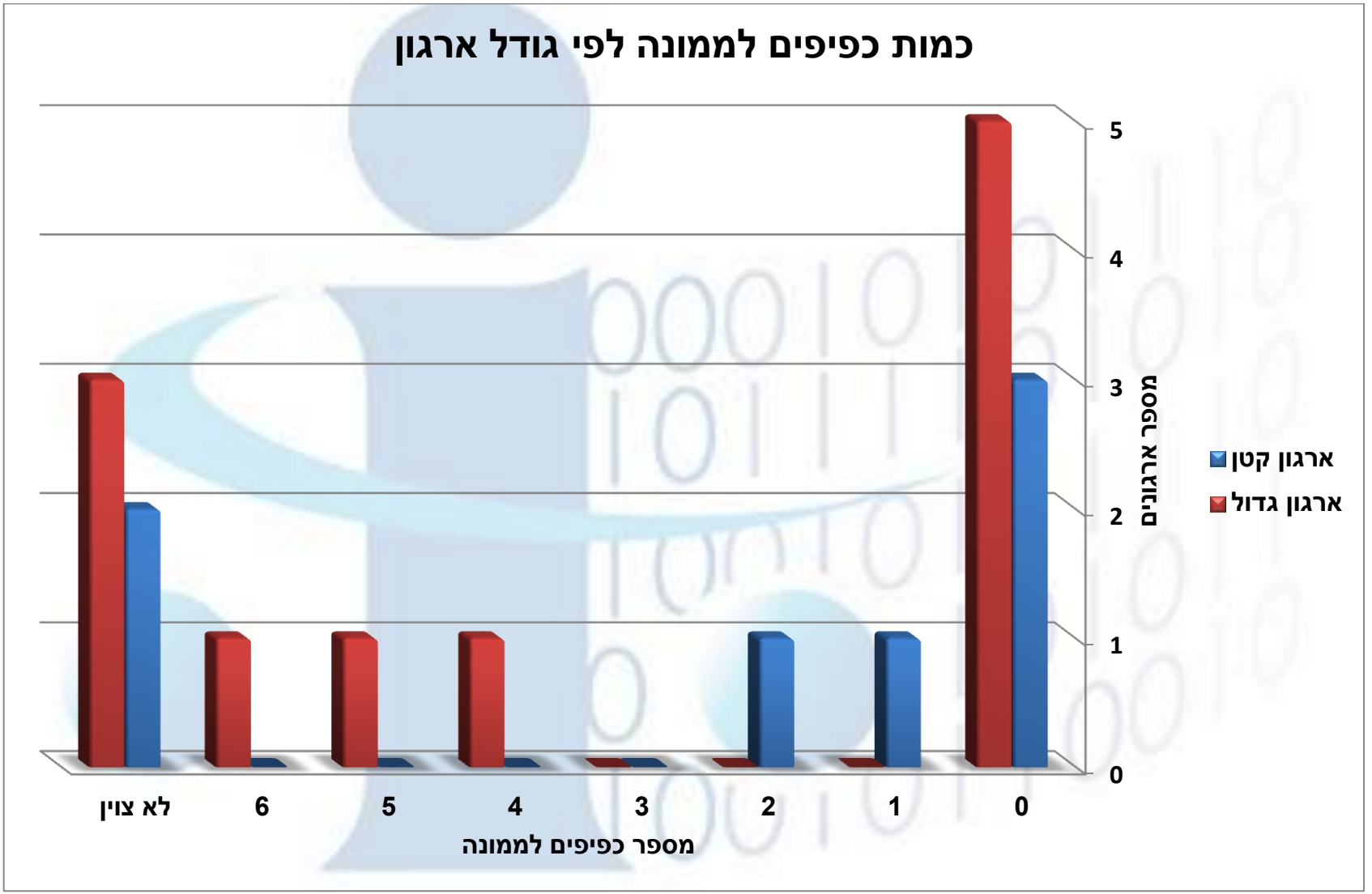
בעמודים הבאים יוצגו הממצאים באופן מפורט.


