תאריך: 17 מרץ, 2011
י"א אדר ב, תשע"א
סימוכין: 015-99-2010-001034

לכבי
ועדת חוקה, חוק ומשפט
כנסת ישראל

לכבי
ועדת הכלכלה
כנסת ישראל

לכבי
ועדת המדע והטכנולוגיה
כנסת ישראל

לכבי
שר המשפטים פרופ יעקב נאמן
משרד המשפטים

נכבדי,

שלום רב,

הנדון: **<u>דין וחשבון על פעילות הרשות למשפט, טכנולוגיה ומידע בשנת 2009</u>**

1. אני מתכבד בזאת להעביר אליכם את הדין וחשבון השנתי של הרשות למשפט, טכנולוגיה ומידע לשנת 2009.
2. לצערי תהליך הפקת הדוח ארך יותר מהמצופה והרצוי, בשל ריבוי האירועים בשנת 2010, כמפורט בהערות המועצה להגנת הפרטיות.
3. אני מקווה שאיכות הדוח והנושאים המעניינים המפורטים בו יחפו על תקלה זו.
4. כבשנה שעברה, הדוח מפרט את כלל הנושאים אשר הרשות למשפט, טכנולוגיה ומידע עסקה בהם בשנת 2009. בשנה זו ביקשנו להציב זרקור על תפיסת ה"עיצוב לפרטיות" (privacy by design) ככלי מרכזי בשמירה על הפרטיות.

בכבוד רב,

יורם הכהן
ראש הרשות למשפט, טכנולוגיה ומידע

העתקים: מר יהודה ויינשטיין, היועץ המשפטי לממשלה
מר משה לדור, פרקליט המדינה
ד"ר גיא רוטקופף, מנכ"ל משרד המשפטים
הגב' שרית דנה, המשנה ליועץ המשפטי לממשלה (אזרחי)
הגב' אורית קורן, המשנה ליועץ המשפטי לממשלה (חקיקה)
מר אבי ליכט, המשנה ליועץ המשפטי לממשלה (כלכלי-פיסקלי)
מר מייק בלס, המשנה ליועץ המשפטי לממשלה (ייעוץ)
הגב' שביט מטיאס, המשנה ליועץ המשפטי לממשלה (הסכמים בינלאומיים)
הגב' רחל גוטליב, המשנה ליועץ המשפטי לממשלה (פלילי)

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2009

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

תוכן עניינים

א.	מבוא	4
ב.	תמצית מנהלים	4
ג.	סטטוס הקמת רמו"ט	6
ד.	חקיקה בתחומי פרטיות וחתימה אלקטרונית	7
ה.	עיצוב לפרטיות (Privacy By Design)	11
ו.	פעילות בין-לאומית של רמו"ט	14
ז.	מכתב מלווה של המועצה להגנת הפרטיות לדוח רשם מאגרי מידע	17
ח.	דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2009	23
ט.	דין וחשבון של רשם גורמים מאשרים בדבר הפעלת סמכויותיו לפי תקנה 16ל לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב–2001	32
י.	דין וחשבון של רשם שירותי נתוני אשראי ושירותי מידע על עוסקים לשנת 2009	37
יא.	נספח א' – נוסח תזכיר הצעת חוק הגנת הפרטיות (תיקון מס'...) (סמכויות אכיפה), התש"ע – 2009	39
יב.	נספח ב' – נייר עמדה בנושא תקנות אבטחת מידע להגנת פרטיות	77
יג.	נספח ג' – הצעת פרופ' עדי שמיר להגנת המידע במאגר הביומטרי	106
יד.	נספח ד' – סקרים אודות תפיסת הפרטיות בציבור הישראלי ובמגזר העסקי בישראל	124
טו.	נספח ה' - החלטת Working Party 29 לגבי עמידת ישראל בהוראות הדירקטיבה האירופית להגנת מידע אישי	189

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

א. מבוא

1. הדוח השנתי של הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים (להלן – **רמו"ט**) סוקר את פעילותה במהלך שנת 2009 במגוון ההיבטים של המשימות המוטלות עליה כרשות הגנת המידע האישי (data protection authority) של ישראל.

2. רמו"ט משמשת כרשות הרגולציה הישראלית להגנה על מידע אישי המעובד במערכות מידע ממוחשבות, הן בהבטי הפרטיות הנובעים מכך והן לעניין הזהות האלקטרונית כפי ביטויה בחוק חתימה אלקטרונית, התשס"א-2001.

3. בהתאם למגמה שהוחל בה בשנת 2008, הדוח השנתי של רמו"ט מפרט, בצד חובת הדיווח הקבועה בחוקים השונים שרמו"ט אחראית לאכיפתם, גם מידע אודות מכלול פעולות רמו"ט הקשורות במילוי תפקידיה.

4. במהלך שנת 2009 נמשך בקצב מואץ תהליך הקמת רמו"ט, תהליך אשר החל בתחילת שנת 2007. רמו"ט אמורה להגיע ליעדים הראשוניים שהוגדרו במסמך הייזום של רמו"ט בשנת 2010. כמתואר בדוח זה, במהלך השנה התרחשו מספר אירועים, אשר מעידים על מיקומה של רמו"ט בשיח הציבורי המקומי והבינלאומי בנושאים הנמצאים בתחום אחריותה.

ב. תמצית מנהלים

5. הדוח השנתי של רמו"ט מובא זו הפעם השניה כדוח מאוחד של מכלול פעולות הרגולציה של רמו"ט כרשות הגנת מידע אישי. להלן עיקרי הדברים:

5.1 מצבת כוח האדם של רמו"ט טרם הגיעה למצבת אשר תוכננה בהחלטה על הקמת רמו"ט, ועמדה בסוף שנת 2009 על 12 עובדי מדינה בלבד.

5.2 רמו"ט ניסחה בשנת 2009 הצעות לשני שינויי חקיקה משמעותיים בחוק הגנת הפרטיות, אשר אמורים לייצר שינוי דרמטי ברגולציה בתחום הגנת מידע אישי. שינוי אחד עניינו שיפור משמעותי של סמכויות האכיפה של רשם מאגרי מידע, והשני עניינו החלפת משטר רישום מאגרי המידע בחובת ניהול תקין של מאגרי מידע. הצעות אלה עברו לטיפול המקצועי של מחלקת ייעוץ וחקיקה במשרד המשפטים.

5.3 רמו"ט ממליצה על יישום הצעת פרופ' עדי שמיר ל"עמעום" המידע במימוש המאגר הביומטרי אשר יוקם על בסיס חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשס"ט-2009.

5.4 רמו"ט מקדמת באופן משמעותי את תפיסת ה"עיצוב לפרטיות" (Privacy By Design) כמתודה האופטימלית להקטנת הסיכון לפרטיות הנובע מפיתוח מערכות מידע המכילות מידע אישי.

5.5 פורום הנציבים של רשויות הגנת מידע אישי באירופה קבע בסוף שנת 2009 כי ישראל הוכיחה כי רמת הגנת המידע האישי בה תואם את הוראות הדירקטיבה האירופית להגנת מידע אישי. הליך אישור ישראל נוהל על ידי רמו"ט, ולהקמת רמו"ט יוחסה חשיבות רבה בקביעה זו.

5.6 רמו"ט התקבלה כחברה בכנס הבינלאומי של רשויות הגנת מידע אישי והתקבלה הצעתה לארח את הכנס בשנת 2010 בירושלים.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

5.7 בפעם הראשונה הופעל בשנת 2009 מנגנון הקנס המנהלי בעבירות לפי סעיף 31א לחוק הגנת הפרטיות כאשר הוטל קנס בשיעור של 177,000 ₪ על חברת נקודת שיווק וסחר בע"מ בשל שימוש במאגר מידע בלתי חוקי.

5.8 בוצע מבדק רוחבי אודות הפצת פנקס הבוחרים על ידי המפקח על הבחירות במשרד הפנים והשימוש בו על ידי המפלגות. הוחל תהליך תיקון הליקויים שנתגלו בפיקוח.

5.9 נמשכו תופעות של אי עמידת הגורם המאשר הרשום חברת קומסיין בהנחיות רשם גורמים מאשרים, ועקב כך הוכנס במסגרת תיקון מס' 2 לחוק חתימה אלקטרונית מנגנון של עיצום כספי לחוק.

5.10 הוטלו לראשונה עיצומים כספיים על בעלי רישיונות לשירותי נתוני אשראי בשל הפרת החוק. על חברת BDI Cofas הוטל עיצום כספי בשיעור של 67,300 ₪ בשל איסוף מידע חיובי בניגוד להוראות החוק. על חברת CIA הוטל עיצום כספי בשיעור של 12,900 ₪ בשל אי דיווח בהתאם לחוק שירות נתוני אשראי.

5.11 בעלת הרישיון לשירות נתוני אשראי חברת CIA הפסיקה את פעולתה בעקבות חשיפת ליקויים משמעותיים ברמת אבטחת המידע של פעילותה בפיקוח של רשם שירות נתוני אשראי.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

ג. סטטוס הקמת רמו"ט

6. כ"א

6.1 במהלך שנת 2009 נמשכה בניית תשתית כח האדם ברמו"ט, ואף כי חלה התקדמות רבה בגיוס כח האדם גם בשנה זו לא הושלמה יצירת תקני כח האדם ואיושם ליעד של 24 עובדי מדינה שנקבע על ידי משרד המשפטים בהקמת רמו"ט.

6.2 בסוף שנת 2009 עמדה מצבת כח האדם של רמו"ט על 18 איש, מהם שלושה קבלנים ושלושה מתמחים באופן הבא:

מחלקה	מצבת כ"א (סוף 2009)			מצבת כ"א מתוכננת	הערות
	סה"כ עובדים	עובדי מדינה קבועים	קבלנים ועובדים זמניים	עובדי מדינה קבועים	
לשכת ראש רמו"ט	2	2	-	3	ראש רמו"ט ומזכירה
מחלקת רישום ופיקוח	6	4	2	7	
מחלקת אכיפה וחקירה	4	3	1	7	
מחלקה משפטית	6	3	3	7	מהם שלושה מתמחים
	18	12	6	24	

6.3 בשנת 2010 אמורה רמו"ט להשלים את בניית התקנים ואיושם.

7. משרדים

7.1 בתחילת שנת 2009 עברה רמו"ט למשרדים חדשים בקריית הממשלה בתל-אביב אשר תוכננו באופן ייעודי לתפקידה.

7.2 המשרדים מתוכננים לפי היקף כוח האדם המתוכנן לרמו"ט כאמור, וכוללים גם חדרים ייעודיים לחקירות ולמעבדה הפורנזית, אשר נבנו על פי מפרט מיוחד לפעילות זו.

8. הקמת מעבדה פורנזית

8.1 במחצית השניה של 2009, עם גיוסו של מנהל למעבדה, הוחל בבניית מעבדה פורנזית ברמו"ט. מטרתה של המעבדה הפורנזית לספק את התשתית הטכנולוגיות בביצוע פיקוחים וחקירות בנושא של פרטיות במאגרי מידע, ולמטרה זו היא מאופיינת ונבנית.

8.2 בשלהי 2009 הסתיים האפיון של המעבדה, ובהתאם הוגדרו התשתית, המערכות הנדרשות, הפריסה, שיטות ונהלי עבודה (חלקם עדיין בתהליך). בתחילת 2010 הוחל בהליכי הרכש למערך מחשוב הנדרש שם הקמת המעבדה. המעבדה הפורנזית נבנית על מנת לתמוך בהליכי חקירות מחשב מקובלות, תוך התמחות ספציפית בחקירת מאגרי מידע ממוחשבים.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

ד. חקיקה בתחומי פרטיות וחתימה אלקטרונית

9. מבוא

9.1 פעולת רמו"ט בתחום החקיקה עיקרה קידום נושאים המצויים תחת אחריותה כרגולטור הגנת מידע אישי וחתימה אלקטרונית, ולעיתים עיסוק בנושאים משפטיים אחרים העוסקים בממשק שבין משפט וטכנולוגיות מידע.

9.2 פעילות רמו"ט בתחום זה מנוהלת על ידי המחלקה המשפטית של רמו"ט, בשיתוף מחלקת רישום ופיקוח ומחלקת אכיפה וחקירות.

9.3 במהלך שנת 2009 הקדישה רמו"ט את מירב העיסוק שלה כמוקד ידע במספר יוזמות העוסקות בהגנת מידע אישי מתוך מטרה לעדכן את התשתית הרגולטורית הקשורה בפעילותה.

10. פעילויות חקיקה מרכזיות

10.1 תזכיר תיקון חוק הגנת הפרטיות - סמכויות אכיפה וביטול חובת הרישום

10.1.1 תהליך החקיקה המרכזי שקודם על ידי רמו"ט בשנת 2009 מול מחלקת ייעוץ וחקיקה (פלילי) ומחלקת ייעוץ וחקיקה (חקיקה), הינו הכנת תזכיר מקיף לשינוי חוק הגנת הפרטיות ולרפורמה בהסדרים הנוגעים לרגולציה של הפרטיות במידע.

10.1.2 משיקולים פרקטיים של עומס עבודה, הופרד התהליך לשני חלקים, המוביל לשני תזכירי חוק. החלק הראשון עוסק בביצור סמכויות האכיפה של רשם מאגרי מידע, והשני בקביעת משטר רגולציה חדש בנושא הגנת פרטיות במידע המבטל, בין היתר, את חובת הרישום של מאגרי מידע כמעט לחלוטין ומחליפה בעקרון של ניהול תקין של מידע אישי.

10.2 תזכיר תיקון חוק הגנת הפרטיות (סמכויות אכיפה)

10.2.1 תזכיר זה מהווה מימוש של אחת מהמלצות הועדה לבחינת החקיקה בתחום מאגרי המידע בראשות מר יהושע שופמן ("דוח שופמן"). דו"ח שופמן המליץ להוסיף סמכויות אכיפה ופיקוח לרשם מאגרי המידע. בנוסף, התזכיר משקף תובנות שנצברו ברמו"ט במסגרת הפעלת סמכויות פיקוח ואכיפה, כמו גם לימוד משווה מפעילויות של רשויות מקבילות בעולם.

10.2.2 הציר המרכזי של התזכיר הינו השימוש באכיפה חלופית, בהתאם לדגם שגובש במשרד המשפטים. על רקע האתגרים, השוני והמורכבות של צרכי הפיקוח בתחום מאגרי המידע, נקבע מדרג של סמכויות פיקוח, באופן שקיימים כלי פיקוח בסיסים, וכלי פיקוח מוגברים. הפעלת כלי הפיקוח המוגברים נועדה לאפשר מימוש אכיפה חליפית, במקרים בהם יש חשד להפרה, ונדרש איסוף ראיות לצורך הפעלת הליך האכיפה.

10.2.3 חידוש משמעותי בתזכיר הינו ההצעה להסמיך את מפקחי רמו"ט לחדור לחומר מחשב ללא צו, כאשר מדובר בגישה למידע שאינו מידע אישי, אלא "נתוני מערכת", כלומר אותם נתונים המלמדים על פעולת מערכת המידע, ומאפשרים לאסוף ראיות אובייקטיביות, ובאופן בלתי אמצעי, אודות השימוש במידע בפועל בארגון. מהנסיון הנצבר בפעילות הפיקוח והאכיפה ברמו"ט עולה שלמידע זה חשיבות רבה לבדיקה ופיקוח של אופן השימוש במערכות מידע ובמידע בארגונים.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

10.2.4 לעניין סמכויות הטלת הסנקציות, מאחר שהרגולציה בתחום מאגרי המידע חלה על כלל המשק, ועל מגוון רב של גורמים מסחריים, מלכ"רים, וציבוריים, נקבעה בתזכיר גם נוסחה לקביעת חומרת הסנקציה שתוטל בגין ההפרות, המבוססת על מדרג עולה של הפרות (חומרה בסיסית, חומרה בינונית, חומרה גבוהה), ובהתאמה היקף הקנסות המוטלים. מרכיב נוסף בקנס המוטל הינו סוג המידע בו מדובר. מידע בעל רגישות גבוהה יביא לקנס גבוה יותר.

10.2.5 לצדן של הפרות אלה שביצוען יביא להטלת עיצום כספי שהוא סנקציה מינהלית, נוספו בתזכיר גם עבירות פליליות מפורשות בתחום הפרת הפרטיות במאגרי מידע.

10.2.6 במסגרת התזכיר מוצע גם לשנות את שם הפונקציה הרגולטורית מ"רשם מאגרי מידע" ל"ממונה על הגנת מידע", שינוי המעיד גם המעבר ממשטר של מרשם למשטר רגולטורי מודרני.

10.2.7 עיקר עבודת רמו"ט הושלמה בתחילת דצמבר 2009, ובסופו של דבר הפיץ משרד המשפטים את התזכיר להערות הציבור בפברואר 2010. נוסח התזכיר מצ"ב כ**נספח א'.**

10.3 צמצום ומיקוד חובת הרישום וקביעת חובת אחזקת תיעוד בדבר ניהול תקין

10.3.1 לצד התזכיר המוצע לעניין סמכויות אכיפה, ובמסגרת מימוש המלצות דוח שופמן, מבקשת רמו"ט גם לצמצם את חובת רישום מאגרי מידע הקיימת לפי הנוסח הקיים של חוק הגנת הפרטיות בצורה משמעותית.

10.3.2 העמדה של רמו"ט היא כי יש לבטל כמעט לחלוטין את חובת הרישום של מאגרי מידע ותחתיה להטיל חובה מפורטת ל"ניהול תקין" של מאגר מידע המכיל מידע מוגן פרטיות.

10.3.3 תמציתה של חובת ניהול תקין זו הינה בהקפדה על תהליכי קבלת החלטות שיביאו את סוגיות ניהול המידע וחובות הארגון המנהל את המידע לפי החוק, לידיעת ההנהלה הבכירה, בדרך פרוצדורלית שתאפשר בקרה ופיקוח, על ידי צדדים שלישים, ובכלל זה הרשם.

10.3.4 על פי עמדת רמו"ט, הגורמים היחידים שיהיו חייבים ברישום מאגרי מידע לאחר שינוי החוק יהיו מי שעוסק בסחר במידע - קרי מכירה של מידע אודות אנשים לאחרים. על מגזר זה יוטלו חובות מוגברות, הנובעות מפוטנציאל הרב של הפגיעה בפרטיות הכרוך בסחר במידע.

10.3.5 נוסח מוצע לרפורמה זו הועבר למחלקת ייעוץ וחקיקה במחצית שנת 2009, והוא אמור להתפרסם לתגובות הציבור במחצית הראשונה של 2010.

10.4 טיוטת תקנות אבטחת מידע

10.4.1 במהלך 2009 הכינה רמו"ט נייר עמדה בנושא אבטחת מידע במסגרת חוק הגנת הפרטיות, המכיל גם טיוטה מוצעת לתקנות מתאימות. ההסדר הקיים כיום בתחום אבטחת המידע חלקי מאוד ומיושן. מטרת הנייר להניע הליך לעדכון הוראות אבטחת המידע לפי החוק, על מנת לכוון את הארגונים המעבדים מידע, ולהתמודד עם הסיכונים הגוברים לפגיעה במידע.

10.4.2 נייר העמדה מפרט וקובע את עקרונות אבטחת המידע הקשורים בעיבוד מידע אישי במאגרי מידע, בהתבסס על תקנים מקובלים. יישום העקרונות בהקשר של מאגרי

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

מידע נועד לסייע במימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע מפני שימוש לרעה הפוגע בפרטיותם. עם זאת, ניתן להניח כי עמידה בעקרונות המוצעים תבטיח כי התנהלות הארגון בתחום המידע באופן כללי תהיה תקינה.