האם ישנו ממונה על אבטחת מידע בארגון?
כן
לא
2
18
2
6
ארגון גדול
ארגון קטן


הכשרת הממונה לפי סוג ארגון
4
3
2
1
0
ארגון קטן
ארגון גדול
מדעי מחשב / הנדסה
קורס אבטחת מידע
תואר אקדמי אחר
אחר - מחשוב ומערכות מידע
לא צוין
אבטחת מידע + קורסים
אבטחת מידע + תואר אקדמי אחר
מדעי מחשב/הנדסה + אבטחת מידע


למי כפוף הממונה?
7
6
5
4
3
2
1
0
ארגון קטן
ארגון גדול
מנכ"ל / ראש ארגון
מערכות מידע
סמנכ"ל / מנהל
קב"ט
אחר
לא צוין


האם הממונה ממלא תפקיד נוסף?
12
10
8
6
4
2
0
לא צוין
כן
לא
ארגון קטן
ארגון גדול


כמות כפיפים לממונה לפי גודל ארגון
מספר ארגונים
0
1
2
3
4
5
ארגון קטן
ארגון גדול
לא צוין
6
5
4
3
2
1
0
מספר כפיפים לממונה

משמעות והמלצות

ממונה אבטחת המידע - כללי

מטרת המידע שהתבקש בשאלון הייתה לקבל תמונה על אודות המימוש בפועל של תפקיד הממונה, נוכח היות הגדרת "אבטחת מידע" כללית ועמומה, אי הקביעה מראש את רמת הידע ותחומי הידע הנדרשים לתפקיד (ידע משפטי, ידע טכני, ידע ניהולי) ומהות ביצוע תפקידו של ממונה אבטחת המידע בפועל.

המידע שהתקבל בפיקוח מעיד על חוסר אחידות בסוגיות של הכשרתו של ממונה אבטחת המידע, כפיפותו המקצועית והמשאבים העומדים לרשותו למילוי תפקידו.

אחריותו של הממונה

בסעיף 17 לחוק נכתב: "*בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת במידע שבמאגר המידע*". בתקנה 1 נכתב כי ממונה אבטחה הוא אדם שמונה לפי סעיף 17ב לחוק או אדם שמנהל המאגר קבע כי הוא אחראי על אבטחת המידע. בתקנה 3(ב) נכתב כי מנהל מאגר אחראי לאבטחת המידע במאגר המידע. בעוד שתפקיד מנהל מאגר מידע מוגדר בחוק ובתקנות, הרי **שלממונה על אבטחת מידע אין קביעה והגדרת תפקיד נוסף על חובת המינוי.**

לכתב מינויו של הממונה, המגדיר את מהות התפקיד וחלוקת האחריות, חשיבות רבה מעבר למישור הפורמאלי. עם זאת, מהפיקוח עולה כי מרבית הגופים אינם מיחסים חשיבות לכך ואינם מסדירים את פעילותו של הממונה.

אנו סבורים שיש להבהיר את תפקידם של בעל המאגר, מנהל מאגר המידע ושל הממונה לגבי אבטחת מאגר המידע, בקביעת השימוש במאגר המידע, מדיניות הפרטיות של הארגון וחלוקת האחריות לטיפול בנושאים השונים, כאמור בנספח ב' למסמך זה. **אנו ממליצים לבחון האם נדרשים תיקוני חקיקה או תקנות כדי ליישם את האמור.**

עוד אנו ממליצים כי בקביעת נהלי עבודת הממונה תהיה התייחסות, בין השאר, לנושאים הבאים (להרחבה ראו נספח ב' למסמך זה):

א. דרך הכנת תכנית עבודה שנתית ורב-שנתית;

ב. דרך עריכת בדיקות ופיקוח;

ג. הליכי המעקב אחר תקלות וליקויים שדווחו על ידי הממונה;

ד. הגדרת הגורם המוסמך לאשר סיום טיפול בתקלה או דיווח;

ה. אופן תיעוד וסיכום הממצאים.

הכשרתו של ממונה אבטחת המידע

מהממצאים אודות הכשרתם של ממוני אבטחת המידע עולה, די בבירור, כי התפקיד נתפס כתפקיד טכנולוגי בתחום אבטחת המידע המעשית. לא זוהתה הכשרה של ממונים בסוגיות הרחבות של הגנת פרטיות, לרבות לא בשאלות של לגיטימיות השימוש במידע על ידי הארגון לצורך תפקודו.