10.4.3 טיוטת התקנות מציעה מנגנונים וכלים פנים ארגונים, שמטרתם הפיכת אבטחת המידע במאגר, לחלק משגרת ניהול המידע בפרט וניהול הארגון בכלל. מטרת המנגנונים לכוון באופן מוחשי וברור יותר לחובותיהם ואחריותם בתחום אבטחת המידע. בשל כך נדרש כי הארגון יקבע נהלים בתחום אבטחת המידע, שיסדירו בצורה מפורטת וברורה יותר היבטים אלה. החובה לקבוע מסמכים המפרטים את הנהלים נגזרת מעקרונות יסוד של אבטחת מידע ושל ניהול תקין, ומאפשרות הנחלה של עקרונות ההתנהלות בתוך הארגון.

10.4.4 בנוסף, הנהלים גם יאפשרו לארגון להציג לצדדים שלישים – לקוחותיו, ספקיו, בתי משפט ורשם מאגרי מידע את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט באמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה.

10.4.5 בשל מגוון הארגונים המעבדים מידע אישי, נייר העמדה הוא מודולארי, בכך שהוא מחיל חובות ברמה עולה וגדלה ככל שפעילות עיבוד המידע שבארגון הינה משמעותית יותר. תפיסה זו, של חובות מודולאריות נגזרת ישירות מעקרונות יסוד של אבטחת מידע ומוצאת ביטויה גם במסמכים דומים בעולם.

10.4.6 במסגרת מגמת רמו"ט לקדם "עיצוב לפרטיות" (ראו פרק ה' להלן), התקנות המוצעות כוללות חובה על ארגון לשקול שיקולי פרטיות בתחילת איפיון של מערכת מידע חדשה, באופן שיקטין את האיומים שנובעים ממנה.

10.4.7 המסמך הופץ להערות הציבור בינואר 2010, ועורר עניין רב, לקראת פעילות משותפת עם הרשות הספרדית במסגרת פרויקט ה- twinning. בכוונת רמו"ט להעביר לאישור מחלקת ייעוץ וחקיקה ושר המשפטים גרסה מתוקנת של התקנות לאחר הערות הציבור. נוסח המסמך שהופץ מצ"ב כ**נספח ב'** לדוח זה.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

10.5 חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשס"ט-2009

10.5.1 במהלך 2009 נטלה כאמור רמו"ט חלק פעיל בתהליך חקיקת חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשס"ט-2009.

10.5.2 בחוק נקבעה סמכות להתקין תקנות שיעסקו בשימוש באמצעים אלקטרונים לזיהוי, ולכן הוגדר מנגנון של "אמצעי זיהוי אלקטרוני" - מידע שיונפק על תעודת הזהות החכמה ויאפשר זיהוי ייחודי ובלעדי של התושב, באמצעות תעודה אלקטרונית לאימות, למטרות של קבלת שירות מרחוק.

10.5.3 המנגנון האמור דומה בעיקרו למנגנון החתימה האלקטרונית, אלא שבניגוד לו, הוא משמש לזיהוי בגישה מרחוק ולא לחתימה אלקטרונית של מסמכים. המחלקה המשפטית ברמו"ט מסייעת לרשות האוכלוסין במשרד הפנים בניסוח תקנות מתאימות שיממשו אפשרות זו בתעודת הזהות.

10.6 חוק חתימה אלקטרונית

10.6.1 דיווח אלקטרוני למע"מ

10.6.1.1 כאמור בחוק ההסדרים לשנת 2009 ו– 2010 נכללו הוראות הקשורות בדיווח אלקטרוני לרשות המסים, באמצעות חתימה אלקטרונית. על רקע הנסיון שנצבר ברמו"ט, ועל מנת לאפשר לרשות המסים גמישות תפעולית ומשפטית, ליוותה רמו"ט הסדר המאפשר גמישות בשימוש בחתימה אלקטרונית. מדובר בהסדר לשימוש, בתנאים שיקבעו, בחתימה אלקטרונית מאובטחת לצורך הדיווחים.

10.6.1.2 רמו"ט ליוותה נושא זה בשלב ההסדרה בכנסת, וממשיכה ללוות את היישום.

10.6.1.3 רמו"ט ליוותה את התהליך האמור והציעה פתרונות משפטיים וטכנולוגיים שונים למטרה זו. כדי ליישם את הפרויקט האמור נבחנו חלופות שונות של אימות הזהות של מגישי הדוחות, ווידוא האמינות של הדוחות המוגשים.

10.6.2 תיקון מספר 2 לחוק

10.6.2.1 במהלך שנת 2009 נערכו מספר דיונים בהצעת חוק חתימה אלקטרונית (תיקון מס' 2). כגורם מפקח ובעל מומחיות בתחום זה רמו"ט היתה שותפה לדיונים הפנים ממשלתיים וכן לדיונים בוועדת המדע של הכנסת.

10.6.2.2 בעקבות הדיווח של רשם גורמים מאשרים המופיע בדוח רמו"ט לשנת 2008 אודות חסרונם של כלי אכיפה יעילים, הציעה ועדת המדע הוראות בעניין עיצום כספי בשל אי קיום הוראות הרשם. הליך החקיקה הושלם בשנת 2010 וידווח בדוח לשנה זו.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

ה. עיצוב לפרטיות (Privacy By Design)

11. במהלך שנת 2009 הניעה רמו"ט מספר תהליכים המקדמים את נושא ה"עיצוב לפרטיות" בתהליכי תכנון ופיתוח מערכות מידע במגזר הציבורי והפרטי.

12. הסיבה המרכזית לקידום נושאים אלה היא התפיסה שגובשה ברמו"ט כי ניתן למנוע נזקים לפרטיות אם נלקחים בשלב תכנון מערכת המידע ומימושה שיקולים של פוטנציאל הפגיעה בפרטיות של המערכת המפותחת ומיושמים אמצעים הממזערים את הפגיעה הפוטנציאלית בפרטיות.

13. עמדת רמו"ט היא כי תהליך של עיצוב לפרטיות מתחייב מיישום עקרון המידתיות הקבוע בסעיף 8 לחוק יסוד: כבוד האדם וחירותו וזאת לאור היות הזכות לפרטיות זכות יסוד על-חוקית. עקרון המידתיות מכתיב כי בשלבי התכנון, הפיתוח, המימוש והתפעול של מערכת מידע הטומנת בחובה פוטנציאל של פגיעה בפרטיות יבוצעו תהליכים הממזערים את פוטנציאל הפגיעה האפשרי.

13.1 במקרים רבים, כאשר בוחנים נזקים לפרטיות שנגרמו ממערכות מידע, כגון מדלף של מידע או שימוש לא ראוי בו, המסקנה היא שלו המערכת הייתה מתוכננת, מפותחת ומופעלת באופן הלוקח בחשבון מראש שיקולי פרטיות, ניתן היה למנוע את הנזק מראש, מבלי לפגוע באופן משמעותי ביכולות המערכת.

13.2 התהליך מחייב ביצוע תהליך מקדים של ביצוע "תסקיר השפעה על הפרטיות" (privacy impact assessment), במסגרתו מאותרים וממופים ההיבטים השונים של הפגיעה בפרטיות אשר עשויים להגרם מפיתוחה של מערכת מידע מסוימת, בהתייחס למידע אשר אמור להיות מעובד במערכת. על תהליך זה לבחון, בין היתר, מהו היקף איסוף ויצירת המידע המינימליים הנדרשים לצורך תכליתה של מערכת המידע, כמו גם לברר את ההצדקה החוקתית הראשונית בהקמתה לעומת חלופות אחרות.

13.3 לאחר מכן, מתחיל שלב העיצוב לפרטיות (privacy by design) אשר בוחן כל צורך עיבוד מידע ומוודא את חיוניותו. ככל שהחיוניות של עיבוד המידע נמוכה יותר, ופוטנציאל הפגיעה בפרטיות גבוה – תגבר הנטיה להמנע מיישום של משימת עיבוד מידע זו במסגרת המערכת.

13.4 מקום שנמצא כי יש צורך משמעותי בעיבוד מידע, ולזה פוטנציאל פגיעה משמעותי בפרטיות – ייושמו במסגרת המימוש של מערכת המידע ומשימות עיבוד המידע אמצעים משפרי פרטיות (PET – Privacy Enhancing Technologies). אמצעי PET מקובלים הינם טכנולוגיות מזעור מידע (data minimization), טכנולוגיות אנונימיזציה של מידע (data anonymization), טכנולוגיות הצפנה (encryption), מערכות ניהול זהות (IDM – Identity management) וכד'.

13.5 מימוש תפישה זו על מחזור החיים הכולל של מערכת המידע, החל בייזומה, תכנונה, פיתוחה, השימוש בה, עדכונה והוצאתה משירות יאפשר הקטנה משמעותית של הסיכון לפרטיות מעצם קיומה של מערכת המידע, בצד אפשור שימוש מבוקר בטכנולוגיות חדשניות.

13.6 רמו"ט פועלת לשילוב תפיסת ה"עיצוב לפרטיות" בתכנון של מערכות מידע ממשלתיות ופרטיות, ובעתיד תפעל לשילוב עיקרון זה במסגרת חקיקת הגנת הפרטיות והוראות שונות הקשורות לפיתוח מערכות מידע.

13.7 לדעת רמו"ט מימוש עקרון ה"עיצוב לפרטיות" כלשונו יתרום להקטנת סיכוני אבטחת מידע וצמצום עלויות תפעוליות של מערכות מידע, ולא רק בהיבט הפרטיות. מימוש עקרון זה

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

גורם לפיתוח של מערכות מידע שכמות המידע הנאסף בהם הוא מזערי, ולכך יש השלכות החורגות מעבר לסוגית הפרטיות, כגון עלות אחסון, עלות מנגנוני אבטחת מידע, פישוט תהליכים תפעוליים וכד'.

14. פרויקטי עיצוב לפרטיות שקודמו על ידי רמו"ט בתקופת הדוח

14.1 חוק ההסדרים – המלחמה בחשבוניות פיקטיביות

14.1.1 במסגרת טיוטת חוק ההסדרים לשנת 2009 ו– 2010 ביקשה הממשלה לחייב את מכלול העוסקים לדווח באמצעים אלקטרונים למע"מ, וכן להקים מסלקה אלקטרונית של חשבוניות שתאפשר לבקר בצורה טובה יותר את השימוש בחשבוניות, ותסייע במלחמה בחשבוניות הפיקטיביות.

14.1.2 במסגרת הדיון הפנים ממשלתי בהצעה, רמו"ט הצביעה על סיכוני הפרטיות וסיכונים אחרים למידע רגיש הנובעים מהקמה של מאגר כולל כאמור. בעקבות זאת נקבע בהחלטת הממשלה שליוותה את הצעת המחליטים, כי רמו"ט תלווה את תהליך עיצוב המערכת ברשות המיסים על מנת לוודא כי לא נוצרים סיכונים מיותרים לפרטיות.

14.1.3 תהליך זה מתקיים מול רשות המיסים וזרוע המחשוב שלה - שע"מ (שירות עיבודים ממוכנים).

14.2 חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשס"ט-2009 (להלן בפרק זה – חוק המאגר הביומטרי או החוק)

14.2.1 התהליכים לקראת חוק המאגר הביומטרי תוארו בדוח רמו"ט לשנת 2008. בשנת 2009 דנה הכנסת בהצעת החוק, והחוק פורסם בספר החוקים בתאריך 15.12.2009.

14.2.2 חוק המאגר הביומטרי היווה כר נרחב לפעולות של עיצוב לפרטיות, בהתאם לתהליך המפורט בסעיף 10 לעיל. בתהליכים אלה השתתפה רמו"ט ועמדה על הכנסתם של רכיבים משמעותיים להגנה על הפרטיות במסגרת החוק. להלן רשימת הפריטים בחוק שהם תולדה של תהליך זה:

14.2.2.1 הגדרת "תמונת פנים באיכות פחותה" בסעיף ההגדרות בחוק;

14.2.2.2 חובת הצפנת המידע לפי סעיף 3(ב) לחוק;

14.2.2.3 איסור אגירה של המידע הביומטרי בעת נטילתו לפי סעיף 3(ה) לחוק;

14.2.2.4 איסור אגירה של המידע הביומטרי במרכז ההנפקה לפי סעיף 4(ב) לחוק;

14.2.2.5 הגבלה על העברת המידע לפי סעיף 5(א) לחוק;

14.2.2.6 חובת דיווח שנתית על העברות המידע מהמאגר הביומטרי לפי סעיף 5(ג) לחוק;

14.2.2.7 חובת מחיקת אמצעים ביומטריים שניטלו לצורך השוואה לפי סעיפים 6(ו) ו-7(ב) לחוק;

14.2.2.8 חובת הצפנת מאגר המידע הביומטרי לפי סעיף 10(א) לחוק;

14.2.2.9 חובת הפרדה בין המאגר הביומטרי למידע אחר אודות האדם (אלפא נומרי) לפי סעיף 10(ב) לחוק;

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

14.2.2.10 אפשרות יצירת מנגנון הפרדת תפקידים בין משרדי ממשלה לפי סעיף 10(ד) לחוק;

14.2.2.11 הקמת רשות ייעודית לניהול המאגר הביומטרי לפי סעיף 11 לחוק;

14.2.2.12 חובת מזעור כמות מורשי הגישה למאגר על פי סעיף 13(ג) לחוק;

14.2.2.13 חובת מימוש אמצעי הגנה מפני דליפת מידע, פריצה אליו או חשיפתו באופן בלתי מורשה לפי סעיף 25(א) לחוק;

14.2.2.14 חובת תיעוד שימוש במאגר המידע לפי סעיף 25(ב) לחוק;

14.2.2.15 חובת מינויו של ממונה על הגנת הפרטיות במאגר לפי סעיף 26 לחוק;

14.2.2.16 הגבלה על שימוש בתמונה בעלת איכות פחותה לפי סעיף 27 לחוק;

14.2.3 גם מימושו של החוק מחייב יישומם של כללי העיצוב לפרטיות, שכן נוסח החוק הינו רק היסוד עליו יבנה מאגר המידע – ובמימוש בניית המאגר הביומטרי יש מקום נרחב לעיצוב לפרטיות ויישומם של אמצעים משפרי פרטיות (PET).

14.2.4 לעניין זה הועלתה הצעה על ידי פרופ' עדי שמיר, מגדולי המומחים בתורת ההצפנה בעולם למימוש תהליך של "עמעום" המידע הביומטרי במאגר המידע, באופן שגם דליפת המאגר הביומטרי או פריצתו לא תאפשר לחשוף את המידע ולקשור בין זהות אדם לנתוניו הביומטריים.

14.2.5 פרופ' שמיר מציע לנתק את הקשר החד-ערכי בין נתוניו הביומטריים (סריקת שתי טביעות האצבע המורות ותמונתו) של אדם והמידע אודות זהותו (שמו ו/או מספר תעודת הזהות שלו) של האדם, וליצור קשר בין נתונים ביומטריים לבין קבוצה של זהויות. פרופ' שמיר מראה כי במימוש שיטתו ניתן לקיים במלואה את תכליתו העיקרית של המאגר הביומטרי, קרי מניעה של הנפקה של תיעוד כפול לאדם. בנוסף מאפשרת שיטתו גם לקיים את הוראות החוק בהקשר של שימוש במאגר הביומטרי למטרות המנויות בסעיפים 7 ו-18-16 לחוק, אך לכך יידרשו משאבי חקירה נוספים שכן המידע שיהיה קיים במאגר הביומטרי יהיה מעומעם, ועל כן תידרש העזרות בתהליכי חקירה נוספים לצורך הגעה לזהות המדויקת.

14.2.6 ביוזמת רמו"ט הוצג הפתרון של פרופ' שמיר על ידו בפני בעלי העניין בתהליך במשרד הפנים, המשרד לבטחון הפנים, משטרת ישראל, משרד המשפטים וגופי בטחון אחרים בתחילת שנת 2010. המצגת שהוצגה על ידי פרופ' שמיר מצ"ב **כנספח ג'** לדוח זה.

14.2.7 **רמו"ט מחזיקה בעמדה כי הצעת פרופ' שמיר לבניית המאגר הביומטרי מיישמת איזון נכון וראוי של הזכות החוקתית לפרטיות במימוש החוק שכן היא מגנה על הזכות לפרטיות כבר בשלב הראשוני של איסוף המידע[1] תורמת משמעותית למימוש חובת אבטחת המידע הנגזרת ממנה ומונעת "זחילה פונקציונלית". במקביל, ההצעה מאפשרת לקיים ללא כל פגיעה את התכלית העיקרית של הקמת המאגר הביומטרי[2], ומאפשרת גם שימוש מושכל ומוגבל בו לתכליות המשניות של אכיפת חוק, תוך הוספות מגבלות מימוש אשר תמנענה זילות שימוש בו.**

[1] המידע שייאסף הוא המינימלי שנדרש לצורך קיום הוראות חוק המאגר הביומטרי
[2] מניעת הנפקה כפולה של תיעוד.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

14.3 שילוב הוראת עיצוב לפרטיות בנוסח המוצע לתקנות אבטחת מידע

14.3.1 תפיסת רמו"ט היא כי עיצוב לפרטיות הוא מרכיב מהותי באבטחת המידע של כל מאגר מידע, שכן הוא גורם למזעור המידע במאגר ויישום אמצעים נכונים להגנתו.

14.3.2 על כן, שולב בנוסח המוצע של תקנה 2(ג) ו-2(ד) לתקנות אבטחת המידע (ראו לעיל - סעיף 10.4) חובה למזער מידע ולתכנן את המערכת באופן שיפחית את סיכוני אבטחת המידע בפעולתה.

ו. פעילות בין-לאומית של רמו"ט

15. פרויקט Twinning עם רשות הגנת המידע הספרדית (AEPD)

15.1 בחודש יוני 2009 נחנך פרויקט הצימוד (Twinning) בין רמו"ט לרשות להגנת המידע הספרדית (AEPD – Agencia Española de Protección de Datos) במימון הנציבות האירופית. פרויקט זה מתקיים במסגרת הסכם ברצלונה בין הנציבות האירופית ומדינות הים התיכון, ואמור לארוך 18 חודשים.

15.2 מטרתו של הפרויקט הוגדרה "חיזוק הגנת מידע אישי בישראל" ולשם כך הועמד על ידי הנציבות האירופית תקציב של כ-1,000,000 אירו המשמש לחילופי ידע בין רשויות הגנת מידע אישי באירופה ורמו"ט.

15.3 הפרויקט כולל את המרכיבים הבאים:

15.3.1 שלושה כנסים בינלאומיים בישראל בנושא של הגנת מידע אישי

15.3.2 ימי עיון, סדנאות ומפגשים בנושא הגנת מידע אישי בנושאים שונים. מרביתן של הפעילויות פתוחות לציבור הרחב בחינם, מיעוטן – מיועד להכשרה של אנשי רמו"ט בלבד.

15.3.3 סיורים לימודיים של אנשי רמו"ט ברשויות הגנת מידע אישי באירופה.

15.3.4 ביצוע סקרים אודות תפיסת הציבור הישראלי את נושא הפרטיות במידע. תוצאות הסקרים שבוצעו באוקטובר 2009 במדגם מייצג של אוכלוסיית ישראל, ובמדגם מייצג של המגזר העסקי בישראל, מצ"ב **כנספח ד'** לדוח זה.

15.3.5 הכנת חומרי פרסום בנושא פרטיות במידע לציבור.

15.4 תוצאות רוב ימי העיון הנושאיים יהיו גיבושן של הנחיות ספציפיות בנושא הגנת מידע אישי למגזרים או בנושאים מסוימים.

15.5 בשנת 2009 התקיים כנס בינלאומי אחד שהציג את תפיסת הגנת המידע האישי האירופאית, והשתתפו בו נציבי הגנת מידע אישי של ספרד ואיטליה, ובכירים מרשויות הגנת המידע האישי של בריטניה וצרפת ויחידת הגנת המידע האישי של הנציבות האירופית. בנוסף, התקיימו במספר סדנאות בנושאים שונים ובוצעו מקצת מהסיורים הלימודיים ברשות הגנת המידע הספרדית.