על הממונה להיות בעל ידע מקיף על אודות השימושים שעושה הגוף הציבורי במאגר המידע, עסקיים וטכנולוגיים כאחד. לממונה צריכה להיות יכולת שליטה בכל הקשור להרשאות הגישה של משתמשים למידע אישי, באמצעות המערכות הממוחשבות של הארגון, בגישה מקומית ובגישה מרחוק, והשימושים שהם עושים במידע זה. להרחבה בעניין כישוריו, תפקידו וחובותיו של הממונה, ראו נספח ב' למסמך זה.

המלצתנו היא כי הממונה יהא ברמת ראש אגף או ידווח אליו ישירות, ויהא בעל רקע נרחב בתחום פעילות הארגון והכרות עם היבטי הפרטיות הנוגעים לארגון. ממונה אבטחת המידע לא אמור למלא תפקיד נוסף, בפרט כזה שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו.

מאחר וכל הגופים הציבוריים במדינת ישראל, לרבות כלל משרדי הממשלה ויחידות הסמך חייבים במינוי ממונה על פי החוק, הננו ממליצים להגדיר עיסוק זה באופן סדור על ידי נציבות שירות המדינה, לגבי עובדי מדינה, ומשרד הפנים ומרכז השלטון המקומי לגבי עובדי רשויות מקומיות. בנוסף, נדרש לתקצב את איוש המשרות הללו בכלל הגופים הציבוריים, שכן מדובר בחובה חוקית. רמו"ט תפנה בעניין לנציב שירות המדינה ולמנכ"ל משרד הפנים בבקשה להנעת עבודת מטה בנושא.

ו. נספח א' – הנחיית המשנה ליועמ"ש – העברות מידע בין גופים ציבוריים

מדינת ישראל
משרד המשפטים

המשנה ליועץ המשפטי לממשלה
(ייעוץ)

ט"ז אדר, תשס"ו
16 מרץ, 2006

תיקנו: 117-95 הגנת הפרטיות

אל : היועצים המשפטיים במשרדי הממשלה

שלום רב,

הנדון: העברת מידע בין גופים ציבוריים

1. פרק ד' לחוק הגנת הפרטיות מסדיר את נושא מסירת מידע או ידיעות מאת גופים ציבוריים. הכלל הוא, כפי שמוסדר בסעיף 23ב לחוק הגנת הפרטיות, התשמ"א-1981 (להלן – **החוק**) כי מסירת מידע מאת גוף ציבורי אסורה למעט במקרים הבאים :
   א. המידע פורסם לרבים או הועמד לעיון הרבים על פי סמכות כדין (סעיף 23ב(א) לחוק) ;
   ב. האדם אשר המידע מתייחס אליו נתן הסכמתו למסירה (סעיף 23ב(א) לחוק) ;
   ג. מסירת המידע או קבלתה נעשתה על ידי רשות בטחון לשם מילוי תפקידה, ובלבד שמסירת המידע או קבלתה לא נאסרה בחיקוק (סעיף 23ב(ב) לחוק) ;
   ד. מסירת המידע היא בין גופים ציבוריים ועומדת בדרישות סעיף 23ג לחוק.

2. סדרי העברת המידע בין גופים ציבוריים הוסדרו בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים) התשמ"ו-1986 (להלן – **התקנות**).

3. בבג"צ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים ואח'**[1] דן בית המשפט העליון בחוקיות ההסדר הקיים להעברת המידע הממוחשב ממרשם האוכלוסין במשרד הפנים לגופים ציבוריים ופרטיים שלא אגב שאילתות פרטניות. ביהמ"ש פסק כי על רשויות המדינה להגביר את הפיקוח, באמצעות תקנות או הנחיות, על הגישה למאגרי המידע השונים, וזאת הן בהיבט של כמות העובדים בעלי הרשאת גישה למידע המצוי במאגרים והן בהיבט של היקף המידע המועבר בין גופים ציבוריים לצורך מילוי עבודתם. בנוגע לגופים פרטיים ביהמ"ש קבע כי העברת המידע צריכה להיות מעוגנת בחקיקה מתאימה.

[1] בג"צ 8070/98 **האגודה לזכויות האזרח נ' משרד הפנים ואח'**, פ"ד נח(4) 842.

רח' צלאח א-דין 29, ת.ד. 1087, ירושלים 91010 ☎ 02-6466673, 02-6466592 פקס. 02-6466766

4. בעקבות פסק הדין הוחלט לתקן את הוראות תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986.