16. תהליך הכרת הנציבות האירופית בהתאמת ישראל לדירקטיבה האירופית להגנת מידע אישי

16.1 בשנת 2009 הוכתר בהצלחה השלב הראשון במהלך, שהחל בשנת 2007 בפניית מנכ"ל משרד המשפטים דאז, משה שילה, אל הנציבות האירופית בבקשה להכיר במשטר הגנת המידע

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

האישי בישראל כהולם (adequate) את הדין האירופי בנושא, בהתאם למנגנון הקבוע בסעיף 25(6) לדירקטיבה האירופית להגנת מידע אישי (EC/95/46).

16.2 במהלך השנה ייצגה רמו"ט את המדינה בתהליך מול יחידת הגנת המידע האישי במשרד המשפטים של הנציבות האירופית (Directorate General Justice and Home Affairs), אשר רכזה את הטיפול האירופי בנושא. לאחר מכן, עבר הנושא לוועדת משנה של קבוצת העבודה הפועלת מכוח סעיף 29 לדירקטיבה האירופית להגנת מידע אישי (Working Party 29) שהיא הפורום המקצועי החשוב באירופה בנושא הגנת מידע אישי, המורכב מנציגי רשויות הגנת המידע האישי באירופה. נציגי רמו"ט הכינו מסמך משלים אודות משטר הגנת המידע האישי בישראל, בפרט אודות המימוש של חוק הגנת הפרטיות, התשמ"א-1981 והופיעו לשימוע בפני תת הוועדה בנושא.

16.3 בדצמבר 2009 אישרה המליאה של ועדת 29 את המלצת ועדת המשנה וקבעה כי בישראל מתקיים משטר הגנת מידע אישי התואם את הנדרש בדירקטיבה האירופית להגנת מידע אישי. הדוח מתייחס בפירוט לרמו"ט ולמעמדה העצמאי כרגולטור הגנת המידע האישי הישראלי, ונותן להקמתה ותפקודה משקל רב במסגרת ההחלטה לאשר את התאמת ישראל.

16.4 על פי התהליך הקבוע בדירקטיבה, מסמך זה צריך עדיין להיות מאושרר על ידי קבוצת עבודה הפועלת על פי סעיף 31 לדירקטיבה האירופית ולקבל את האישור הסופי מהפרלמנט האירופי ותהליך זה יתרחש במהלך שנת 2010.

16.5 המשמעות המעשית של החלטה זו היא הסרת מכשולים משמעותיים הקיימים כיום להעברת מידע אישי אודות אזרחי אירופה אל ישראל. התוצאה היא הקלה משמעותית לחברות ישראליות בהתקשרות עם חברות אירופאיות, בעיקר בחוזים למיקור חוץ של עיבוד מידע.

16.6 מדובר בהחלטה נדירה ובהישג משמעותי ביותר לישראל. המדינות שזכו עד כה להכרה זו היו שוויץ, קנדה וארגנטינה ואיי התעלה הבריטיים. נוסח ההחלטה של קבוצת העבודה 29 מצורף כ**נספח ה'** לדוח זה.

17. ייצוג מול ועדת ICCP של ה-OECD

17.1 כפי שדווח בדוח רמו"ט לשנת 2008, רמו"ט הובילה את המענה הישראלי לסוגיות שנבחנו על ידי ועדת מדיניות מחשבים, מידע ותקשורת (ICCP – Information, Communication and Computers Policy) של ארגון ה-OECD במסגרת תהליך ההצטרפות של ישראל לארגון.

17.2 בחודש מרץ 2009, במסגרת הישיבה ה-57 של ICCP נדון הדוח אודות ישראל. את מדינת ישראל יצגו בפני הוועדה מנכ"ל משרד המשפטים, מר משה שילה, סמנכ"ל לכלכלה במשרד התקשורת ד"ר אסף כהן וראש רמו"ט עו"ד יורם הכהן. הדוח התקבל ללא הסתייגויות ובכך נסללה, מבחינת הוועדה, הדרך לקבלת ישראל לארגון.

17.3 במהלך השנה השתתף ראש רמו"ט כנציג ישראל בישיבות העיתיות של ועדת ICCP ושל קבוצת העבודה לאבטחת מידע ופרטיות (WPISP – Working Party on Information Security and Privacy).

17.4 בדיוני קבוצת העבודה WPISP הציעה רמו"ט לארח בישראל כנס של ה-OECD לציון 30 שנה לחיבור ופרסום הנחיות ה-OECD לגבי הגנת מידע אישי והעברות מידע בין גבוליות. קבוצת העבודה קיבלה בברכה את הצעת רמו"ט, והכנס ייערך בתאריכים 25-26 לאוקטובר

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2010 בבנייני האומה בירושלים, בסמוך לכנס הבינלאומי של נציבי הגנת מידע אישי ופרטיות (ראו להלן).

17.5 יהיה זה הכנס הבינלאומי הראשון שעורך ארגון ה-OECD בישראל לאחר קבלתה לארגון.

18. קבלת רמו"ט לכנס הבינלאומי של רשויות הגנת מידע אישי ואישור אירוחו בירושלים

18.1 במהלך שנת 2009 הגישה רמו"ט בקשה להתקבל לכנס השנתי של רשויות הגנת מידע. כנס זה הוא המפגש השנתי של רשויות הגנת מידע אישי עצמאיות ברחבי העולם, וחברות בו למעלה מ-40 רשויות הגנת מידע מרחבי העולם.

18.2 בתהליך בדיקת הבקשה נעשית בחינה של המסגרת התפקודית של רשות הגנת המידע המבקשת להתקבל, כדי לוודא שהיא עומדת בכללי המינימום של עצמאות תפקודית כרשות הגנת מידע. ועדת המשנה לנושא המליצה על קבלת רמו"ט, ובכנס השנתי ה-31 שנערך במדריד בחודש נובמבר 2009 אושרה קבלת רמו"ט כחברה מלאה בכנס.

18.3 במעמד זה התקבלה, פה אחד, הצעת רמו"ט לארח בישראל את הכנס הבינלאומי ה-32 של נציבי הגנת מידע אישי והגנת פרטיות. הכנס ייערך בתאריכים 27-29 באוקטובר 2010 בבנייני האומה בירושלים.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

ז. מכתב מלווה של המועצה להגנת הפרטיות לדוח רשם מאגרי מידע

המועצה הציבורית להגנת הפרטיות

כ"ז באדר א תשע"א
3 במרץ, 2011

לכבוד
ועדת החוקה חוק ומשפט
הכנסת
<u>ירושלים</u>

נכבדי,

הנדון: **<u>הערות המועצה הציבורית להגנת הפרטיות על דוח רשם מאגרי מידע לשנת 2009</u>**

בהתאם לסעיף 10א לחוק הגנת הפרטיות, התשמ"א-1981, מגישה המועצה הציבורית להגנת הפרטיות את הדוח השנתי של רשם מאגרי מידע לשנת 2009, בצירוף הערות המועצה. דוח הרשם נכלל בדוח השנתי של הרשות למשפט טכנולוגיה ומידע (רמו"ט) במשרד המשפטים. ראש רמו"ט מכהן כרשם מאגרי המידע לפי חוק.

למרבה הצער, דוח זה מוגש באיחור רב. הרשם הגיש את טיוטת הדוח לעיון המועצה בתחילת חודש אפריל 2010. המועצה דנה בטיוטה, יחד עם הרשם, בישיבות המועצה של חודש אפריל ושל חודש מאי. המועצה העירה הערות לטיוטה וביקשה לערוך שינויים במתכונת הדוח ובמידת הפירוט שבו. ואולם, הדוח המלא של הרשם, שנכלל כאמור בתוך הדוח הכללי של רמו"ט, הועבר למועצה רק בסוף חודש דצמבר 2010. המועצה סבורה כי נכון לקיים שיח עם הרשם על אודות הדוח לפני עריכת הדוח הסופי וגיבוש הערות המועצה. אך אין מקום ששיח זה יגרום לכך שהדוח מוגש באיחור כה רב. המועצה ערה לעומס העבודה המוטל על רמו"ט ועל ראש הרשות באופן אישי, ומודעת לכך ששנת 2010 הייתה שנה מיוחדת, לאור פעילות רמו"ט במישור הבינלאומי (הליך ההכרה במשטר הגנת הפרטיות במדינת ישראל כהולם את אמות המידה של האיחוד האירופי, פעילות ה – twinning ואירוח כנס בינלאומי של נציבי ההגנה על מידע אישי). הרשם התחייב בפני המועצה להעביר אליה את הדוח לשנת 2010 בהקדם, והמועצה תקיים דיון בדוח הרשם בתחילת חודש מרץ 2011. אנו מצטערים על האיחור בהגשת הדוח לשנת 2009, ומקווים שניתן יהיה להגיש את הדוח לשנת 2010 במועד.

קיים קושי להעיר במועד זה על דוח המתייחס לתקופה שהסתיימה לפני יותר משנה. הערות המועצה נועדו בעיקר להצביע על נקודות הטעונות שיפור ושינוי – לדעת המועצה – בשנה שלאחר שנת הדוח, ובמקרה הנוכחי, חלפה גם השנה העוקבת לשנת הדוח. לכן, הערות המועצה העיקריות והעדכניות יצורפו לדוח הרשם לשנת 2010 שיוגש בזמן הקרוב.

המועצה מברכת על ההתקדמות המרשימה בפעילות רמו"ט בשנת 2009 בכל הקשור להגנת הפרטיות במאגרי מידע. בשנת 2009 היה גידול ניכר במשאבים המוקצים למטרה זו, לרבות הגדלת כוח האדם ומילוי התקנים שהוקצו לרמו"ט. הקמת הרשות והקצאת המשאבים שינו באופן משמעותי את יכולת הפיקוח והאכיפה, כמו גם את המעורבות של הרשם בשלבי גיבוש מדיניות בכל הקשור להקמת מאגרי מידע על ידי גופים ציבוריים.

עם זאת, למיטב הבנתנו טרם הושלם הליך התקנים הקצאת התקנים שתוכננו עם הקמת רמו"ט. לנוכח היקף עיבוד המידע האישי במגזר הפרטי והציבורי והאתגרים ההולכים ומתרבים לשמירה על פרטיות האזרחים, העובדים והצרכנים (למשל, מאגר מידע ביומטרי מרכזי, מאגרי מידע מרכזיים רחבי-היקף בתחומי הרפואה, החינוך והמערכת הפיננסית, הצבה נרחבת של מצלמות אבטחה במרחב הציבורי, שימוש במידע על אודות צרכנים, ועוד) – אנו סבורים כי יש להקצות לרמו"ט תקנים נוספים כך שלרשות רמו"ט יעמוד – לכל הפחות – כוח האדם בהיקף שהובטח במסמכי הייזום של הרשות. ברי, כי ארבעה עובדי מדינה המאיישים כיום את מחלקת הפיקוח של רמו"ט (העוסקים לא רק במאגרי מידע אלא גם בשירותי אשראי ובחתימה אלקטרונית) אינם יכולים להתמודד אלא עם חלק זעיר מהמטלות הניצבות בפניהם. לדעתנו, חשוב לאייש את רמו"ט לא רק באנשי משפט אלא גם במומחים לטכנולוגיה, מהנדסים, מדעני מחשבים ואנשי הצפנה ואבטחת מידע. רשויות מקבילות בעולם הקימו מחלקות המתמחות בטכנולוגיה, שכן המערכות מורכבות וקשות להבנה על ידי עובדים ללא הכשרה מתאימה.

ההתקדמות של רמו"ט נתנה את אותותיה גם במישור הבינלאומי. כפי שמצוין בסעיף 16 לדוח, בשנת 2009 המליצה ועדת הרגולטורים האירופיים הפועלת לפי סעיף 29 לדירקטיבה האירופית על הגנת מידע אישי להכיר בישראל כמדינה שמשטר הגנת המידע שלה הולם את אמות המידה האירופיות. תהליך זה הושלם לפני זמן קצר בעקבות ההכרזה הסופית של הנציבות האירופית מיום 31.1.11 בדבר עמידתה של ישראל באמות מידה אלו. הכרזה זו ניתנה במידה רבה בזכות התרשמותם של נציגי האיחוד האירופי מהיכולות ומהעצמאות של רמו"ט. הרשות השקיעה עבודה מאומצת בתהליך הארוך לקראת מתן הכרזה זו, והיא ראויה להערכה רבה בעקבות הישג זה, שיתרום לכלכלת ישראל ולמעמדה הבינלאומי.

עם זאת, המצב השורר בכל הקשור להגנה על מידע במאגרי מידע בישראל ממשיך לעורר דאגה. בשנים האחרונות התרבו היוזמות הציבוריות להקים מאגרים ומערכות מידע מקיפים האוספים ומעבדים כמויות אדירות של מידע אישי, בחלקו רגיש מאוד, על מצבם הרפואי, הסוציו-אקונומי, הפיננסי והחינוכי של אזרחים, כולל לרבות מידע על ילדים. דו"ח מבקר המדינה לשנת 2008 (שפורסם בחודש מאי 2009) התריע על מחדלים קשים באבטחת מידע של אזרחים במשרד הפנים ובביטוח הלאומי. מחקר של שני

מומחים מובילים הראה חוסר הקפדה על קיום הכללים של איסוף ושימוש במידע באינטרנט על ידי בעלי אתרים הן במגזר הפרטי והן במגזר הציבורי.[3]

מצב החקיקה

הדוח מצביע על הפעולות לקידום תיקון החקיקה הנוגעת להגנת הפרטיות במאגרי מידע. החקיקה בנושא זה, הקיימת משנת 1981, אינה מתאימה עוד לעידן הנוכחי, ויש צורך דחוף לתקנה. הדבר בא לידי ביטוי גם בהחלטת הנציבות האירופית שהוזכרה לעיל, שניתנה בין היתר על יסוד הצהרה מטעם המדינה על כוונה לתקן את החקיקה ברוח ההמלצות של צוות במשרד המשפטים, שכלל גם מומחים מחוץ לממשלה[4]. האיחוד האירופי, ארגון מדינות OECD, וממשלת ארה"ב השיקו במהלך השנה האחרונה הליכים מקיפים של התייעצות עם המגזר הפרטי והאקדמיה במטרה לתקן את המסגרת החקיקתית הקיימת בנושא זה. החקיקה האירופית היא משנת 1995 (דירקטיבת הגנת המידע) ו-2002 (דירקטיבת הגנת הפרטיות ברשתות תקשורת) והמסגרת הרגולטורית האמריקנית מתחילת שנות ה-2000. ברי, כי על ישראל, הנסמכת על חקיקה מתקופה שקדמה לעידן המחשב האישי, לאינטרנט ולטכנולוגיות הסלולר, הביומטריה וה-RFID, לעדכן במהירות את המסגרת החקיקתית הקיימת. למרבה הצער, ההליכים לקראת תיקון החקיקה מתקדמים לאט. המועצה קוראת למשרד המשפטים להאיץ הליכים אלה ככל שניתן.

עיצוב לפרטיות (Privacy by Design)

המועצה מסכימה כי הגנה נאותה על הפרטיות במאגרי מידע מחייבת הקפדה על עיצוב של מערכות מידע בדרך שתפחית עד עמה שאפשר את הפגיעה בפרטיות. המועצה מברכת על פעילותה של רמו"ט בתחום זה. אך על אף ההצלחות של רמו"ט, כפי שמשתקפות בדוח, המועצה התרשמה שאין מודעות מספקת בקרב הרשויות הציבוריות השונות לצורך לשלב שיקולי פרטיות בכלל, וכללי העיצוב לפרטיות בפרט, כבר בשלבים הראשוניים של גיבוש מדיניות הכרוכה באיסוף מידע אישי, עיבודו והחזקתו במאגרי מידע. אין די בשמיעת הערות הרשות כאשר יש כבר הצעה אופרטיבית של רשות ציבורית זו או אחרת, ויש לשלב שיקולי פרטיות ולהיעזר במומחיות הנצברת ברשות בכל שלבי גיבוש המדיניות.

המועצה מצטרפת להמלצת רמו"ט לצמצם את סכנת הפגיעה בפרטיות שבהקמת מאגר המידע הביומטרי בדרך של אימוץ פתרון טכנולוגי ברוח הצעתו של פרופ' עדי שמיר (סעיף 14.2 ונספח ג' לדוח). המועצה

[3] Michael D. Birnhack & Niva Elkin-Koren, Does Law Matter Online? Empirical Evidence on Privacy Law Compliance, 17 Mich. Telecomm. & Tech. L. Rev. (forthcoming, 2011). http://works.bepress.com/cgi/viewcontent.cgi?article=1014&context=michael_birnhack

[4] http://www.justice.gov.il/NR/rdonlyres/74594019-306F-4578-B604-189BE42EA1A0/8153/DochDB.pdf

מציעה לוועדות הרלוונטיות בכנסת לקיים דיוני מעקב אחר הפעולות להקמת המאגר על מנת לוודא כי יישום החוק ייעשה בדרך המצמצמת במידה המרבית את סכנת הפגיעה בפרטיות.

<u>התייחסות לפרק ז: דוח רשם מאגרי מידע (עמ' 17 – 16)</u>

דוח הרשם מצביע על פעילות רבה וחשובה בתחומי הפיקוח והאכיפה. אך המועצה סבורה כי מתכונת הדוח אינה מאפשרת לקבל תמונה מלאה של מאפייני הפעולות האלה והיקפם. לדעת המועצה, הנתונים המובאים בסעיף 2 לפרק ז הם לקוניים מדי.

הדוח מורכב בחלקו הגדול מפירוט של תיקי פיקוח ותיקי מבדק נבחרים. זה מידע חשוב ביותר, אך ספק אם מקומו של פירוט זה הוא בדוח השנתי. המועצה סבורה כי דיווח על מקרים כאלה צריך לבוא באופן שוטף, קרוב ככל האפשר למועד התרחשות הדברים. דיווח כזה יכול וצריך להופיע באתר האינטרנט של הרשות ובאמצעי פרסום אחרים (כפי שנזכר בדוח, לרשות יש עמוד בפייסבוק וחשבון בטוויטר אשר באמצעותם ניתנים דיווחים שוטפים בנושאים שונים).

הדיווח השוטף חשוב לא רק בשל חובת השקיפות של רשויות ציבוריות. הוא יוצר גם הרתעה ונותן הדרכה לבעלי מאגרים בדבר החובות שלהם לגבי עיבוד מידע אישי והחזקתו והתוצאות של הפרתן.

הדוח השנתי צריך לתת מבט כולל על פעילות האכיפה והפיקוח, תוך הפנייה למקרים טיפוסיים אשר כבר נמסר לגביהם דיווח לציבור. אין די בדיווח על מקרים נבחרים. לדעת המועצה, על הדוח לכלול דיווח על כלל התלונות שהוגשו לרשות ותוצאות בדיקתן. אין הכוונה לדיווח פרטני לגבי כל תלונה ותלונה כי אם מידע מעובד בדבר סוגי התלונות, הגופים נגדם הן מופנות, כמה מהן נמצאו מוצדקות, האמצעים שננקטו בעקבותיהן וכיו"ב. למועצה נמסר כי קיים קושי לערוך ניתוח מסוג זה לגבי הפעילות בשנת 2009. לאור העובדה שבקשת המועצה לקבל מידע כאמור הועלתה בישיבות המועצה בחצי הראשון של שנת 2010, המועצה מצפה כי הדוח של שנת 2010 יכלול מידע מפורט יותר על כלל התלונות.

הוא הדין לגבי תיקי המבדק. אין די במספר הכולל ותיאור מספר מקרים לדוגמה. המועצה מצפה לקבל נתונים על כלל תיקי המבדק (סוגי הגופים, ההפרות שנמצאו, האמצעים שננקטו לתיקון וכדו').

המועצה מעריכה את העבודה שהושקעה בבדיקת תלונות הציבור. אך יש לזכור כי רק לעתים רחוקות יידע נשוא המידע (data subject) אם בעל מאגר מידע הפר את החובות המוטלות עליו. הסדרי אבטחה בלתי מספיקים, עיבוד מידע שלא למטרה שלשמה נמסר, העברת מידע או מתן גישה לאדם בלתי-מוסמך – כל אלה נעשים הרחק מעיני נשוא המידע. מספר התלונות בוודאי אינו משקף, אפילו לא במקצת, את

מספר ההפרות. לכן יש חשיבות עליונה לפעולות פיקוח יזומות על ידי הרשות, לרבות ביקורות פתע. כל בעל מאגר צריך לדעת שהוא עשוי להיות נושא לביקורת על ידי הרשם ויחידת הפיקוח. מעבר לבחירת תחומים מרכזיים שייבחנו לעומק במהלך שנה פלונית, יש מקום לפיקוח מדגמי במגוון רחב של סוגי עסקים ומאגרים מדי שנה.

המועצה מקבלת את עמדת הרשות כי לצד הפיקוח והבקרה יש צורך בקביעת אמות מידה לפעולות בעלי מאגרי מידע. נכון יותר לערוך ביקורת כאשר קיימים תקנים ברורים לאבטחת מידע ולחובות בעלי המאגרים. המשאבים המוגבלים העומדים לרשות רמו"ט צרכים להיות מופנים, במידה רבה, לקביעת אמות מידה אלו. אך גם אם יש עדיין תחומים בהם אמות המידה עדיין אינן ברורות די הצורך, יש התנהגויות שהן ללא ספק אסורות לפי הדין הקיים, והפיקוח המדגמי צריך להתקיים באופן שוטף כדי לשרש הפרות אלה וכן כדי לעמוד על הסוגיות הבעייתיות ועל התחומים שבהם יש מקום לגבש אמות מידה ברורות יותר.

<u>סיכום</u>

בשנת 2009 נראו הפירות של תהליך ארוך וחשוב של הקמת הרשות למשפט טכנולוגיה ומידע ושל התבססות פעולותיה. תהליך חיובי טרם הסתיים. המגמה היא חיובית ביותר, אך עדיין יש פעולות רבות שיש לעשות כדי לשפר את ההגנה על המידע האישי במאגרי מידע. לזירוז התיקונים בחקיקה ולהגדלת כוח האדם העוסק בתפקידי פיקוח חלק חשוב בקידום פעולות אלה.

כפי שנאמר בפתח הדברים, הדוח לשנת 2010 - על פי הודעת ראש רמו"ט - יוגש בקרוב. המועצה תדון בה ותעביר אותה לוועדת החוקה חוק ומשפט לפי סעיף 10א לחוק. המועצה מציעה לוועדה לקיים דיון בשני הדוחות יחדיו כדי לעמוד על המגמות, על ההתקדמות ועל הקשיים בהגנה על מידע אישי במאגרי מידע.

בברכה,

יהושע שופמן
יו"ר המועצה

העתקים: שר המשפטים
היועץ המשפטי לממשלה
פרקליט המדינה
מנכ"ל משרד המשפטים
המשנים ליועץ המשפטי לממשלה

ח. דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2009

מוגש למועצה להגנת הפרטיות מכוח סעיף 10א לחוק הגנת הפרטיות

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

1. מבוא

1.1 פעולות הפיקוח והאכיפה של רשם מאגרי מידע מופעלות על ידי שתי מחלקות ברמו"ט – מחלקת רישום ופיקוח ומחלקת אכיפה וחקירות. שנת 2009 הייתה השנה הראשונה לפעילות מובחנת ועצמאית של שתי המחלקות, במהלכה נבחנה ולובנה חלוקת העבודה בין שתי המחלקות באופן מוסדי. הניסיון שנצבר היווה את הבסיס לתזכיר המוצע לשינוי סמכויות האכיפה והפיקוח של רשם מאגרי מידע, בו מוצעת הסדרה מפורטת של הסמכויות הנדרשות לביצוע משימות הפיקוח והאכיפה והגדרה מדויקת של ההפרות והעבירות בהקשר של פרטיות במידע.

1.2 חלוקת העבודה מבוססת על האבחנה שמחלקת רישום ופיקוח עוסקת בהפעלת כלי האכיפה המנהלית של רמו"ט במסגרת פעילות של מבדק (audit) ופיקוח (inspection), בעוד שמחלקת אכיפה וחקירות עוסקת בפעילות האכיפה הפלילית של רמו"ט תוך ביצוע חקירות פליליות (investigation). האבחנה בין פעולות אלה היא כדלהלן:

1.2.1 פעולות מבדק מבוצעות על בסיס תכנית קבועה מראש לבדיקת תאימות פעילות עיבוד מידע מסוימת להוראות החוק, שלא על בסיס תלונה או חשד כלשהו לאי-תקינות פעולת עיבוד המידע. מבדק עשוי להיות מגזרי, נושאי או נקודתי.

1.2.2 פעולות פיקוח נעשות על בסיס תלונה או מידע אחר שהתקבלו ברמו"ט, המחייבים בדיקה האם הופרו הוראות החוק. פעולות הפיקוח של רשם מאגרי מידע מבוצעות כיום מכוח סמכויות הפיקוח המוקנות למפקח על פי סעיף 10(ה1) לחוק הגנת הפרטיות. עם חקיקת התיקון המוצע בתזכיר האכיפה, יופעלו על ידי מחלקת רישום ופיקוח הסמכויות המוקנות למפקח על פי הנוסח שיתקבל בכנסת.

1.2.3 פעולות חקירה הן פעולות חקירה פלילית, המבוצעות כיום מכוח ההסמכה שניתנה על ידי השר לביטחון פנים למנהלת מחלקת אכיפה וחקירות ברמו"ט. עם חקיקת התיקון המוצע בתזכיר האכיפה, יופעלו על ידי מחלקת אכיפה וחקירות כל הסמכויות המוקנות לחוקר על פי הנוסח שיתקבל בכנסת.

1.3 בשנת 2009 הוטלו בפעם הראשונה קנסות מנהליים על הפרת הוראות סעיף 31א לחוק הגנת הפרטיות, וזאת לאחר שהתשתית להטלתם גובשה בשנת 2008.

2. נתונים

2.1 בתחום הגנת הפרטיות הוגשו בשנת 2009 107 תלונות[5], המהוות כ-88% מכלל התלונות שהגיעו לרמו"ט.

2.2 במהלך השנה נפתחו ברמו"ט 105 תיקי פיקוח בנושא הגנת פרטיות, המהווים כ-94.5% מכלל תיקי הפיקוח[6].

[5] יצוין כי לאור שינויים באופן איסוף הנתונים, שונו ההגדרות של פניות ותיקי פיקוח ועל כן ההשוואה בין מספרים אלו למספרי שנים קודמות עשויה להטעות.

[6] תיק פיקוח הוא מסוג של ביקורת או פיקוח, ויכול להיפתח על בסיס תלונה או על בסיס החלטה פנימית של רמו"ט, בין אם על בסיס מידע שהגיע, ובין אם על בסיס תכנית עבודה.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.3 22 מכלל תיקי הפיקוח בתחום הגנת הפרטיות כללו הגעה של מפקחים אל חצרי המפוקח ("פיקוח בשטח"). מכלל הפיקוחים בשטח שבוצעו על ידי רמו"ט, הפיקוחים בתחום הגנת הפרטיות היוו כ-56%.

3. <u>תיקי פיקוח נבחרים</u>

3.1 מגזר ציבורי

3.1.1 שימוש במאגר לא חוקי ע"י רשות מקומית - מועצה מקומית זיכרון יעקב

3.1.1.1 ביום 11.1.2009 ניתן פסק דין בהליך אזרחי בו תבע אזרח את המועצה המקומית זכרון יעקב אודות נזקים שנגרמו לו, לטענתו, עקב פעולות גביה מוטעות שהופעלו כלפיו. מפסק הדין ומפרוטוקול הדיון עלה, כי חברת מילגם בע"מ, המספקת בין היתר שירותי גביה במיקור חוץ עבור מועצת זכרון יעקב, עשתה שימוש כזרוע הגביה של המועצה במאגר המידע הידוע בכינויו "אגרון" שהורד מרשת האינטרנט. מאגר ה"אגרון" מכיל מידע ממקור בלתי חוקי בהיקף רחב אודות אזרחי ישראל.

3.1.1.2 כב' השופט יחיאל ליפשיץ שהכריע בסכסוך האמור ביקש שיועבר עותק מפסק הדין אל רשם מאגרי מידע, ובשל כך החל הטיפול האכיפתי. במקביל הועבר המקרה גם על ידי האגף לחקירות ולמודיעין במטה הארצי של משטרת ישראל לרמו"ט בהמשך להנחיית בית המשפט בתיק הנ"ל.

3.1.1.3 נוכח אי חוקיות מקורות המידע, אחזקתו, והשימוש שנעשה במידע פנתה רמו"ט למועצה המקומית ולחברת מילגם. לאחר בירור העובדות ואימותן ננקטו הצעדים הבאים:

3.1.1.3.1 ניתנה הוראה על הפסקה לאלתר של כל שימוש (לרבות החזקה) ופעילות במאגר המידע שאינו חוקי והסרה שלו לצמיתות מכל מחשביהם של המפוקחים וצדדים שלישיים הנוגעים לפעילותם (ספקי שירותי מיקור חוץ או לקוחות).

3.1.1.3.2 לאחר הסרת מאגרי המידע, התבקשו המפוקחים להעביר תצהיר ביעור חתום על ידי מנכ"ל החברה וראש המועצה כתימוכין להפסקת הפעילות ולהשמדת המאגר.

3.1.1.3.3 ניתנה הוראה למפוקחים לוודא שלא נעשה שימוש בלתי חוקי אחר במידע מוגן פרטיות על ידם.

3.1.1.3.4 המפוקחים נדרשו ליידע את כל הגופים הקשורים בהם (ספקים ולקוחות) לבל ישתמשו באופן שאינו חוקי במאגרי מידע.

3.1.1.3.5 הובהר כי בניהול ושימוש במידע באופן לא חוקי על ידי גוף ציבורי כדוגמת רשות מקומית יש לפגיעה בפרטיות השלכה, חשיבות, משקל וחומרה יתרים.

3.1.1.3.6 הובהר כי היות המאגר ניתן להורדה מרשת האינטרנט ולכאורה נגיש לכל, אינה מכשירה את אי החוקיות הכרוכה בשימוש בו.

3.1.1.4 המועצה המקומית זכרון יעקב וחברת מילגם, הצהירו כנדרש כי ביערו את מאגר המידע, הפסיקו כל שימוש בו ופעלו למניעת העבירה בעתיד.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

3.1.1.5 במקביל יודעו הגורמים הרלבנטיים במשרד הפנים ובחברה למשק וכלכלה של השלטון המקומי בע"מ אודות הממצאים. בעקבות זאת, החברה למשק וכלכלה הודיעה לרמו"ט כי אזהרה כאמור תצורף להליך המכרז שיערכו רשויות מקומיות לקבלת שירותי גביה באמצעות החברה למשק וכלכלה.

3.1.2 צה"ל – אגף כוח אדם

3.1.2.1 ידיעה בתקשורת דיווחה על כך, שבאתר האינטרנט של אגף כוח אדם בצה"ל, "עולים על מדים", נחשף מידע אישי פרטי של מועמדים לגיוס לשירות הביטחון. נפתח הליך פיקוח לבירור האירוע.

3.1.2.2 אגף כ"א בצה"ל נדרש להציג את העובדות המדויקות באשר לאירוע לאחר ביצוע תחקיר, ולפרט את האופן בו יתוקנו הליקויים שהובילו לפגיעה בפרטיות המועמדים לגיוס.

3.1.2.3 תוצאות התחקיר שהוגשו לרמו"ט הראו, שתקלה טכנית ולא פרצת אבטחת מידע גרמו לחשיפת מידע על 6 מועמדים לגיוס, למשך כשעתיים.

3.1.2.4 צה"ל דיווח על כך שבעקבות התחקיר שונו נהלי עבודה למניעת קרות התקלה הטכנית שאירעה, וכן שונה נוהל הטיפול בתקלות במערכת המדוברת. בנוסף, בעקבות הפיקוח, הוקמה בצה"ל ועדה להעברת מידע בין גופים ציבוריים כנדרש בחקיקה, והרמטכ"ל מינה את ראש אכ"א לעמוד בראשה.

3.1.3 בית חולים איכילוב

3.1.3.1 בהמשך לדיווח לשנת 2008, ביצע הרשם בקרה על התקדמות ביה"ח איכילוב לתיקון ליקויי האבטחה שנתגלו על ידי רמו"ט במהלך השנה הקודמת.

3.1.3.2 מהבחינה עלה כי ביה"ח הכין תכנית מקיפה על בסיס הליקויים שאותרו ושילב תכנית זו במסגרת תכנית העבודה השנתית.

3.2 מגזר פרטי

3.2.1 קופ"ח מאוחדת

3.2.1.1 בעקבות תלונה על אופן הקצאת סיסמאות גישה על ידי קופת חולים מאוחדת, נערך פיקוח מול הקופה אשר העלה כי נגישות למידע רפואי מבוססת על העברת מאפיין מזהה אחד (כרטיס).

3.2.1.2 בעקבות הפיקוח התחייבה קופ"ח מאוחדת כי יבוצע שינוי בזיהוי המשתמש בטרם תתאפשר נגישות למידע רפואי.

3.2.2 חברת יתרון אנושי

3.2.2.1 חברת השמה נהגה להעביר מידע אודות מי שמסר קו"ח ליועץ חיצוני אשר פנה, על בסיס המידע האמור, לשיווק שירותיו לנושאי המידע.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

3.2.2.2 בעקבות פעילות הפיקוח שערכה רמו"ט לבירור מקור הסמכות של חברת ההשמה להעביר את המידע ליועץ חיצוני, הפסיקה החברה את העברת הנתונים.

3.2.3 סיוע במימוש זכויות פרטניות

3.2.3.1 במסגרת טיפול בתלונות, סייעה רמו"ט במספר מקרים לאזרחים לממש את זכויותיהם על פי חוק הגנת הפרטיות אל מול בעלי מאגרי מידע גם באופן פרטני, לדוגמא – הזכות למחיקה מבעל מאגר מידע במסגרת סעיף 17ו, וכן מימוש זכות העיון הקבועה בסעיפים 13 ו-14 לחוק הגנת הפרטיות.

4. <u>תיקי מבדק</u>

4.1 מגזר ציבורי

4.1.1 פנקס הבוחרים

4.1.1.1 במסגרת המבדק נבדקה הפצת פנקס הבוחרים על ידי המפקח על הבחירות, תהליך הנפקת הפנקס ואופן העברתו למפלגות והשימושים שנעשים בפנקס על ידי המפלגות ועל ידי צדדים שלישיים.

4.1.1.2 המבדק כלל פיקוח ביחידת המפקח על הבחירות, פניה לכלל המפלגות אשר הופקו להם פנקסים ופיקוח מדגמי בשטח במספר מפלגות. דוח המבדק הועבר לידי משרד הפנים ולהלן עיקרי ממצאיו -

4.1.1.3 מאיסוף הממצאים עלו מספר ליקויים הדורשים תיקון, ובין היתר נמצא כי -

4.1.1.3.1 קיים פער בין ההסדר החוקי הקיים לבין הצרכים והשימושים של המפלגות והרשימות בפנקס בפועל. לדוגמא, הטמעת מידע הפנקס במערכות מידע קיימות בשירות המפלגות למול הדרישה החוקית להחזירו בתום השימוש; אופן השליטה במידע על ידי בא-כוח המפלגה כמתחייב מהטפסים עליהם הוא חותם למול המציאות שבה לעיתים אין לו כל נגיעה לטיפול במידע וכד';

4.1.1.3.2 האופן בו מופץ הפנקס, טכנולוגית ונוהלית, אינו מצמצם את הפגיעה האפשרית בפרטיות ואת הצורך לעמוד בדרישות חוק הבחירות והתקנות מכוחו. לדוגמא, לאור הקלות בה ניתן להעתיק את הפנקס מהתקליטור, יש לבחון את אופן הפצת המידע בדרך זו, ולבחון יכולות טכנולוגיות הקיימות להפצת מידע באופן אשר יקשה על שימוש בו מעבר למטרה לשמה נמסר.

4.1.1.3.3 נמצאו מקרים שניתן עותק מהפנקס למי שלא היו מורשים לקבלו עפ"י חוק, ומקרים בהם עותק הפנקס לא הוחזר כחוק ע"י מי שקיבלו אותו;

4.1.1.3.4 ניתן להדפיס עותקים של הפנקס מבלי שיהיה לכך תיעוד במערכות;

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

4.1.1.3.5 אין נהלים ברורים וחלוקת אחריות מוגדרת במערכת היחסים בין המפקח על הבחירות ורשות ההגירה והאוכלוסין;

4.1.1.3.6 המפקח על הבחירות לא יזם פעולות להבטיח את מילוי הוראות חוק הבחירות בהקשר של הגנת הפרטיות במאגר המידע.

4.1.1.4 משרד הפנים והמפקח על הבחירות נתבקשו לפעול על מנת לשנות את המצב הקיים, ולתקן את הליקויים שנמצאו. הפעולות שהתבקשו הן:

4.1.1.4.1 הכנת הצעת חקיקה לתיקון חוק הבחירות והתקנות;

4.1.1.4.2 כתיבת נהלי עבודה מפורטים ליחידת המפקח על הבחירות בנושא הפצת הפנקס;

4.1.1.4.3 נקיטת פעולות להעלאת מודעות לחשיבות ההגנה על המידע בקרב המפלגות;

4.1.1.4.4 ביצוע פעילות ביקורת על אופן הפעולה של המפלגות במידע הפנקס.

4.1.1.5 יצוין כי נכון למועד כתיבת דוח זה המפקח על הבחירות החל בביצוע פעולות על מנת לבחון כיצד לבצע את השינוי הנדרש באופן הפצת הפנקס.

4.1.1.6 בהקשר זה יש להבהיר כי בנוסף לפיקוח הרוחבי, ממשיכה רמו"ט לאכוף את הוראות החוק כנגד גורמים העושים שימוש בפנקס הבוחרים שלא למטרה לשמה הפנקס הופק. בעקבות פעילות רמו"ט, ובהמשך לפעילות פיקוח שבוצעה במהלך שנת 2009, הוטלו (נכון למועד כתיבת הדוח), בשני מקרים שונים קנסות מינהליים על צדדים שלישיים שעשו שימוש בפנקס הבוחרים שלא למטרה לשמה הופק הפנקס.

4.2 מגזר פרטי

4.2.1 בחינת היקף השימוש במידע אישי במגזר הסלולר

4.2.1.1 במהלך שנת 2009 הוחל בביצוע ביקורת במגזר מפעילי שירותי רט"ן (סלולרי) לבחינת היקף האיסוף של מידע אישי על ידי בעלי הרישיונות בהתקשרות ובמהלך מתן השירות, מגוון השימושים שנעשים במידע ונאותות ההסכמה המתקבלת מהמנויים לשימוש במידע.

4.2.1.2 במסגרת ביקורת זו, נשלחו דרישות מידע ומסמכים אל ארבעת בעלי רישיונות הרט"ן הפועלים בישראל כיום למסירת מידע בנושאים הנ"ל.

4.2.1.3 על בסיס המידע המקיף שהתקבל, יבוצעו במהלך שנת 2010 פיקוחי המשך בחצרי מפעילים, לצורך בחינה של נכונות ושלמות המידע שהתקבל ועמידת החברות בהוראות חוק הגנת הפרטיות.

5. <u>הטלת קנסות מנהליים</u>

5.1 לקראת סוף שנת 2009 הסתיים התהליך הראשון בו הוטל קנס מנהלי בגין הפרה של סעיף 31א לחוק הגנת הפרטיות. הקנס הראשון הוטל על חברת נקודת שיווק וסחר

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

בע"מ, אשר עשתה שימוש במאגר המידע הבלתי חוקי "אגרון" לפעילות של דיוור ישיר. להלן תיאור המקרה:

5.1.1 ברמו"ט התקבלו תלונות כנגד חברת נקודת שיווק וסחר בע"מ לפיהן נעשתה פניה שיווקית למתלוננים כלקוחות פוטנציאליים לקניית מוצר מהחברה תוך ידיעה של מועד יום ההולדת של המתלונן ושימוש בו לצרכי שיווק. על פניו, המידע הנ"ל לא היה אמור להיות ברשות החברה.