5. מכתב זה בא להנחות את הגופים הציבוריים בעקבות שינוי התקנות, אשר פורסם בק"ת תשס"ה, עמ' 968, ונכנס לתוקף בתאריך 19/12/2005.

<u>הוועדה להעברת מידע</u>

6. סעיף 3א לתקנות קובע כי בכל גוף ציבורי אשר מוסר מידע או מקבל מידע, ימנה המנכ"ל של אותו גוף ועדה להעברת מידע (להלן – **הוועדה**). יו"ר הוועדה יהיה המנכ"ל או סגנו או עובד בכיר הכפוף למנכ"ל ישירות. מספר חברי הוועדה לא יפחת משלושה, כאשר חובה למנות בין חברי הוועדה את היועץ המשפטי של הגוף הציבורי או נציגו ועובד שתחום עיסוקו הוא ניהול מאגר מידע ואבטחתו.

7. תפקידה של הוועדה הוא כפול: ראשית, בחינה של בקשות למסירת מידע מאת הגוף הציבורי וכן בקשות לקבלת מידע של הגוף הציבורי מאת גוף ציבורי אחר. שנית, קביעת הוראות לעניין הגישה למאגרי המידע שברשות הגוף הציבורי, אשר יבטיחו את השמירה על המידע המצוי במאגרים.

א. קביעת כללי גישה

8. על הוועדה לקבוע קריטריונים, בנוגע לכל מאגר מידע המצוי ברשות הגוף הציבורי, ובין היתר -
   - מיהם בעלי התפקידים הזכאים לעיין במידע
   - אופן הגישה למאגר
   - צמצום המידע אליו קיימת גישה למינימום הנדרש
   - דרכי הבקרה
   - קבלת דיווח תקופתי על אופן יישום הוראות הוועדה

9. את כללי הגישה יש לפרסם לפי הוראת סעיף 6 לחוק חופש המידע, התשנ"ח-1998 (להלן – **חוק חופש המידע**).

ב. בחינת בקשות לקבלת מידע

10. בקשה לקבלת מידע של גוף ציבורי, על גבי טופס א' המצוי בתוספת לתקנות, תועבר לאישור הוועדה לאחר שבעלי התפקידים באותו גוף ציבורי אישרו את הבקשה, אך <u>בטרם</u> העברת הבקשה לגוף הציבורי ממנו נתבקש המידע. על הוועדה לבחון כי המידע המבוקש אכן נדרש, ובאופן בו הוא נתבקש, וכי מובטח שהגישה למידע תהיה מצומצמת ומפוקחת.

ג. בחינת בקשות למסירת מידע

<u>גופים פרטיים</u>

11. אין לאשר מסירת מידע לגוף שאיננו גוף ציבורי כהגדרתו בחוק, אלא כאשר מתקיימת אחת מהחלופות הבאות:

1. קיים חיקוק ספציפי המתיר את מסירת המידע;
2. ישנה הסכמה של האדם נשוא המידע להעברתו. לעניין זה יש לבחון את מהות ההסכמה והאם כללה הסכמה בדבר העברת המידע לאותו גוף פרטי.

<u>גופים ציבוריים</u>

12. הוועדה תבחן בקשות למסירת מידע מאת הגוף בו היא יושבת רק לאחר שהוגש טופס א' המצוי בתוספת לתקנות, ולאחר שהבקשה אושרה על ידי מנהל מאגר המידע, הממונה על האבטחה והיועץ המשפטי של הגוף ממנו נתבקש המידע. להלן אופן בדיקת הבקשות הן על ידי בעלי התפקידים הרלוונטים והן על ידי הוועדה:

1. **עמידה באישורים הנדרשים לפי התקנות** – האם הבקשה הוגשה על גבי טופס א' שאושר על ידי כל הגורמים הרלוונטים בגוף המבקש (מנהל מאגר המידע, הממונה על האבטחה, היועץ המשפטי והוועדה);
2. **תנאי מקדים מעמדו של הגוף מבקש המידע** - האם הוא "גוף ציבורי" כהגדרתו בסעיף 23 לחוק (משרד ממשלתי, מוסד מדינה, רשות מקומית, גוף אחר הממלא תפקידים ציבוריים על פי דין או גוף שנקבע בצו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו-1986).
3. **מניעה למסירת המידע** – האם מסירת המידע לא נאסרה בחיקוק או בעקרונות של אתיקה מקצועית, והאם לא הותנתה מסירתו בכך שהמידע לא יימסר לאחר.
4. **תנאי מסירת המידע** – סעיף 23ג יוצר הבחנה בתנאי מסירת המידע בין בקשות לקבלת מידע מאת משרד ממשלתי או מוסד מדינה (ס"ק (2)) לבין בקשות לקבלת מידע מיתר הגופים הציבוריים (ס"ק (1)).