5.1.2 נוכח זאת, נוהל הליך פיקוח שעיקרו התמקד בבחינת מקורות המידע של החברה בתהליך הדיוור הישיר ובשימוש שנעשה במידע.

5.1.3 במהלך הפיקוח הונחה תשתית ראייתית לכך שפניות טלפוניות ללקוחות לשיווק מוצר של החברה (המכונה בעיקר "לוטו-דיל"), נעשו על סמך מידע שנשלף ממאגר מידע לא חוקי – מאגר ה"אגרון".

5.1.4 השימוש נעשה בין היתר בכך שהחברה, עובדיה ונציגים מטעמה השתמשו במידע שהופק ממאגר המידע לצורך פנייה טלפונית אישית ביום ההולדת של אדם לשם שיווק המוצר "לוטו דיל". הפניה של החברה נעשתה במכוון ביום ההולדת על סמך אותם נתונים.

5.1.5 הממצאים העלו כי התנהלות החברה מהווה הפרה של הוראות ס' 8(ב) לחוק. נוכח זאת הוחלט להטיל על החברה קנסות מנהליים בהתאם לסעיף 31א(א)(1) לחוק הגנת הפרטיות.

5.1.6 על החברה הוטלו 59 קנסות מינהליים בסך 3,000 ₪ כל אחד (בסה"כ 177,000 ₪). לפנים משורת הדין ערכה רמו"ט שימוע בפני החברה ובא-כוחה טרום הטלת הקנסות המנהליים.

5.2 במהלך שנת 2009 נוהלו מספר פיקוחים אשר הובילו את מפקחי רמו"ט להטיל קנסות מינהליים בגינם במהלך חודשיה הראשונים של שנת 2010. קביעות רמו"ט על קיומן של הפרות החוק מפורסמות בטבלה באתר האינטרנט של רמו"ט[7], וידווחו בהרחבה בדיווח של רמו"ט בשנה הבאה.

6. <u>חקירות פליליות</u>

6.1 במהלך שנת 2009 התקיים תהליך מול המשרד לביטחון פנים ומשטרת ישראל, לצורך קבלת הרשאה לבצע חקירות פליליות בהתאם לקבוע בפקודת הפרוצדורה הפלילית (עדות).

6.2 בסיומו של התהליך הוקנו בחודש יולי 2009 למנהלת מחלקת אכיפה וחקירות, עו"ד מילי בך, באופן פרסונאלי סמכויות חקירה פליליות לפי הסעיפים העונשיים בחוק הגנת הפרטיות ובחוק שירות נתוני אשראי.

6.3 מכוח הסמכה זו הוחל במחצית השניה של שנת 2009 בפעולות חקירה, הנמצאות בשלב סמוי שלהן ועל כן לא ניתן להרחיב אודותן.

6.4 השקת "קו חם"

[7] http://ilita.justice.gov.il

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

6.4.1 בראשית שנת 2009 הושק "קו חם" אשר נועד לספק לאזרחים פניה ישירה למחלקת אכיפה בהגשת תלונות העשויות להצביע על הפרות חמורות של חוק הגנת הפרטיות.

6.4.2 הקו החם מספק לאזרח הנפגע אפשרות תקשורת בטלפון ובאינטרנט באמצעות טופס מקוון. במסגרת הקו החם התקבלו פניות אשר חלקן הביאו לפתיחת תיקי פיקוח ואכיפה.

6.5 שיתופי פעולה עם גורמי אכיפה אחרים

6.5.1 בשל היות נושא מאגרי המידע נושק בתופעות הנחקרות גם על ידי גופי חקירה אחרים, פעלה במהלך 2009 מחלקת האכיפה ליצירת קשרי עבודה ושיתופי פעולה עם גורמי אכיפה וגופי חקירה אחרים.

7. <u>רישום מאגרי מידע</u>

7.1 במהלך שנת 2009 נמשך הניסיון ברמו"ט לבחון את אופן פעילותה בתחום רישום מאגרי מידע באופן שהשקעת המשאבים של רמו"ט בתחום זה, תייצר את התועלת שפעולות רישום המאגרים עשויות להניב.

7.2 בהמשך לשינוי שרמו"ט הצהירה עליו בדוח לשנת 2008 ומהטעמים המצוינים שם[8], הכינה רמו"ט בשנת 2009 נוסח תזכיר לשינוי משטר הרישום הנהוג כיום. ההצעה לתיקון החקיקה נמצאת בתהליך אישור במחלקת ייעוץ וחקיקה (חקיקה) במשרד המשפטים. להרחבה ראו פרק פעילויות חקיקה מרכזיות, צמצום ומיקוד חובת הרישום וקביעת חובת אחזקת תיעוד בדבר ניהול תקין.

7.3 במקביל, וכל עוד משטר הרישום הנוכחי קיים, פועלת רמו"ט לשפר את השירות שניתן לציבור בתחום רישום מאגרי המידע. במהלך שנת 2009 קיבל ראש רמו"ט, בתפקידו כרשם מאגרי מידע מספר החלטות, אשר שינו את הפרשנות שניתנה להגדרת "בעל מאגר" על ידי קודמתו בתפקיד. ההחלטות התקבלו בסוגיות הבאות:

7.3.1 בתי ספר

7.3.1.1 בעקבות דיונים מול משרד החינוך ופניות של בתי ספר, החליט הרשם כי בעל המאגר במאגרים המצויים בבתי ספר הוא כדלקמן –

7.3.1.1.1 במערכת המנב"ס אשר מוטמעת בבתי הספר על ידי משרד החינוך – משרד החינוך;

7.3.1.1.2 בבתי ספר רשמיים שאינם בעלי אישיות נפרדת ממשרד החינוך – משרד החינוך;

7.3.1.1.3 בבתי ספר שאינם רשמיים במאגרי מידע שאינם המנב"ס – בית הספר עצמו.

7.3.1.2 במסגרת השינוי האמור התחייב משרד החינוך ליטול אחריות על אופן ניהול המאגרים שברשותו, וכחלק מכך, ובהתאם להתחייבותו בפניי הרשם, פרסם משרד החינוך חוזר מנכ"ל בנושא.

[8] עמ' 12-13 לדו"ח רמו"ט לשנת 2008 http://www.justice.gov.il/NR/rdonlyres/D3CA8326-D3FB-4EA0-AB09-D0BE74A40161/15556/doch.pdf

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

7.3.2 קופות חולים

7.3.2.1 פורסמה הנחיה[9] המגדירה מחדש את הבעלות על מאגרי המידע המוחזקים בידי נותני שירותים רפואיים עבור קופות החולים.

7.3.3 עורכי דין

7.3.3.1 הרשם פנה לראש לשכת עורכי הדין במטרה להבהיר את החובות המוטלים על בעלי מאגרים שהם חברי הלשכה, וזאת בשל הנחיות שניתנו בעבר על ידי קודמתו בתפקיד.

7.4 נציין כי בימים אלו בוחן הרשם את הגדרת בעל מאגר המידע במאגרים שמשרד האוצר ומשרד הבריאות אחראיים על ניהולם בשיתוף עם משרדים אלו.

7.5 נתונים

7.5.1 בשנת 2009 הוגשו 408 בקשות רישום – ירידה של כ-13% בבקשות הרישום החדשות ביחס לשנת 2008.

7.5.2 בשנת 2009 נתקבלו 557 אישורי רישום בבקשות שהוגשו לרשם.

7.5.3 במהלך שנת 2009 נגבו 2,301,223 ש"ח עבור תשלום אגרות הרישום והאגרות התקופתיות. יצוין כי אגרות אלו הן אגרות ייעודיות אשר נועדו לממן, בין היתר, את פעילות ההסברה והאכיפה של רמו"ט בתחום הגנת הפרטיות, ועל כן הן מוטלות על הגורמים שיש בידם מאגרי מידע.

7.6 בהמשך להתחייבות רמו"ט בדוח של שנת 2008, כי עד סוף 2010 יבוצע מהלך לצמצום מספר המאגרים הממתינים לרישום, נבחנו מחדש 828 מאגרים (53% מכלל המאגרים שנדרשה לגביהם בדיקה), והטיפול בהם התחדש ובמקרים רבים אף הסתיים.

[9] הנחיה 1-2009 אשר פורסמה ביוני 2009 http://www.justice.gov.il/NR/rdonlyres/6F8F05C5-90E5-4A3A-A36F-6E5667C9A963/15037/12009.pdf

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

ט. דין וחשבון של רשם גורמים מאשרים בדבר הפעלת סמכויותיו לפי תקנה 16ל לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב–2001

מוגש לוועדת מדע וטכנולוגיה מכוח תקנה 16 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"א-2001

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

1. מבוא

1.1 עיקר תפקידי רשם גורמים מאשרים אמור להשתלב במסגרת סמכויות מחלקת הרישום והפיקוח של רמו"ט, ובכך לנצל את בצורה יעילה יותר את כוח האדם הפיקוחי ואת הניסיון בנושא זה. מהלך ארגוני זה הושלם במהלך שנת 2009.

1.2 פעילות הפיקוח בשנת 2009 מהווה המשך ישיר של פעילות הפיקוח בשנים 2007 עד 2008, תוך מיקוד בתחומים בהם התגלו ממצאים שמחייבים טיפול. בשנת 2009 הושם דגש משמעותי בפעילות הפיקוח על תחום אבטחת המידע וההגנה על המערכות הקריטיות של הגורם המאשר.

1.3 במרשם הגורמים המאשרים רשום כיום גורם מאשר אחד, חברת קומסיין בע"מ (להלן – קומסיין). במהלך שנת 2009 נערכו מספר בדיקות שמטרתן השלמה של תיקונים שהתחייבו לבצע בחברת קומסיין בעקבות ליקויים שהתגלו בשנים 2007 ו-2008.

1.4 בהתאם לדרישת הרשם החלה חברת קומסיין בפעילות מתקנת על-מנת להביא את רמת אבטחת המידע לרף הנדרש ולתקן את יתר הליקויים שנתגלו בתהליכי העבודה. תהליכי תיקון הליקויים בחברת קומסיין הושלמו לאחר עיכובים, במהלך השנה[10].

1.5 בתקופה זו החלה עלייה משמעותית בשימוש בחתימה אלקטרונית בשל תיקון חקיקה שמחייב שימוש בחתימה אלקטרונית לפעולות מסוימות מול רשות המסים. כתוצאה מכך נערכו פניות רבות יותר אל הרשם של לקוחות ומשתמשי קצה, בנושאים שונים הקשורים ביישום החוק, באופן זיהוי המשתמשים, ובהפעלת אמצעי החתימה.

2. פעולות פיקוח על הגורם המאשר

2.1 נתונים

2.1.1 בתחום חתימה אלקטרונית הגיעו לרמו"ט בשנת 2009 4 פניות[11], המהוות כ-3% מכלל הפניות שטופלו ברמו"ט בשנת 2009. נפתחו 2 תיקי פיקוח, המהווים כ-2% מכלל תיקי הפיקוח, ובוצעו 7 פיקוחים בשטח, המהווים כ-19% מכלל הפיקוחים בשטח.

2.2 פיקוחים בקומסיין

2.2.1 במהלך שנת 2009 בוצעו מספר פיקוחים לבדיקת ביצוע פעולות מתקנות בתחום אבטחת המידע של חברת קומסיין, שנדרשו ע"י הרשם, לאחר שמצא ליקויים בתחום זה.

2.2.2 כמו כן, בוצעו 2 פיקוחים בהוצאה לאור של לשכת עורכי הדין אשר קיבלה אישור מאת רשם גורמים מאשרים להיות גורם רושם עבור חברת קומסיין. בפקוחים נמצאו פערים בין הנהלים וההתחיבויות שאושרו לבין המצב בפועל. בעקבות זאת ניתנו הנחיות לפעולות מתקנות ולפיכך, החליט רשם

[10] ראו לעניין זה הערותינו לעניין חסרונה של סנקציה אפקטיבית על אי עמידה בהתחייבויות כלפי הרשם בסעיף 4 להלן.

[11] יצוין כי לאור שינויים באופן איסוף הנתונים, שונו ההגדרות של פניות ותיקי פיקוח ועל כן ההשוואה בין מספרים אלו למספרי שנים קודמות הינה בעייתית.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

גורמים מאשרים להאריך את האישור שניתן להוצאה לאור בשלושה חודשים בלבד, ובתנאים.

2.2.3 תיקון ליקויים שהתגלו בשנת 2007 – הנפקת תעודות שלא לפי התקנות

2.2.3.1 במהלך שנת 2009 נוהל מול חברת קומסיין הליך ארוך שמטרתו תיקון ליקוי שהתגלה על ידי הרשם בפעילותה של קומסיין[12] שהנפיקה תעודות אלקטרונית לפי החוק, תוך שימוש באמצעי חתימה באורך 1024 סיביות, בניגוד מפורש להוראת בניגוד להוראת תקנה 4 בתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה והגשת בקשות), התשס"ב-2001 (להלן – תקנות חומרה ותוכנה).

2.2.3.2 אף כי קומסיין צייתה להנחיה שלא להנפיק תעודות אלקטרוניות חדשות תוך שימוש באמצעי חתימה זה, נותרו מאות תעודות אלקטרוניות תקפות שהונפקו באופן כאמור.

2.2.3.3 עמדת הרשם היתה כי על קומסיין להחליף את התעודות האמורות לאלתר, אך על מנת למזער את הפגיעה בפעילותה ובשירות ללקוחות, הרשם הסכים לקיים הליך חלופי. במהלך המחצית הראשונה של 2008 התנהל דין ודברים, במסגרתו נקטה קומסיין בדחיות חוזרות ונשנות ובסופו של עניין נקבע תהליך עבודה שהתיר ביצוע פעולת ההחלפה מרחוק. תהליך זה היה אמור להסתיים בנובמבר 2008.

2.2.3.4 קומסיין לא עמדה בסיכומים, והציגה את האופן בו היא מבקשת לבצע את הפעולה רק בפברואר 2009. התהליך הטכנולוגי שהוצג יצר סיכונים חדשים לאבטחת המידע בקומסיין, ולכן נדרשו הרשם ויועץ אבטחת המידע שלו להתערב בהליך זה, ולקבוע בו שינויים נוספים.

2.2.3.5 רק במחצית 2009 החלה קומסיין לכאורה בהליך ביטול והחלפת התעודות, אולם בנובמבר 2009 התברר כי נותרו כ- 1008 תעודות שלא הוחלפו.

2.2.3.6 על רקע דברים אלה נמסרה לקומסיין התראה על התלייה של רישומה במרשם בהתאם לסעיף 14(א) לחוק, במידה שלא תבצע את ההחלפה עד ליום 31.12.09. במקביל נמסרו הודעות על מהלך עניינים זה לרשות ניירות ערך, רשות המסים, ופרויקט תהיל"ה במשרד האוצר, המייצגים את הגורמים המחייבים את הציבור בשימוש בתעודה אלקטרונית מולם.

2.2.3.7 רק בעקבות התראה זו ביצעה קומסיין את ההחלפה כנדרש.

2.2.4 הנחיה בעניין הנפקת תעודה אלקטרונית על גבי חומרה שלא נמכרת על ידי קומסיין

2.2.4.1 במהלך שנת 2009 הגיעו אל הרשם תלונות של חברת מחקר אלגוריתמים, ושל לקוחות שמעוניינים בשימוש במוצר של חברת מחקר אלגוריתמים, לשמירה ולביצוע חתימות אלקטרוניות.

2.2.4.2 על פי התלונה סירבה קומסיין להנפיק תעודות אלקטרוניות לפי החוק על גבי התקן לחתימה אלקטרונית שנמכר על ידי מחקר אלגוריתמים,

[12] שדווח בדוח השנתי לשנת 2007 ולשנת 2008.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

וזאת משיקולים לא עניינים. טענת חברת קומסיין בתגובה לתלונה היתה כי לשיטתה המוצר שנמכר על ידי חברת מחקר אלגוריתמים אינו עומד בדרישות תקנות חתימה אלקטרונית, בכך שאינו בעל תו תקן הנדרש בתקנות אלה.

2.2.4.3 נערכה על ידי הרשם בדיקה מקיפה ומעמיקה של טענות קומסיין ברמה העובדתית והמשפטית. על בסיס זה הנחה הרשם את חברת קומסיין, כי החוק והתקנות מאפשרות לבעל תעודה אלקטרונית – כלומר לקוח קצה – לבחור בהתקן החומרה שהוא מבקש, ואף מאפשרות לגורם המאשר להסתפק בהצהרה שלו בדבר התאמה של המוצר לתקן.

2.2.4.4 עמדת הרשם היא כי לפי החוק והתקנות הגורם המאשר יכול להנפיק תעודה על גבי התקן שלא הוא מוכר או משווק, אלא נמכר על ידי צד שלישי.

2.2.4.5 מאחר שהלקוחות בהם דובר בתלונה הינם לקוחות עסקיים, ולא צרכני קצה רגילים, נמצא כי אין מקום להתערבות של קומסיין בנושא זה. עם זאת, על מנת למנוע טענות כי הלקוחות אינם מבינים נושא זה, ועל מנת למנוע טענות לא רלבנטיות, נקבע טופס הצהרה של לקוח שעל בסיסו רשאי הגורם המאשר להנפיק תעודה אלקטרונית גם על גבי חומרה שלא הוא משווק.

2.2.5 הנפקת תעודות שלא על בסיס מסמך הנהלים המאושר

2.2.5.1 במסגרת בדיקת נושא חומרת ההנפקה התברר עוד כי קומסיין מספקת תעודות למורשה חתימה בתאגיד, המותקנות על גבי שרת חתימות, באופן שהשרת מבצע את החתימה באופן אוטומטי.

2.2.5.2 מסמך הנהלים התקף של חברת קומסיין באותה עת, לא הסדיר נושא זה כלל. בעקבות זאת נדרשה הנחיה מטעם הרשם להפסיק הנפקה של תעודות אלה מבלי הסדרה מתאימה במסמך הנהלים של חברת קומסיין.

2.2.5.3 במסגרת הדיונים על עדכון מסמך הנהלים של חברת קומסיין, שפורסם בשנת 2010, הוסדרה סוגיה זו.

2.2.6 הרחבת מתחם ההנפקה של קומסיין בתל-אביב

2.2.6.1 במהלך השנה אושרה לקומסיין הרחבת המתחם ההנפקה שלה ברמת החייל בתל-אביב בשל הרחבת פעילותה הנובעת מהגידול בביקוש לתעודות אלקטרוניות.

2.3 פעילות קביעת מדיניות בתחום החתימה האלקטרונית

2.3.1 חוות דעת בנושא אלגוריתמים לשימוש בחתימה אלקטרונית

2.3.1.1 בשנת 2009 התקשרה רמו"ט עם ד"ר בני פנקס, מומחה להצפנה מאוניברסיטת חיפה, לעניין קבלת המלצות בתחום אלגוריתמים ופרמטרים לאלגוריתמים לחתימה אלקטרונית. המלצות אלה פורסמו על ידי רמו"ט להערות הציבור ביום 3.8.09.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.3.1.2 ביום 22.09.09 קיימה רמו"ט דיון פומבי להצגת הממצאים ולשמיעת הערות מגופים מעוניינים. באופן כללי נשמעה תמיכה בהמלצותיו של ד"ר פנקס.

2.3.1.3 רכיב משמעותי מאוד בהמלצות, הינו הנחיה לעניין שימוש בפונקציות גיבוב (Hash), והצורך לעבור לפונקציות מתקדמות יותר[13].

2.3.1.4 המלצות אלה הובאו לידיעת הגורמים הרלבנטיים ובמהלך שנת 2010 יקבע תחילת תוקף להמלצות, אם כי הן כבר משמשות להכוונת תחום זה.

2.4 נייר עמדה בנושא חתימה אלקטרונית מאובטחת ומאושרת

2.4.1 עקב פניות חוזרות ועניין גובר בהבנת חוק חתימה אלקטרונית מהצד הטכנולוגי והמשפטי, הוחלט לפרסם מסמך ובו התייחסות למונחי היסוד של החוק, ובהם "חתימה אלקטרונית מאובטחת" (להלן - חתימה מאובטחת) ו-"חתימה אלקטרונית מאושרת" (להלן - חתימה מאושרת), ואת השימושים האפשריים בחתימה המאובטחת לעומת שימושי החתימה המאושרת[14].