כאשר הבקשה לקבלת מידע היא מאת משרד ממשלתי או מוסד מדינה יש לבחון האם "מסירת המידע דרושה למטרת ביצוע כל חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו".

כאשר הבקשה למסירת מידע היא מאת גוף ציבורי אחר, יש לבחון האם התקיימו שני אלה:

א. "מסירת המידע היא במסגרת הסמכויות או התפקידים של מוסר המידע";

ב. "היא דרושה למטרת ביצוע חיקוק או למטרה במסגרת הסמכויות או התפקידים של מוסר המידע או מקבלו".

או לחילופין, האם הגוף הציבורי אשר ביקש את המידע רשאי לדרוש את אותו מידע על פי דין מכל מקור אחר.

5. **דרישת המידתיות והסבירות** – מכיוון שיש למלא את הוראות החוק בהתאם להוראות חוק יסוד: כבוד האדם וחירותו יש לבחון כי הבקשה מידתית וסבירה על פי המבחנים הבאים:

א. הבקשה לקבלת המידע מתאימה לשם יישום המטרה לשמה נדרש המידע, ויש קשר הגיוני בין הבקשה למטרה;

ב. העברת המידע באופן המבוקש היא האמצעי הפחות פוגע מבין מגוון האמצעים האפשריים למימוש אותה מטרה;

ג. קיים יחס סביר בין המטרה לבין הפגיעה שנגרמת בזכות לפרטיות לשם השגתה.

בבחינת מבחנים אלו, יש לתת את הדעת לרגישות המידע האישי אותו מבקשים לקבל. ככל שהמידע רגיש יותר, יש צורך בהגנה רבה יותר על הפרטיות;

6. **בחינת אמצעי האבטחה בגוף המקבל** – על הוועדה לבחון מהם אמצעי האבטחה של מאגר המידע אליו יועבר המידע המבוקש בשלושה היבטים עיקריים:

א. אמצעי מיחשוב – סיסמאות כניסה למערכת, מידור בתוך מאגר המידע בין פרטי מידע שונים, אמצעי הגנה על חדירה מבחוץ וכד';

ב. אמצעים פיסיים – מיקום המאגר, הגישה הפיסית אליו וכד';

ג. אמצעי בקרה – תדירות הבדיקות שנעשות למניעת חדירה למאגר המידע מבחוץ, אופן הפיקוח על השימוש שנעשה במידע על ידי מורשי הגישה וכד'.

7. **בחינת מורשי הגישה** – מי יהיו בעלי התפקידים שתינתן להם רשות לעיין במידע שנמסר, מספרם ולצורך איזו מטרה ניתנת להם הגישה למידע.

8. **בחינת הטיפול במידע עודף** – כיצד משמידים מידע עודף, אשר נמסר באופן נלווה לבקשה העיקרית, ומה עושים במידע ישן שאין בו עוד שימוש.

היחס בין הוועדה לממונה על האבטחה ולמנהל המאגר

13. תפקיד הוועדה להעברת מידע לפקח על התנהלות הגוף הציבורי בו היא עובדת בכל הנוגע להעברת מידע המצוי בידי הגוף הציבורי. העובדה כי המדינה, ככלל, מחזיקה בידיה מידע רב ורגיש אודות הציבור מחייב אותה להשתמש בזהירות רבה במידע שבידה. לצורך כך, נדרש פיקוח בתחום זה, במיוחד כאשר ישנו שיתוף במידע בין רשויות שונות.

14. בטרם הועבר התיקון בתקנות, כל מנהל מאגר ויועץ משפטי קבעו את הסטנדרטים לניהול המאגר הן בהיבט של הרשאות הגישה והן בהיבט של שיתוף המידע בין גופים ציבוריים. התיקון מנסה ליצור אחידות בתוך הגוף הציבורי, כך שכל ממלאי התפקידים הנוגעים בדבר יהיו כפופים לוועדה בשני היבטים אלה. בנוסף, מעתה הפיקוח והבקרה בנושא זה יהיו של הדרג הבכיר בכל גוף ציבורי.

15. כפי שצוין לעיל, אישור הוועדה להעברת מידע ינתן רק לאחר בחינה מדוקדקת של המורשים לאשר בקשות להעברת מידע (מנהל המאגר, הממונה על האבטחה והיועץ המשפטי), ובכך אישור זה יהווה מדרג נוסף בטרם תתאפשר העברת מידע בין גופים ציבוריים.

<u>החובה לפרסם רשימה של הגופים אליהם מועבר מידע דרך קבע</u>

16. שינוי נוסף שנעשה בתיקון האחרון היא החובה המוטלת על מנהל המאגר בגוף ציבורי לערוך רשימה של כל הגופים, פרטיים וציבוריים כאחד, שאליהם נמסר מידע דרך קבע ממאגר המידע של הגוף הציבורי. הרשימה לא תכלול גופים המנויים בסעיף 13(ה) לחוק. הרשימה תכלול את הגוף הציבורי אליו מועבר המידע, תדירות העברת המידע או עדכונו, אופן העברת המידע (על פי בקשות פרטניות או באצווה) וכן סוג המידע המועבר.

17. הרשימה תעמוד לעיון הציבור בהתאם להוראות סעיף 6(ב) לחוק חופש המידע המסייג וקובע כי במידה שאחד מהסייגים המנויים בסעיף 9 לחוק חופש המידע (כגון בטחון המדינה, פגיעה ביחסי חוץ וכד') מתקיים גם לגבי מידע מסוים המצוי ברשימה, אין לפרסם מידע זה.

18. פרסום הרשימה יהיה באתר האינטרנט של הגוף הציבורי, ובאין אתר אינטרנט - במשרד הראשי ובמשרדיו המחוזיים, ככל שישנם.

<u>סיכום</u>

19. יישום התקנות בנוסחן החדש, נועד להגביר את הפיקוח והבקרה על העברת מידע פרטי בין גופים ציבוריים, הן על ידי פיקוח הדוק יותר של הדרג הבכיר בכל גוף ציבורי, והן על ידי שקיפות כלפי הציבור לגבי מידע המועבר עליו דרך קבע על ידי הגופים הציבוריים. יש לקוות ששני המנגנונים חללו יגרמו לאכיפה מוגברת של הוראות חוק הגנת הפרטיות ולזהירות הנדרשת בגינן.

ב ב ר כ ה,

מלכיאל בלס
משנה ליועץ המשפטי לממשלה

העתק: היועץ המשפטי לממשלה
גב' דלית דרור – כאן
גב' רבקי דב"ש - כאן

ז. נספח ב': אחריות בעל המאגר והממונה לאבטחת המידע

מטרת נספח זה היא לקבוע את חלוקת האחריות הראויה בין בעל המאגר והממונה לאבטחת המידע במאגר ולהגדיר את הכישורים והאחריות של הממונה האמור בנספח מבוסס על ניסיונה המצטבר של רמו"ט בתחום זה.

קביעת אחריות לאבטחת מידע

מוצע לקבוע כי האחריות הראשונית למאגר היא של בעל המאגר, אשר באחריותו להגדיר במסמך, לכל הפחות, את כל העניינים האלה:

א. תיאור כללי של פעילות האיסוף, השימוש והעיבוד של המידע לצורך פעילות בעל המאגר;

ב. תיאור המטרות המותרות של פעולות עיבוד המידע;

ג. תיאור של סוגי המידע השונים הכלולים במאגר המידע, וכן הערכת הרגישות של כל סוג מידע. הערכת רגישות תבוצע בהתאם להערכת בעל המאגר את מידת הנזק לפרטיות נושא המידע בשל פגיעה באבטחת המידע במאגר;

ד. פירוט לעניין ביצוע פעולות עיבוד מידע באמצעות מחזיק;

ה. הסיכונים המרכזיים לפגיעה באבטחת המידע במאגר בשים לב לסוגו ולבדיקת הרגישות ואופן ההתמודדות עם סיכונים אלה;

ו. שמו של מנהל המאגר ושמו של הממונה והגדרת תפקידיו.