2.4.2 המסמך הוכן לצורך מענה לשאלות נפוצות שהופנו לרשם הגורמים המאשרים בדבר משמעותה של החתימה המאובטחת, דרכי ההוכחה כי טכנולוגיה מסוימת מקיימת את תנאי הסף להכרה בחתימה מאובטחת, וההבדלים בין חתימה מאובטחת לחתימה מאושרת.

2.4.3 בין היתר עוסק המסמך גם בשימוש בחתימה אלקטרונית על גבי שרתי חתימות, וזאת עקב פניות שונות בנושא זה. במהלך 2010 יפורסם על ידי הרשם מסמך המשך בנושא זה.

2.5 שימוש בסיסמאות גישה (PIN) לצורך הפעלת אמצעי חתימה

2.5.1 במהלך 2009 בוצעה בדיקה משווה לעניין שינוי הוראות לפי התקנות לעניין שימוש בסיסמאות גישה להפעלת אמצעי חתימה. בתמצית, תקנות חתימה אלקטרונית דורשות כי במידה שנקבעה סיסמת גישה לצורך הפעלת אמצעי חתימה, סיסמא זו תעמוד בהוראות תקן ישראל 1495 חלק 3, ברמה הגבוהה.

2.5.2 לפי פניות שהגיעו לרשם, תקן זה מציב דרישות גבוהות שאינן רלבנטיות בהכרח לגישה לאמצעי המצוי בשליטתו הפיזית של אדם. לצורך גיבוש הנחיה בנושא בוצע מחקר משווה שמטרתו עדכון הוראות אלה. ההנחיה פורסמה בתחילת 2010.

[13] קישור לנייר העמדה: http://www.justice.gov.il/NR/rdonlyres/9F1794AC-E73E-4094-BDE9-49406DAE8F4A/16104/Esignaturealgorithms3.pdf

[14] http://www.justice.gov.il/NR/rdonlyres/735E0187-8A1C-4E4D-A1DB-D7B25A136296/18655/chatima_electronit_Reka1.pdf

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

י. דין וחשבון של רשם שירותי נתוני אשראי ושירותי מידע על עוסקים לשנת 2009

פיקוח על בעלי רישיונות שירותי נתוני אשראי

1.1 נתונים אודות תלונות ופעולות פיקוח

1.1.1 בתחום נתוני אשראי הגיעו לרמו"ט בשנת 2009 11 פניות[15], המהוות כ-9% מכלל הפניות, נפתחו 7 תיקי פיקוח, המהווים כ-6.5% מכלל תיקי הפיקוח, ובוצעו 10 פיקוחים בשטח, המהווים כ-27% מכלל הפיקוחים בשטח.

2. תיקי פיקוח נבחרים

2.1 דן אנד ברדסטריט – הודעה על פגם מהותי

2.1.1 ביום 29.7.09, הודיעה בעלת הרישיון חברת די אנד בי החברה לנתוני אשראי בע"מ על פגם מהותי במערכת התוכנה של החברה אשר גרם לכך שמידע שלילי אודות נושאי מידע הוצג למבקשי דוח אשראי למרות שחלפה התקופה על פי החוק שניתן היה להציגו בדוח האשראי.

2.1.2 לאחר בירור מול החברה, ובחינת מקור התקלה ומועד הדיווח עליה לרשם, עלה כי מספר נושאי המידע שנפגעו מהתקלה עמד על כ-1200.

2.1.3 על מנת ליידע את נושאי המידע שהועבר אודותם מידע שלא במסגרת הוראות החוק על חשיפת המידע אודותם לצד שלישי, הורה רשם שירותי נתוני אשראי לחברה לפנות לנושאי המידע האמורים וליידע אותם על התקלה, על מי נחשף למידע האמור ובאיזה תאריך.

2.1.4 ביום 13.12.09 הודיעה החברה על סיום משלוח ההודעות לנושאי המידע וכן דיווחה על כך מספר המכתבים החוזרים (10).

2.1.5 לאור עמידת החברה בחובותיה מכוח תקנה 80 לתקנות שירות נתוני אשראי, ולאור האחריות שלקחה על מעשיה הסתיים הפיקוח ללא הטלת סנקציה מינהלית.

2.1.6 בעקבות הפיקוח הוסכם עם מחלקת ייעוץ וחקיקה על שינוי תקנה 80.

2.2 BDI-coface – איסוף מידע חיובי

2.2.1 במהלך פיקוח בחברת BDI-coface הסתבר כי החברה נהגה לאסוף מידע חיובי מרגע שנתקבל מידע שלילי כלשהו אודות אדם גם אם אינו ניתן להצגה בדוח האשראי. יובהר, כי החקיקה קובעת כי בעל רישיון חייב להציג מידע חיובי בדוח האשראי מרגע שקיים מידע שלילי להצגה.

2.2.2 בגין ההפרה האמורה הוטל על החברה עיצום כספי בסך 67,300 ש"ח.

[15] יצוין כי לאור שינויים באופן איסוף הנתונים, שונו ההגדרות של פניות ותיקי פיקוח ועל כן ההשוואה בין מספרים אלו למספרי שנים קודמות היא בעייתית.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

2.3 קרדיט אינפורמיישיין אסוסיאיישן בע"מ – ליקויי אבטחת מידע

2.3.1 בפיקוח שנתקיים בבעלת הרישיון חברת קרדיט אינפורמיישיין אסוסיאיישן בע"מ נתגלו ליקויי אבטחת מידע חמורים. בסיומו של ההליך, ובעקבות הפיקוח, הודיעה החברה על הפסקת פעילותה כבעלת רישיון. ראה פירוט בהמשך.

2.3.2 הממצאים העלו כי על אף רמת אבטחת המידע הגבוהה שהייתה נהוגה בחברה עם קבלת הרישיון, החברה לא השכילה לשמר את הרמה הגבוהה של אבטחת המידע המצופה מבעל רישיון בתחום שירותי נתוני אשראי.

2.3.3 במהלך הפיקוח נתגלה גם כי בעל הרישיון לא דיווח במועד (תוך 30 יום) על שינוי שחל בבעלי השליטה בחברה. בגין הפרה זו הוטל על בעל הרישיון עיצום כספי בסך 12,900 ש"ח.

3. בתחום מתן הרישיונות

3.1 סיום פעילות בעל רישיון

3.1.1 בעקבות פעילות פיקוח אינטנסיבית, אשר חשפה ליקויים משמעותיים בהתנהלות בעל הרישיון, ולאור חוסר יכולתו של בעל הרישיון לעמוד בדרישות רמו"ט לתיקון הליקויים, הודיעה חברת קרדיט אינפורמיישיין אסוסיאיישן בע"מ, ביום 21.1.10, על הפסקת פעילותה כבעלת רישיון שירות נתוני אשראי.

3.1.2 ההליך האמור הוביל את הרשם לבחון מחדש את הוראות החוק הנוגעות לביטול רישיון בתחום שירות נתוני אשראי, והמלצותיו לתיקון חקיקה יועברו למחלקת ייעוץ וחקיקה במשרד המשפטים.

3.2 בחינת רישיון

3.2.1 חברת לב אמון יזמים בע"מ קיבלה רישיון לשירות נתוני אשראי (שלב א') ביום 14.8.08, אשר מאפשר לה איסוף מידע ממקורות המידע אך אוסר עליה להפיק דוחות אשראי למזמיני דוחות. נכון לסוף שנת 2009, החברה טרם עמדה בדרישות הרשם המהוות תנאי למתן הרישיון הסופי (שלב ב').

3.2.2 לאור משך הזמן שלקח לחברה לעמוד בדרישות הרשם, התריע הרשם בפני החברה על חובתה לעמוד בדרישות בהקדם שאם לא כן ישקול הרשם שלילת הרישיון שניתן.

קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

יא. נספח א' – נוסח תזכיר הצעת חוק הגנת הפרטיות (תיקון מס'...) (סמכויות אכיפה), התש"ע – 2009

<u>תזכיר חוק</u>

א. שם החוק המוצע

הצעת חוק הגנת הפרטיות (תיקון מס'...) (סמכויות אכיפה), התש"ע - 2009

ב.מטרת החוק המוצע והצורך בו

מטרת החוק המוצע היא שיפור כלי האכיפה ומנגנוני הפיקוח על קיום הוראות חוק הגנת הפרטיות, תשמ"א – 1981 (להלן – "החוק" או "חוק הגנת הפרטיות") הנוגעות לפרטיות במאגרי מידע. הזכות לפרטיות היא זכות חוקתית מוגנת על פי סעיף 7 לחוק-יסוד: כבוד האדם וחירותו. מטרת ההצעה היא להקנות ליחידת רשם מאגרי מידע, המופקדת על שמירה על פרטיות במאגרי מידע ועל קיום הוראות החוק הנוגעות למאגרי מידע, כלי פיקוח ואכיפה מתאימים ההולמים את מידת הסיכונים לפרטיות כיום, ואת המעמד הראוי של זכות זו במשפט הישראלי. ההצעה הנוכחית נועדה ליצור מנגנון אכיפה מנהלי יעיל שיהיה חלופי להליך הפלילי, במקרים בהם עולה חשש להפרה של הוראות החוק ולשפר את כלי האכיפה הפלילית ביחס להפרות החמורות יותר של החוק.

פרק ב' לחוק הגנת הפרטיות מסדיר את ההגנה על המידע במאגרי מידע ממוחשבים. הפרק מגדיר מהו מאגר מידע ומבחין בין סוגים שונים של מידע, מקים מוסד רישום ופיקוח על מאגרי מידע, וקובע הוראות לגבי איסוף המידע למאגרי המידע, אופן ניהול מאגרי מידע והשימוש במידע האגור בהם. תכלית ההסדר בפרק ב' היא למנוע פגיעה בפרטיות בהקשר של מאגרי מידע.

בהחלטת הממשלה מספר 4660 מיום 19.1.2006 הוקמה הרשות למשפט טכנולוגיה ומידע במשרד המשפטים (להלן – "הרשות"). ויחידת רשם מאגרי מידע לפי חוק הגנת הפרטיות מוזגה ארגונית לתוכה. מטרת החלטת הממשלה היתה בין היתר לשנות ולייעל את תחום הפיקוח המשפטי-טכנולוגי בנושא זה.

מאז תחילת פעולתה במתכונתה הנוכחית ערכה הרשות בדיקה יסודית של הכלים הדרושים להשגת מטרות אלה. זאת גם בהתאם לדין וחשבון שהגישה בינואר 2007 הועדה לבחינת החקיקה בתחום מאגרי המידע בראשות מר יהושע שופמן (להלן – "דו"ח ועדת שופמן"), שבו המליצה הוועדה להוסיף סמכויות אכיפה ופיקוח לרשם מאגרי המידע.

התזכיר המוצע משקף את תוצרי עבודה זו.

במהלך העשורים האחרונים, התרחשו שינויים טכנולוגיים ומשקיים מרחיקי לכת באופן שבו נאסף מידע, מעובד, ונעשים בו שימושים נוספים, וזאת במסגרת הפעילות השגרתית של ארגונים ויחידים. שינויים אלה יוצרים גם איומים חדשים על הזכות לפרטיות במידע. המציאות מלמדת שדליפת מידע רגיש, גישה לא מורשית למאגרים ושימוש במידע מתוכם למטרות זרות – הופכים לשכיחים יותר ויותר. היקפם ועוצמתם של האיומים וההפרות, מחייבים אפוא לעדכן גם את הסדר ההגנה על הפרטיות המפורט בפרק ב' לחוק.

עמד על כך גם בית המשפט העליון בבג"ץ 8070/98 **האגודה לזכויות האזרח בישראל נ' משרד הפנים**, פד"י נ"ח (4), 842 : עמ' 864 :

> **"ההתפתחויות בעולם המדע והטכנולוגיה הופכות מהירות יותר מאשר בעבר ועל כן ניצב המשפט בפני אתגרים חדשים בתכיפות גדולה מאשר בעידן קודם. כך קורה גם בתחום בו עסקינן. אמצעי המחשוב המודרניים והטכנולוגיה המתקדמת בתחום התקשורת מביאים עימם ברכה רבה בצד <u>סכנות גוברות לפגיעה בזכותו של האדם לפרטיות</u>"** (ההדגשות לא במקור).

סמכויות פיקוח ואכיפה אפקטיביות הן גם נדבך מרכזי במתכונת פעילותן של רשויות הגנת מידע דומות בעולם ובמסמכי מדיניות מרכזיים של האיחוד האירופי ושל הארגון לשיתוף פעולה ופיתוח כלכלי (OECD). בין המאפיינים הבולטים של רשויות הגנת מידע במדינות זרות, ניתן למנות סמכויות חיפוש וחקירה, סמכות רחבה למתן הוראות מסוגים שונים, ובהן דרישות מידע, הודעות אכיפה (צווי עשה ואל תעשה) וסמכויות פיקוח.

התוספות המוצעות בתזכיר נועדו לחזק במידה משמעותית את סמכויות הפיקוח, החקירה והאכיפה של יחידת הרשם.

נדבך מרכזי בתזכיר המוצע הוא יישום תובנות שנצברו בתחום **האכיפה החלופית** – שימוש בכלי אכיפה של המשפט המנהלי חלף נקיטת בהליכים פלילים. לצורך כך מוצע להקנות למפקחי יחידת הרשם כלים אפקטיביים לפיקוח שגרתי וכלים נוספים לבירור מהיר ויעיל במקרה של חשד להפרה. הכלים המוצעים נועדו להתמודד עם האתגרים הייחודים של אכיפת הגנת פרטיות במאגרי מידע ממוחשבים, שהמרכזים שבהם :

- כמעט לעולם יבוצעו ההפרות בדלת אמותיו של המפר, לרוב אין ראיה "חפצית" לקיומן ובשל טבעה של המאטריה ומידת התחכום של העוסקים בה ויתרונם בהכרת המערכת שלהם – יכולות טשטוש העקבות, בזמן קצר, קלות מאוד ;
- ביצוע ההפרות הוא פשוט ועלות ביצוע ההפרה ושכפול עותקים "מפרים" של המידע – זניחה, ומנגד הרווח הכספי מביצוען - גדול ;
- מרגע שבוצעה ההפרה (כגון שדלף מידע ממאגר) כמעט בלתי אפשרי לתקנה. מכאן, שיש נסיבות שבהן נדרשת תגובה ופעולה מיידית, במסגרת פיקוח, המאפשרת איסוף ראיות או הקפאת מצב.
- לא מדובר בפעילות המיוחדת לסקטור מסוים במשק. מאגרי מידע מוחזקים ופועלים בתחומים מגוונים – בסקטור הציבורי והפרטי, בכל תחומי המשק והחברה ובידי תאגידי ענק כמו גם אזרחים מן השורה.

המהלך המשלים הוא קביעה של רשימה של הפרות המכסה את המעשים היוצרים סיכון להגנת הפרטיות במאגרי מידע, או בהם התממש הסיכון, ויש צורך בנקיטת אמצעי אכיפה.

בנוסף, ביחס להתנהגויות שבהן מידת האנטי חברתיות רבה יותר או שהן החמורות יותר, כגון שימוש במידע שלא למטרה לשמה נמסר, וראויות להתמודדות במישור הדין הפלילי, מוצע להשלים את הכלים הקיימים בידי הרשות בכלי חקירה פלילים מקובלים ולקבוע עבירות מסוימות המגלמות את המעשים החמורים ביותר ביחס לפגיעה בפרטיות במאגרי מידע.

ג. השפעה על החוק הקיים

בתזכיר מוצע לתקן את חוק הגנת הפרטיות כמפורט להלן:

- הוספת פרק ד'1 המתקן את סמכויות הפיקוח המסורות לרשם ולעובדי יחידתו, ומוסיף להם סמכויות בירור של הפרות מינהליות וסמכויות של חקירה פלילית;
- הוספת סעיף 17ב1 המסמיך את הרשם לקבוע תקינת אבטחת מידע אישית באמצעות צו אבטחת מידע;
- תיקון סעיף 10 לחוק כך שתעודכן ותשודרג הכשרת המפקחים שהרשם מוסמך למנות ותיקבע ההכשרה שתינתן לחוקרים;
- הוספת פרק ד'2 המצייד את הרשם בכלי אכיפה חלופיים לענישה הפלילית: הטלת עיצום כספי, משלוח התראה ודרישת התחייבות להימנע מהפרה;
- הוספת פרק ד'3 הקובע רשימה של עבירות הנוגעות לשימוש במידע ובמאגרי מידע, ובמקביל ביטול סעיף 31א לחוק שעניינו "עונשין בעבירות של אחריות קפידה".

ד.השפעת החוק המוצע על תקציב המדינה ועל התקן המנהלי

לחוק המוצע לא צפויה השפעה תקציבית בנוסף על העלות והוספת התקנים שהתחייבו מהקמת הרשות למשפט טכנולוגיה ומידע, מכוח החלטת הממשלה מספר 4660 מיום 19.1.2006.

ה. להלן נוסח החוק המוצע ודברי הסבר:

שינוי מונחים

1. בחוק הגנת הפרטיות, התשמ"א-1981[16] (להלן – החוק העיקרי), בכל מקום, במקום "פנקס" יבוא "מרשם" ובמקום "רשם" יבוא "ממונה".

תיקון סעיף 7

2. בסעיף 7 לחוק העיקרי, במקום ההגדרה "רשם" יבוא:

""**ממונה על הגנת מידע**", "**הממונה**" – מי שמתקיימים בו תנאי הכשירות למינוי שופט של בית משפט מחוזי והממשלה מינתה אותו, בהודעה ברשומות, לפקח על הגנת המידע במאגרי מידע לפי הוראות חוק זה";".

תיקון סעיף 10

3. בסעיף 10 לחוק העיקרי -

(1) במקום סעיפים קטנים (ה) עד (ה1) יבוא:

"(ה) הממונה יעמוד בראש יחידת הפיקוח והוא רשאי להסמיך חוקר או מפקח מבין עובדי המדינה בסמכויות לפי חוק זה, כולן או חלקן, אם התקיימו בו כל אלה:

(1) משטרת ישראל לא הודיעה, בתוך שלושה חודשים מפנייתו של הממונה אליה, כי היא מתנגדת להסמכתו מטעמים של ביטחון הציבור, לרבות בשל עברו הפלילי;

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה שר המשפטים בהסכמת השר לביטחון הפנים; לא יוסמך חוקר או מפקח בסמכויות חדירה לחומר מחשב, או העתקתו אלא אם הוא בעל תפקיד המיומן לביצוע פעולות כאמור, כמשמעותו בסעיף 23א לפקודת סדר הדין הפלילי (מעצר וחיפוש)[נוסח חדש], התשכ"ט – 1969[17] ;

(3) הוא עומד בתנאי כשירות נוספים ככל שהורה שר המשפטים בהסכמת השר לבטחון הפנים."

(2) סעיף קטן (ז) - בטל.

תיקון סעיף 17ב

4. בסעיף 17ב לחוק העיקרי -

(1) במקום כותרת השוליים יבוא "האחראי על הגנת מידע";

---

[16] ס"ח התשמ"א, עמ' 128; התשס"ז, עמ' 368.
[17] ס"ח התש"ל, עמ' 16; התשס"ה, עמ' 526.

(2) בסעיף קטן (א) במקום "ממונה על אבטחת מידע (להלן – הממונה)" יבוא "אחראי על הגנת מידע";

(3) בסעיפים קטנים (ב) – (ג) במקום "ממונה" יבוא "האחראי על הגנת המידע".

הוספת סעיף 17ב1 5. אחרי סעיף 17ב לחוק העיקרי יבוא:

"צו אבטחת מידע 17ב1. (א) הממונה או עובד המדינה שהוא הסמיך לעניין סימן זה, רשאי להורות בצו למי שחייב באבטחת מידע לפי סעיף 17, לנקוט פעולות שיפורטו על ידו בנוגע לאבטחת מידע של המאגר (בסעיף זה - צו אבטחת מידע) לרבות הוספה של אמצעי אבטחת מידע.