הגדרת הכישורים הנדרשים מהממונה

א. על הממונה להיות בעל יכולת, ידע ומומחיות בתחום פעילות הארגון, תהליכיו ועבודתו וכן בתחום הגנת המידע.

ב. על הממונה להיות בעל יכולת ורצון להרחיב אופקים בתחומים בהם נדרשת מומחיות גדולה יותר. השכלה משפטית לממונה, ובפרט בנושאי הגנת פרטיות במידע, יכולה להוות יתרון בולט.

ג. לממונה נדרש ידע בסיסי בטכנולוגיית מידע.

ד. על הממונה להיות בעל יכולת עמידה והתמודדות עם לחצים.

ה. רצוי להגדיר מראש את תקופת כהונתו של הממונה, ולקחת בחשבון שנדרשת תקופה ארוכה יחסית על מנת לאפשר לו לתכנן ולפעול בהתאם לתכניותיו באופן עצמאי.

ו. מומלץ כי מינוי הממונה יעשה על ידי מנכ"ל הארגון.

ז. יש להגדיר נהלים לביטול מינוי ממונה או החלפתו.

ח. רצוי כי הממונה לא ימלא תפקיד נוסף בארגון. עם זאת, בארגונים קטנים בהם אין מקום לממונה בתקן מלא, והממונה ממלא תפקיד נוסף, יש להבטיח שאין בשילוב זה ניגוד עניינים כלשהו.

ט. מוצע כי הממונה יפעל בתיאום עם בעל המאגר ומנהל המאגר ובכפוף למסמך הגדרות המאגר. להלן המלצות לקביעת תפקידיו ותחומי אחריותו:

י. יש להגדיר את התפקיד כ"ממונה על הגנת מידע אישי", שמסגרת תפקידו הוא קביעת צרכי הפרטיות בארגון, הגדרת הפערים, העברת המידע למקבלי ההחלטות ובעלי התפקיד האמונים על אבטחת המידע וסיוע בכתיבת נהלים בנושא.

יא. על הממונה לוודא שהארגון עומד בחוק, בתקנות ובהנחיות הנוגעות להגנה על מידע.

יב. על הממונה לנטר, לבקר ולבדוק, באופן תכוף, את פעולות עיבוד המידע שהארגון מבצע. כמו כן, עליו לתת מענה, על סמך מומחיותו וניסיונו, לבעיות שהארגון נתקל בהם בתחום הגנת המידע בשלבים המוקדמים.

יג. על הממונה להוות חלק בלתי נפרד בתהליכים בארגון, תוך שמירה על דרך ידידותית לשימוש ועיבוד מידע.

יד. על הממונה לקבוע את מדיניות הפרטיות של הארגון ולהביאה לאישור הוועדה. מדיניות זו תכלול, לכל הפחות את העניינים האלה:

- הגדרה של כלל הסיכונים האיומים העומדים מול הארגון;
- מיפוי השימושים המותרים בפעולות הארגון, רשימת הגורמים המורשים והיקף הרשאתם;
- מיפוי סיכונים מעודכן למאגרי המידע של הארגון;
- הוראות קבע לעניין אופן העמידה של הארגון בהוראות החוק וחוק הגנת הפרטיות וחובותיהם של בעלי התפקידים השונים;
- עיקרי תפקידו של הממונה על הפרטיות וסגניו ככל שמונו;
- אופן מימוש זכויות במידע המצוי במאגר (לדוגמה זכות עיון ותיקון כאמור בסעיפים 14-13 לחוק).

טו. על הממונה לפקח על כך שהגוף פועל בהתאם למכלול ההוראות וההנחיות הקשורות בשמירה על הפרטיות, בהתאם לתוכנית עבודה שנתית ותוך ביצוע בדיקות תקופתיות.

טז. הממונה יכין מפרט בדיקה ופיקוח לכל מערכת, סיכון או תהליך הקשור בעיבוד מידע, ויעדכן אותו בהתאם לצורך ולשינויים הטכנולוגיים ברשות. במפרט הבדיקה יהיה, בין השאר, התייחסות לחוקים, תקנות והנחיות רלוונטיות לנושא פעולת הארגון.

יז. הממונה יוודא, ככל הניתן מראש, שפעילות המאגר ומערכותיו בנויים באופן שיפחית את סיכוני השימוש במידע שבמאגר, ואת סיכוני הפגיעה בפרטיותם של נשואי המידע.

יח. הממונה יהיה בעל גישה ישירה למערכות הבקרה והניטור המתעדות את פעולות העיבוד במאגרי המידע של הארגון (ובכלל זה, גישה לכל החדרים בארגון, כל מאגרי הנתונים וכלל מערכות הארגון). כמו כן, הממונה יוכל להגדיר אירועים ספציפיים אותם הוא מבקש לתעד.

יט. הממונה יקבע מערך הדרכות תקופתי לתפקידי העובדים בגוף ובכלל זה הדרכות כלליות לכלל העובדים.

כ. הממונה מהווה גורם לקבלת כל הפניות, התלונות והשאלות הנוגעות להגנה על המידע בתוך הארגון ומחוצה לו.

כא. בסמכות הממונה לבצע חקירות לפי שיקול דעתו הבלעדי, במידה ועולה חשד לפגיעה במידע. כמו כן, באחריותו להציע פתרונות לבעיות שנחשפות בחקירות.

כב. היות ועל הממונה להיות גוף עצמאי לחלוטין, ומאחר ולצורך עבודתו, יש לפעמים צורך במשאבים נוספים, מומלץ להעמיד לרשותו תקציב נפרד על מנת שלא תפגע עבודתו ושיקול דעתו במידה ויאלץ בכל פעם מחדש לבקש אישור לפעולה כזו או אחרת.

כג. במידה ומדובר בארגון גדול, רצוי למנות סגן ממונה אשר ייהנה מאותם סמכויות ויהיה כפוף לממונה.

כד. יש לוודא כי לא ניתן יהיה לפטר את הממונה כתוצאה מפעילותו בתחום הגנת המידע (בתנאי כי הוא מבצע את עבודתו כנדרש).

ח. נספח ג': רשימת הגופים המפוקחים

מגזר	סידורי	הגוף	חלוקת הארגונים ע"פ גודל	ענה	לא ענה
מוסדות מדינה	1	הכנסת	גדול	✓[6]	
	2	צה"ל	גדול	✓	
	3	משטרת ישראל	גדול	✓	
משרדי ממשלה	4	האוצר	גדול	✓	
	5	החינוך	גדול	✓	
	6	המשפטים	גדול	✓	
	7	הפנים	גדול	✓	
	8	הבריאות	גדול		✓
	9	התמ"ס	גדול	✓	
	10	קליטת עליה	גדול	✓	
רשויות מקומיות	11	תל אביב	גדול	✓	
	12	ירושלים	גדול	✓	
	13	חיפה	גדול	✓	
	14	מ.אזורית מטה יהודה	קטן	✓	
	15	מ.אזורית אבו בסמה	קטן	✓	
	16	מ.אזורית משגב	קטן	✓	
	17	מ.מקומית דאלית אל כרמל	קטן		✓
	18	מ.מקומית זכרון יעקב	קטן	✓	

[6] התשובה הוגשה באיחור רב, בסמוך לסיום כתיבת הדו"ח ונתוניה לא נכללו.

תאגידים סטטוטוריים	19	רשות המיסים	גדול	✓	
	20	בנק ישראל	גדול	✓	
	21	האפוטרופוס הכללי	קטן	✓	
	22	המוסד לביטוח לאומי	גדול	✓[7]	
	23	הרשות הלאומית למלחמה בסמים ואלכוהול	קטן	✓	
	24	הרשות לשיקום האסיר	קטן	✓	
	25	מגן דוד אדום	גדול	✓	
	26	שרות התעסוקה	גדול	✓	
גופים ציבוריים שנקבעו בצו	27	בית חולים תל השומר	גדול	✓	
	28	בית חולים אברבנאל	גדול		✓
	29	מכבי שרותי בריאות	גדול	✓	
	30	קופת חולים לעובדים לאומיים	גדול	✓	
	31	אוניברסיטת תל אביב	גדול		✓
	32	האוניברסיטה העברית ירושלים	גדול	✓	
	33	ארגון נכי צהל	קטן	✓	
	34	הסוכנות היהודית	גדול	✓	

[7] התשובה הוגשה באיחור רב, בסמוך לסיום כתיבת הדו"ח ונתוניה לא נכללו.