(ב) לא יוציא הממונה צו אבטחת מידע אלא לאחר שניתנה הזדמנות למי שכלפיו מופנה הצו להשמיע את טענותיו.

(ג) בצו אבטחת המידע תיקבע התקופה לביצוע הפעולות המפורטות בו, אשר תחילתה עם מסירת הצו לאדם המחויב בו.

(ד) המצאת צווי אבטחת מידע תהיה כאמור בסעיף 237 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982[18], בשינויים המחויבים."

הוספת פרקים ד'1 עד ד'3 6. לפני סעיף 24 לחוק העיקרי יבוא:

"פרק ד1 – סמכויות פיקוח, בירור מנהלי וחקירה

הגדרות 23ט. בפרק זה -

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995[19];

[18] ס"ח התשמ"ב, עמ' 41.
[19] ס"ח התשנ"ה, עמ' 366.

"חוק המעצרים" - חוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו-1996[20];

"חומר מחשב", "מחשב" - כהגדרתם בחוק המחשבים;

"חפץ" – כמשמעותו בפקודת המעצר והחיפוש;

"מסמך" – לרבות פלט כהגדרתו בחוק המחשבים;

"נתוני מערכת" – אחד מאלה:

(1) נתונים אודות החזקה וניהול של מידע ושל מאגרי מידע ואודות השימוש בהם, הדרושים לבירור קיום הוראות פרקים ב', ד' ו- ד'3, ובלבד שאין בהם *מידע* כהגדרתו בסעיף 7;

(2) מסמכים שמחזיק אדם לפי סעיף 8א(א) ורישומים אחרים שחייב אדם לשמור לפי חוק זה, אגב ניהול של מאגר מידע, אחזקתו או שימוש בו;

"פקודת המעצר והחיפוש" – פקודת סדר הדין הפלילי (מעצר וחיפוש)[נוסח חדש], תשכ"ט – 1969[21].

סימן א': סמכויות פיקוח

סמכויות מפקח

23י. (א) לשם פיקוח על מילוי הוראות פרקים ב', ד' ו- ד'3 והתקנות לפיהם, רשאי הממונה או מפקח שהוסמך על ידו:

(1) לדרוש מכל אדם למסור לו את שמו ומענו ולהציג בפניו תעודת זהות או תעודה רשמית אחרת המזהה אותו;

(2) לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך;

[20] ס"ח התשנ"ו, עמ' 338; התשס"ז עמ' 93.
[21] ס"ח התש"ל, עמ' 16; התשס"ה, עמ' 526.

(3) לדרוש מכל אדם הנוגע בדבר להציג בפניו או למסור לו עותק מחומר מחשב הכולל נתוני מערכת או מידע מדגמי; מידע מדגמי לפי סעיף זה לא ייאסף בהיקף העולה על הנדרש למימוש תכליות הפיקוח;

(4) להיכנס למקום שיש יסוד סביר להניח שקיים בו מאגר מידע או שנעשה בו שימוש במאגר מידע ובלבד שלא ייכנס למקום המשמש למגורים אלא על פי צו של בית משפט.

(ב) לא ניתן היה לקיים את הפיקוח באמצעים המפורטים בסעיף קטן (א) ולא ניתן היה לדחות את קבלת המידע למועד אחר, רשאי הממונה או מי שמתקיימים בו תנאי הכשירות לשמש כממונה והממונה הסמיכו לעניין זה בהודעה ברשומות (להלן – ממלא מקום הממונה), להתיר למפקח:

(1) לחדור לחומר מחשב שיש בו נתוני מערכת, להעתיקו ולהפיק ממנו פלט, ולצורך כך גם לבצע חדירה לחומר מחשב הנדרשת במישרין לשם חדירה לנתוני המערכת (בסעיף זה – חדירת אגב);

(2) לחדור לחומר מחשב, להעתיק מידע מדגמי, ולהפיק ממנו פלט וכן לבצע חדירת אגב לצורך חדירה לחומר מחשב כאמור.

(ג) מידע מדגמי שנמסר או נאסף לפי סעיף זה, יימחק ממאגרי המידע של הממונה כאשר אינו נדרש עוד באופן סביר להמשך הליכי הפיקוח, ולכל היותר תוך 3 שנים ממועד מסירתו או איסופו, אלא אם כן המידע נדרש לצורך הליכים לפי סימנים ב' או ג' לפרק זה.

סימן ב': סמכויות בבירור מינהלי

צו לחיפוש ולחדירה לחומר מחשב

23יא. התעורר יסוד סביר להניח כי בוצעה הפרה של הוראה מהוראות סעיף 23טז, רשאי הממונה או ממלא מקומו לבקש מבית המשפט צו חיפוש ותפיסה כאמור בסעיפים 23 ו– 24 לפקודת מעצר וחיפוש וצו חדירה לחומר מחשב, כאמור בסעיף 23א לפקודת מעצר וחיפוש, ולבצעם בעצמו או באמצעות מפקח.

צו להצגת חפץ והתייצבות לבירור

23יב. (א) היה לממונה יסוד סביר להניח כי בוצעה הפרה של הוראה מהוראות סעיף 23טז(ב) או (ג), רשאי הממונה או ממלא מקומו -

(1) לבקש מבית המשפט לתת צו לאדם, שלפי ההנחה נמצא בחזקתו או ברשותו חפץ או מסמך הדרוש לצורך בירור ההפרה, להציג את החפץ או המסמך או להמציאו לממונה או למפקח בשעה ובמקום הנקובים בהזמנה;

(2) לזמן כל אדם שעשויה להיות לו ידיעה הנוגעת להפרה, או לנסיבותיה של ההפרה, או לעובדות שיכולות להביא לגילויו של המפר, ולערוך עימו בירור בקשר למידע כאמור; זומן אדם שאינו מפר לכאורה, יזמנו החוקר למועד סביר שיתואם עימו.

(ב) זומן אדם לבירור כאמור בסעיף קטן (א)(2) – ישיב לשאלות שיישאל במסגרת הבירור.

(ג) זומן אדם בהתאם לסעיף קטן (א)(2) ולא התייצב, רשאי הממונה או ממלא מקומו לבקש מבית המשפט לכפות עליו ציות או לענוש אותו בשל הפרת חובת ההתייצבות, כאמור בסעיף 73 לחוק בתי המשפט [נוסח משולב], התשמ"ד-1984[22], כאילו זומן להעיד בפני בית משפט.

חיפוש וחדירה לחומר מחשב ללא צו

23יג. התעורר אגב פיקוח או אגב ביצועו של צו כאמור בסעיף 23יא, יסוד סביר להניח כי בוצעה הפרה נוספת של הוראות סעיפים קטנים 23טז(ב)(1), (3), (5), (7) עד (10) או (12), או (ג), ושוכנע הממונה או ממלא מקומו כי נדרש הדבר באופן מיידי לצורך מניעת המשך הפרת הוראות החוק או לצורך מניעת חשש להעלמת ראיה או שיבוש הפיקוח וכי אין סיפק לבקש צו מבית המשפט לפי סעיף 23יא, רשאי הוא להתיר למפקח, בכתב ומנימוקים שיירשמו, לבצע את הפעולות הבאות, או לבצע אותן בעצמו:

(1) לערוך, ללא צו, חיפוש במקום שיש יסוד סביר להניח שקיים בו מאגר מידע או שנעשה בו שימוש במאגר מידע או שקיימת בו ראיה לקיום מאגר או לשימוש כאמור, ולתפוס כל חפץ העשוי לשמש ראיה לביצוע ההפרה;

(2) להעתיק, ללא צו, חומר מחשב ולבצע חדירה לחומר מחשב הנדרשת במישרין לצורך העתקתו, ובלבד שיפנה לבית המשפט ללא דיחוי לצורך קבלת הוראות לגבי חומר המחשב שהועתק.

[22] ס"ח התשמ"ד עמ' 198; התשס"ט, עמ' 115.

אופן ביצוע חדירה לחומר מחשב והעתקתו

23יד. (א) פעולות העתקת חומר מחשב והחדירה אליו לפי סימן זה יבוצעו בידי מפקח שהוסמך לביצוע חדירה לחומר מחשב לפי סעיף 10(ה) (להלן – מפקח מוסמך) ויתועדו בדוח שיערוך מי שביצע את אותן הפעולות.

(ב) על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סימן זה יחולו סעיפים 24(א)(1), (ב), 26-28, 31 ו-45 והוראות הפרק הרביעי לפקודת המעצר והחיפוש בשינויים המחויבים, ובשינוי זה: בכל מקום, במקום "שוטר" יקראו "מפקח", ובמקום "קצין" יקראו "הממונה או ממלא מקומו".

(ג) לצורך ביצוע חדירה לחומר מחשב שמותר לבצעה לפי סימן א' או לפי סימן זה, יהיה מפקח רשאי להסתייע במומחה, גם אם אינו עובד מדינה, אם לצורך החדירה נדרש ניסיון, ידע או אמצעים שאין לעורך החיפוש, ובלבד שהמפקח נכח במקום בעת ביצוע הפעולות על ידי המומחה, ופיקח על ביצוען; המפקח יודיע למומחה על חובת הסודיות המוטלת עליו כאמור בסעיף קטן (ד); כמו כן יהיה המפקח רשאי לדרוש מכל אדם המצוי במקום לבצע על פי הנחיותיו ובמגבלת סמכויותיו על פי חוק זה פעולה בחומר מחשב, אם יש לו יסוד סביר להניח כי לאותו אדם יש ניסיון, ידע או אמצעים שאין למפקח ואשר דרושים לביצוע החדירה (להלן – מסייע).

(ד) מומחה ומסייע שסייעו למפקח כאמור בסעיף קטן (ג), חייבים לשמור בסוד כל מידע שהגיע אליהם עקב או תוך כדי פעולות הסיוע, ולא ימסרו אותו אלא ככל שהדבר נדרש לצורך הליכי חקירה ומשפט.

סימן ג': סמכויות חקירה

סמכויות חקירה

23טו. (א) התעורר חשד לביצוע עבירה לפי פרקים ב', ד' או ד'3, יהיו לממונה או לחוקר כל סמכויות הפיקוח לפי סימן א' לפרק זה, וכן רשאי הממונה או החוקר -

(1) לחקור כל אדם הקשור לעבירה, או שעשויות להיות לו ידיעות הנוגעות אליה; על חקירה לפי פסקה זו יחולו הוראות סעיפים 2 ו-3 לפקודת הפרוצדורה הפלילית (עדות)[23] והוראות חוק סדר הדין הפלילי (חקירת חשודים), התשס"ב-2002[24], בשינויים המחוייבים;

(2) לדרוש מכל אדם להתייצב לפניו או לפני חוקר אחר לשם מסירת כל פרט, מסמך או ידיעה הנוגעים לאותה עבירה או לשם חקירה וכן לדרוש מכל אדם להתלוות אליו למקום שבו ייעשו המסירה או החקירה;

(3) לדרוש מכל אדם שלפי ההנחה נמצא בחזקתו או ברשותו חפץ או מסמך הדרוש לצורך בירור העבירה, להציג את החפץ או המסמך או להמציאו לממונה או לחוקר בשעה ובמקום הנקובים בהזמנה; על סעיף קטן (2) ועל סעיף קטן זה יחולו הוראות סעיף 23יב(ב) ו - (ג) בשינויים המחוייבים;

(4) לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא חפץ קשור לעבירה;

(5) לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב ע"פ סעיף 23 - 24 לפקודת מעצר וחיפוש ולבצעו.

---

[23] ס"ח התשכ"ה, עמ' 53; התשס"ה עמ' 498.
[24] ס"ח התשס"ב, עמ' 468; התשס"ח עמ' 572.

(ב) (1) על תפיסה לפי סעיף קטן (א)(4) יחולו הוראות הפרק הרביעי לפקודת המעצר והחיפוש, בשינויים המחוייבים, ובשינוי זה: בכל מקום, במקום "שוטר" יקראו "חוקר", ובמקום "קציין" יקראו "הממונה או ממלא מקומו".

(2) נתפס מסמך של אדם בהתאם לסעיף קטן (א)(4), יאפשר לו התופס, אם ביקש זאת, להעתיק את המסמך.

(3) הממונה רשאי לדחות את העתקת המסמך כאמור בפסקה (2), לתקופה של עד שלושה חודשים מיום התפיסה, אם לדעתו העתקת המסמך עלולה לשבש חקירה בקשר לעבירה לפי חוק זה;

(4) בית משפט רשאי, לבקשת הממונה, להאריך את התקופה האמורה בפסקה (3) בתקופות נוספות, ורשאי הוא לעשות כן בתנאים;

(5) על החלטת הממונה לפי פסקה (3), רשאי האדם שמסמכו נתפס לערור בפני בית המשפט.

(ג) לצורך חקירת עבירה על הוראות סעיפים 16 או 23מ עד 23מב, יהיו נתונות לממונה ולחוקר הסמכויות המפורטות בסעיף 23יג, בשינויים המחויבים; לא ניתן היה למנוע את העלמת הראיה או את שיבוש החקירה בדרך של העתקת חומר מחשב כאמור בסעיף 23יג, יהיה חוקר רשאי לחדור לחומר מחשב אף שלא לצורך העתקתו בלבד, ללא צו שופט, ולאחר אישור בכתב מאת הממונה, ובלבד שחומר מחשב שנתפס או הועתק תוך כדי ביצוע סמכות כאמור ולא הופק ממנו פלט במעמד החדירה לפי סעיף זה, לא יעשה בו שימוש נוסף לצורך חקירה עבירה או בירור הפרה של הוראות חוק זה אלא לאחר קבלת אישור בית המשפט.

(ד) על חיפוש לפי סעיף זה יחולו הוראות סעיפים 24(א)(1)ו-(ב), 26 עד 28, 31 ו-45 לפקודת מעצר וחיפוש, בשינויים המחויבים.

(ה) היה לממונה או לחוקר יסוד סביר לחשד שאדם ביצע עבירה לפי פרקים ב', ד' או ד'3, יהיה רשאי לעכב אותו כדי לחוקרו במקום הימצאו, ואם לא ניתן לחקור אותו במקום הימצאו יהיה רשאי לדרוש מאותו אדם להתלוות אליו למשרדי הממונה או לזמנו למשרדי הממונה למועד אחר שיקבע; הוראות סעיפים 23(ב), 66, ו– 72 עד 74 לחוק המעצרים, יחולו על עיכוב לפי סעיף קטן זה בשינויים המחויבים, ולעניין זה - יראו חוקר כ"שוטר" לפי חוק המעצרים, יראו את הממונה כ"קצין הממונה" לפי חוק המעצרים, ויראו את משרדי הרשות שהוכרזו בהודעה ברשומות כ"תחנת משטרה" לפי חוק המעצרים.

פרק ד2: עיצום כספי

סימן א': הטלת עיצום כספי

עיצום כספי

23טז. (א) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בסכום הקבוע בתוספת בהתאם לגודל מאגר המידע ולסוג המידע אשר בזיקה אליהם בוצעה ההפרה (להלן – הסכום הבסיסי):

(1) ניהל או החזיק מאגר מידע החייב ברישום מבלי שנרשם או הוגשה בקשה לרישום בניגוד להוראות סעיף 8(א);

(2) ניהל או החזיק מאגר מידע המשמש לשירותי דיוור ישיר, מבלי שיש בידו רישום המציין מקור אוסף הנתונים המשמש לצרכי מאגר המידע במאגר ומועד קבלתו, וכן למי מסר אוסף כאמור, בניגוד להוראות סעיף 17ה;

(3) כלל פרטים לא נכונים בבקשה לרישום מאגר מידע שהוגשה לפי סעיף 9;

(4) לא הודיע לממונה על שינויים בפרטים המנויים בסעיף 9(ב) או בפרטים שנקבעו לפי סעיף 9(ג), בניגוד להוראת סעיף 9(ד);

(5) מסר פרטים לא נכונים במענה לדרישת מידע של הממונה או המפקח לפי סעיף 23י;

(6) החזיק ברשותו חמישה מאגרי מידע לפחות ולא קיים את חובת הדיווח השנתי הקבועה בסעיף 17א;

(7) לא פרט כי הוא מוסר מידע דרך קבע ממאגר מידע בניגוד להוראות סעיף 23ד(א), לא קיים רישום של המידע שמסר ממאגר מידע בניגוד להוראות סעיף 23ד(ב), או לא הודיע לממונה כי הוא מקבל מידע דרך קבע בניגוד להוראות סעיף 23ד(ג).

(ב) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בשיעור כפל הסכום הבסיסי הקבוע בגין הפרה מסוגה בתוספת:

(1) פנה לאדם אחר לשם קבלת מידע לשם החזקתו או שימוש בו במאגר מידע, מבלי שמסר לו הודעה כנדרש בסעיף 11;

(2) סירב לאפשר לאדם שמידע אודותיו מצוי במאגר לעיין במידע, בניגוד להוראות סעיף 13;

(3) לא תיקן מידע המצוי במאגר מידע שבהחזקתו בניגוד להוראות סעיף 14(ד);

(4) לא הודיע למבקש על סירוב לתקן מידע המצוי במאגר מידע שבבעלותו, בניגוד להוראות סעיף 14(ג);

(5) ביצע שינוי במידע שברשותו אודות אדם במאגר מידע, מבלי שהודיע עליהם לכל מי שקיבל את המידע בניגוד לסעיף 14(ב);

(6) פנה לאדם בדיוור ישיר באופן שאינו עומד בהוראות סעיף 17ו(א) לחוק;

(7) לא נענה לבקשתו של אדם כי מידע המוחזק אודותיו במאגר מידע לדיוור ישיר יימחק, בניגוד לסעיף 17ו(ד);

(8) לא נענה לבקשתו של אדם, כי מידע המוחזק אודותיו במאגר מידע לדיוור ישיר, לא יימסר לאדם, לסוג בני אדם, בניגוד להוראות סעיף 17ו(ד);

(9) החזיק במאגרי מידע של בעלים שונים מבלי שהתקיימו הוראות סעיף 17א(א);

(10) הפר הוראות הממונה בצו אבטחת מידע בניגוד להוראות סעיף 17ב1;

(11) לא מינה אחראי על הגנת מידע, בניגוד לסעיף 17ב;

(12) ניהל מאגר מידע המשמש לשירותי דיוור ישיר, בלא שהיה רשום במרשם ובלא שאחת ממטרותיו הרשומות היא שירותי דיוור ישיר, בניגוד לסעיף 17ד.

(ג) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בשיעור של פי ארבעה מהסכום הבסיסי הקבוע בגין הפרה מסוגה בתוספת:

(1) בהיותו בעל מאגר מידע או מחזיק בו, השתמש במידע מתוך המאגר שלא למטרה לשמה נמסר, בניגוד לסעיף 23מ;

(2) השתמש במידע ממאגר מידע ללא הרשאה כדין מבעל המאגר או תוך חריגה ממנה, בניגוד לסעיף 23מא; לעניין זה, מי שברשותו עותק של מאגר מידע, או חלק מהותי ממנו – יראו אותו כמשתמש במידע כאמור, אלא אם הוכיח אחרת.

הודעה על כוונת חיוב

23יז. (א) היה לממונה יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 23טז (בפרק זה - המפר), ובכוונתו להטיל עליו עיצום כספי לפי אותו סעיף, רשאי הוא למסור למפר הודעה על הכוונה להטיל עליו עיצום כספי (בפרק זה – הודעה על כוונת חיוב).

(ב) בהודעה על כוונת חיוב יציין הממונה בין השאר את אלה:

(1) המעשה או המחדל (בפרק זה - המעשה), המהווה את ההפרה;

(2) סכום העיצום הכספי והתקופה לתשלומו;

(3) זכותו של המפר לטעון טענותיו בפני הממונה לפי הוראות סעיף 23יח;

(4) שיעור התוספת על העיצום הכספי בהפרה נמשכת או בהפרה חוזרת לפי הוראות סעיף 23כ.

זכות טיעון

23יח. מפר שנמסרה לו הודעה על כוונת חיוב לפי הוראות סעיף 23טז רשאי לטעון טענותיו, בכתב, בפני הממונה, לענין הכוונה להטיל עליו עיצום כספי ולענין סכומו, בתוך 30 ימים ממועד מסירת ההודעה.

החלטת הממונה ודרישת חיוב

23יט. (א) טען המפר טענותיו בפני הממונה לפי הוראות סעיף 23יח, יחליט הממונה, לאחר ששקל את הטענות שנטענו, האם להטיל על המפר עיצום כספי, ורשאי הוא להפחית את סכום העיצום הכספי לפי הוראות סעיף 23כא.

(ב) (1) החליט הממונה לפי הוראות סעיף קטן (א) להטיל על המפר עיצום כספי, ימסור לו דרישה לשלם את העיצום הכספי (להלן – דרישת חיוב); בדרישת החיוב יציין הממונה, בין השאר, את סכום העיצום הכספי המעודכן והתקופה לתשלומו.

(2) החליט הממונה לפי הוראות סעיף קטן (א) שלא להטיל על המפר עיצום כספי, ימסור לו הודעה על כך.

(ג) לא ביקש המפר לטעון טענותיו לפי הוראות סעיף 23יח, בתוך 30 ימים מיום שנמסרה לו ההודעה על כוונת חיוב, יראו הודעה זו, בתום 30 הימים האמורים, כדרישת חיוב שנמסרה למפר במועד האמור.

הפרה נמשכת והפרה חוזרת

23כ. (א) בהפרה נמשכת יווסף על העיצום הכספי החלק החמישים שלו לכל יום שבו נמשכת ההפרה.

(ב) בהפרה חוזרת יווסף על העיצום הכספי שניתן היה להטיל בשלה אילו היתה הפרה ראשונה, סכום השווה לעיצום הכספי כאמור; לענין זה, "הפרה חוזרת" – הפרת הוראה מההוראות לפי חוק זה כאמור בסעיף 23טז, בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע.

סכומים מופחתים

23כא. (א) הממונה אינו רשאי להטיל עיצום כספי בסכום הנמוך מהסכומים הקבועים בסימן זה, אלא לפי הוראות סעיף קטן (ב).

(ב) שר המשפטים רשאי לקבוע מקרים, נסיבות ושיקולים שבשלהם ניתן יהיה להטיל עיצום כספי בסכום הנמוך מהקבוע בסימן זה, בשיעורים שיקבע.

סכום מעודכן של העיצום הכספי

23כב. (א) העיצום הכספי יהיה לפי סכומו המעודכן ביום מסירת הודעת החיוב, ולגבי מפר שלא טען טענותיו בפני הממונה כאמור בסעיף 23יט (ג) – ביום מסירת ההודעה על כוונת החיוב; הוגשה עתירה לבית המשפט לעניינים מינהליים לפי סעיף 23לד, ובית המשפט הורה על עיכוב תשלומו של העיצום הכספי - יהיה העיצום הכספי לפי סכומו המעודכן ביום ההחלטה בעתירה.

(ב) סכום העיצום הכספי יעודכן ב-1 בינואר בכל שנה (בסעיף קטן זה – יום העדכון), בהתאם לשיעור עליית המדד הידוע ביום העדכון לעומת המדד שהיה ידוע ביום .....[תחילתו של חוק זה]; הסכום האמור יעוגל לסכום הקרוב שהוא מכפלה של 10 שקלים חדשים; לענין זה, "מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה.

(ג) הודעה על סכום העיצום הכספי המעודכן לפי סעיף קטן (ב), תפורסם ברשומות.

שינוי התוספת

23כג. שר המשפטים, באישור ועדת החוקה, חוק ומשפט של הכנסת, רשאי להוסיף בצו סוגי מידע לקבוצה ב' בתוספת.

המועד לתשלום העיצום הכספי

23כד. העיצום הכספי ישולם בתוך 30 ימים מיום מסירת דרישת החיוב כאמור בסעיף 23יט.

הפרשי הצמדה וריבית

23כה. לא שולם עיצום כספי במועד, ייווספו עליו לתקופת הפיגור הפרשי הצמדה וריבית, עד לתשלומו.

גביה

23כו. עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו תחול פקודת המסים (גביה)[25].

סימן ב': התראה מינהלית

התראה מינהלית

23כז. (א) היה לממונה יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 23טז, והתקיימו נסיבות שקבע הממונה, באישור היועץ המשפטי לממשלה, רשאי הוא, במקום להמציא לו הודעה על כוונת חיוב ולהטיל עליו עיצום כספי, לפי הוראות סימן א', להמציא לו התראה מינהלית לפי הוראות סימן זה.

(ב) בהתראה מינהלית יציין הממונה מהו המעשה המהווה את ההפרה, יודיע למפר כי עליו להפסיק את ההפרה וכי אם ימשיך בהפרה או יחזור עליה יהא צפוי לעיצום כספי בשל הפרה נמשכת או הפרה חוזרת, לפי העניין, כאמור בסעיף 23כט, וכן יציין זכותו של המפר לבקש את ביטול ההתראה לפי הוראות סעיף 23כח.

בקשה לביטול התראה מינהלית

23כח. (א) נמסרה למפר התראה מינהלית כאמור בסעיף 23כז, רשאי הוא לפנות לממונה בכתב, בתוך 30 ימים, בבקשה לבטל את ההתראה בשל אחד מטעמים אלה:

(1) המפר לא ביצע את ההפרה;

(2) המעשה שביצע המפר, המפורט בהתראה, אינו מהווה הפרה.

[25] חא"י, כרך ב' עמ' (ע) 1374, (א) 1399

(ב) קיבל הממונה בקשה לביטול התראה מינהלית, לפי הוראות סעיף קטן (א), רשאי הוא לבטל את ההתראה או לדחות את הבקשה ולהשאיר את ההתראה על כנה; החלטת הממונה תינתן בכתב, ותימסר למפר, בצירוף נימוקים.

הפרה נמשכת והפרה חוזרת לאחר התראה

23כט. (א) נמסרה למפר התראה מנהלית לפי הוראות סעיף זה והמפר המשיך להפר את ההוראה שבשלה נשלחה לו ההתראה, ימסור לו הממונה דרישת חיוב בשל הפרה נמשכת כאמור בסעיף 23כ.

(ב) נמסרה למפר התראה לפי הוראות סעיף זה והמפר חזר והפר את ההוראה שבשלה נשלחה לו ההתראה, בתוך שנתיים מיום מסירת ההתראה, יראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 23כ, והממונה ימסור למפר הודעה על כוונת חיוב בשל ההפרה החוזרת.

סימן ג': התחייבות להימנע מהפרה

התחייבות להימנע מהפרה

23ל. (א) היה לממונה יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 23טז, רשאי הוא להמציא לו, במקום הודעה על כוונת חיוב לפי סעיף 23יז, הודעה שלפיה באפשרותו להגיש לממונה כתב התחייבות ועירבון לפי הוראות סימן זה, במקום שיוטל עליו עיצום כספי לפי הוראות סימן א'.

(ב) בכתב ההתחייבות יתחייב המפר להפסיק את הפרת ההוראה כאמור בסעיף 23טז, ולהימנע מהפרה נוספת של אותה הוראה בתוך תקופה שיקבע הממונה ושתחילתה ביום מסירת ההודעה כאמור בסעיף קטן (א), ובלבד שהתקופה האמורה לא תפחת משנתיים ולא תעלה על חמש שנים (בסימן זה - תקופת ההתחייבות); הממונה רשאי לקבוע בכתב ההתחייבות תנאים נוספים שעל המפר לעמוד בהם במהלך תקופת ההתחייבות במטרה להקטין את הנזק שנגרם מההפרה או למנוע את הישנות ההפרה.

(ג) בנוסף לכתב ההתחייבות יפקיד המפר בידי הממונה עירבון בסכום העיצום הכספי שהממונה היה רשאי להטיל על המפר בשל אותה הפרה.

(ד) מסר המפר כתב התחייבות ועירבון לפי סעיף זה, בתוך 30 ימים מיום מסירת ההודעה לפי סעיף קטן (א), לא יוטל עליו עיצום כספי בשל אותה הפרה, אלא אם כן הפר את התחייבותו כאמור בסעיף 23לא.

(ה) לא מסר המפר כתב התחייבות ועירבון לפי סעיף זה, בתוך 30 ימים מיום מסירת ההודעה לפי סעיף קטן (א), ימציא לו הממונה הודעה על כוונת חיוב בשל אותה הפרה, לפי סעיף 23טז.

הפרת ההתחייבות 23לא. (א) נתן המפר כתב התחייבות ועירבון לפי סימן זה והפר תנאי מהתנאים שבהם התחייב בכתב ההתחייבות, כמפורט להלן, יחולו הוראות אלה, לפי הענין:

(1) המשיך המפר, בתקופת ההתחייבות, להפר את ההוראה שבשלה נתן את כתב ההתחייבות - יחלט הממונה את העירבון וימציא למפר דרישת חיוב בשל ההפרה הנמשכת כאמור בסעיף 23כ;

(2) חזר המפר והפר, במהלך תקופת ההתחייבות, את ההוראה שבשלה נתן את כתב ההתחייבות - יחלט הממונה את העירבון ויראו את ההפרה הנוספת כאמור כהפרה חוזרת לעניין סעיף 23כ; הממונה ימציא למפר הודעה על כוונת חיוב בשל ההפרה החוזרת;

(3) הפר המפר תנאי מהתנאים הנוספים שקבע הממונה בכתב ההתחייבות כאמור בסעיף 23ל(ב) - יחלט הממונה את העירבון.

(ב) לעניין פרק זה יראו בחילוט העירבון לפי הוראות סעיף זה כהטלת עיצום כספי על המפר בשל ההפרה שלגביה ניתן העירבון.

(ג) הופר תנאי מהתנאים שבהם התחייב המפר בכתב התחייבות, כאמור בסעיף זה, לא יאפשר הממונה למפר להגיש כתב התחייבות נוסף לפי הוראות סימן זה בשל הפרה נוספת של ההוראה שבשלה ניתן כתב ההתחייבות שהופר.

השבת העירבון

23לב. עמד המפר בתנאי כתב ההתחייבות שמסר לפי סימן זה, יוחזר לו, בתום תקופת ההתחייבות, העירבון שהפקיד בתוספת הפרשי הצמדה וריבית מיום הפקדתו עד יום החזרתו.

סימן ד': שונות

עיון בחומר שעליו מתבססת החלטת הממונה

23לג. ביקש אדם שנגדו ננקט אמצעי אכיפה לפי פרק זה, לעיין בחומר שעל בסיסו החליט הממונה לנקוט צעד כאמור, לצורך הגשת עתירה, יאפשר לו הממונה לעיין בחומר כאמור.

עתירה לבית המשפט לעניינים מינהליים

23לד. (א) על הטלת עיצום כספי או מתן התראה, או על הוראות בצו אבטחת מידע ניתן לעתור לפני בית משפט לעניינים מנהליים, בתוך שלושים ימים מיום שנמסרה הדרישה למפר.

(ב) אין בהגשת העתירה כדי לעכב את תשלום העיצום הכספי, או את כניסת ההתראה לתוקף או את ביצוע האמור בצו אבטחת מידע, אלא אם כן הסכים לכך הממונה או הורה בית משפט אחרת.

(ג) החליט בית המשפט לקבל את העתירה לאחר ששולם העיצום הכספי, יוחזר העיצום הכספי או כל חלק ממנו אשר הופחת על ידי בית המשפט, בתוספת הפרשי הצמדה וריבית מיום תשלומו ועד יום החזרתו.

פרסום

23לה. הוטל עיצום כספי לפי פרק זה, רשאי הממונה לפרסם בעיתון או בכל דרך אחרת את דבר הטלת העיצום הכספי וסכומו, את שמו של המפר ואת מהות ההפרה שבשלה הוטל ונסיבותיה, ורשאי הממונה להורות למפר לפרסם פרסום כאמור.

שמירת אחריות פלילית

23לו. (א) תשלום עיצום כספי, מתן כתב התחייבות או המצאת התראה לפי פרק זה לא יגרעו מאחריותו הפלילית של אדם בשל ביצוע עבירות על חוק זה.

(ב) הוגש נגד אדם כתב אישום בשל עבירה על חוק זה, לא ינקוט נגדו הממונה בהליכים לפי פרק זה, ואם שילם המפר עיצום כספי יוחזר לו הסכום ששולם בתוספת הפרשי הצמדה וריבית מיום תשלומו עד יום החזרתו.

פרק ד3: עבירות

הפרעה לממונה במילוי תפקידו

23לז. המפריע לממונה, או לחוקר או מפקח מטעמו במילוי תפקידו לפי חוק זה, דינו – מאסר שישה חודשים.

הפרה תוך כוונה להטעות

23לח. מי שעשה אחד מאלה בכוונה להטעות את הממונה או מפקח מטעמו – דינו מאסר שלוש שנים:

(א) כלל פרטים לא נכונים בבקשה לרישום מאגר מידע שהוגשה לפי סעיף 9;

(ב) לא הודיע לממונה על שינויים בפרטים המנויים בסעיף 9(ב) או בפרטים שנקבעו לפי סעיף 9(ג), בניגוד להוראת סעיף 9(ד);

(ג) מסר פרטים לא נכונים במענה לדרישת מידע של הממונה או של מפקח לפי סעיף 23י(א)(1) עד (3).

אי מסירת הודעה בכוונה להטעות

23לט. מי שפנה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע, בלי שמסר לו הודעה כנדרש בסעיף 11, בכוונה לקבל את המידע במרמה, דינו – מאסר שלוש שנים; לעניין סעיף זה, "מרמה" – טענת עובדה בעניין שבעבר, בהווה או בעתיד, הנטענת בכתב, בעל פה או בהתנהגות, ואשר הטוען אותה יודע שאינה אמת או שאינו מאמין שהיא אמת.

שימוש במידע בניגוד למטרה לשמה נמסר

23מ. בעל מאגר מידע או מחזיק בו, המשתמש במידע ממאגר המידע שלא למטרה שלשמה נמסר, או המתיר לאחר להשתמש כאמור, דינו - מאסר שלוש שנים.

שימוש במידע ממאגר מידע ללא הרשאה כדין

23מא. (א) לא ישתמש אדם במידע ממאגר מידע ללא הרשאה כדין של בעל מאגר המידע, או תוך חריגה מהרשאה כאמור; לעניין זה, מי שברשותו עותק של מאגר מידע, או חלק מהותי ממנו –, אלא אם כן הוכיח אחרת.

(ב) המשתמש במידע ממאגר מידע ללא הרשאה או תוך חריגה מהרשאה כאמור בסעיף קטן (א), דינו מאסר שלוש שנים.

מסירת מידע מגוף ציבורי

23מב. המוסר מידע מגוף ציבורי בניגוד להוראות סעיף 23ב, דינו - מאסר שלוש שנים.

תחולה

23מג. הוראות סעיפים 23מ עד 23מא יחולו על ידיעות הנוגעות לענייניו הפרטיים של אדם, אף שאינם בגדר מידע, כשם שהן חלות על מידע.

אחריות נושא משרה בתאגיד

23מד. (א) נושא משרה בתאגיד חייב לפקח ולעשות כל שניתן למניעת עבירות לפי סעיף 16 ולפי פרק זה, למעט סעיף 23לז , בידי התאגיד או בידי עובד מעובדיו; המפר את חובתו האמורה, דינו - קנס כאמור בסעיף 61(א)(4) לחוק העונשין.

(ב) נעברה עבירה לפי סעיף 16 או לפי פרק זה, למעט סעיף 23לז, בידי תאגיד או עובד מעובדיו, חזקה היא כי נושא משרה הפר את חובתו לפי סעיף קטן (א), אלא אם כן הוכיח כי עשה כל שניתן כדי למלא את חובתו האמורה.

(ג) בסעיף זה, "נושא משרה" - מנהל פעיל בתאגיד, שותף, למעט שותף מוגבל, וכן מנהל המאגר.

התראה לעובד רשות ציבורית

23מה. (א) בוצע מעשה או מחדל המהווה הפרה של הוראות פרקים ב', ד' ו-ד'3 או נעברה עבירה על הוראות פרקים ב', ד' ו-ד'3 על ידי רשות ציבורית, רשאי הממונה לשלוח התראה לעובד אחראי ברשות הציבורית (בסעיף זה – ההתראה), לפיה עליו לפקח על ביצוע האמור להלן, במסגרת פרק הזמן הקצוב בהתראה, לפי העניין -

(1) נקיטת אמצעים בידי הרשות הציבורית להפסקת ההפרה המפורטת בהתראה;

(2) נקיטת אמצעים בידי הרשות הציבורית למניעת הישנות ההפרה.

(ב) צו אבטחת מידע שניתן לפי סעיף 17ב1, יראו אותו לעניין סעיף זה כהתראה שניתנה לפי סעיף קטן (א).

(ג) לא ביצעה רשות ציבורית את האמור בהתראה או בצו אבטחת מידע לפי סעיף 17ב1 – יראו את העובד האחראי ברשות הציבורית כאילו הפר את חובתו האמורה בסעיף קטן (א), אלא אם הוכיח כי עשה כל שניתן בנסיבות העניין לקיום חובתו, ודינו - הקנס הקבוע בסעיף 61(א)(4) לחוק העונשין.

(ד) כתב אישום לפי סעיף זה יוגש באישור היועץ המשפטי לממשלה.

(ה) בסעיף זה, "רשות ציבורית" – משרד ממשלתי ויחידה שהיא יחידת סמך של משרד ממשלתי שאינה תאגיד.

(ו) עבירה לפי סעיף זה תיחשב גם כעבירת משמעת של העובד האחראי, כמשמעותה בסעיף 17 (2) לחוק שירות המדינה (משמעת), התשכ"ג – 1963."

ביטול סעיף 31א

7. סעיף 31א לחוק העיקרי - בטל.

הוספת תוספת

8. אחרי סעיף 37 לחוק העיקרי יבוא:

"תוספת

(סעיף 23טז)

הסכום הבסיסי של עיצום כספי בגין הפרה יקבע לפי גודל מאגר המידע וסוג המידע האגור בו, כמפורט להלן:

גודל המאגר לפי מספר האנשים	סוג המידע	
אודותם יש מידע במאגר	קבוצה א'	קבוצה ב'
עד 10,000 אנשים	10,000 ₪	100,000 ₪
10,000 – 100,000 אנשים	20,000 ₪	200,000 ₪
100,000 – 1,000,000 אנשים	40,000 ₪	400,000 ₪
מיליון אנשים ומעלה	80,000 ₪	800,000 ₪

בתוספת זו -

"קבוצה א'" – מידע מסוג שאיננו כלול בקבוצה ב';

"קבוצה ב'" – אחד מאלה:

(1) מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד;

(2) מידע רפואי או נפשי;

(3) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000[26];

(4) מידע אודות דעות פוליטיות ואמונות דתיות;

(5) מידע אודות עברו הפלילי של אדם;

(6) נתוני מנוי ונתוני מיקום כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), תשס"ח – 2007;

(7) מידע שהוא מאפיין אנושי פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת, המשמש לזיהוי אדם;"

דברי הסבר

סעיף 2 לאור הכוונה להרחיב את סמכויות רשם מאגרי המידע, לרבות הסמכות לאשר במקרים מסוימים לערוך חיפוש או חדירה לחומר מחשב ללא צו שיפוטי, מוצע להחמיר ולקבוע כי יוכל להתמנות לרשם רק מי שמתקיימים בו תנאי הכשירות למינוי שופט בבית המשפט המחוזי, במקום שופט של בית המשפט השלום כפי שנדרש בסעיף 7 לחוק כיום.

[26] ס"ח התשס"א, עמ' 62

סעיף 3 סמכויות הפיקוח מאורגנות מחדש בפרק ד׳1 שיתווסף לחוק, ולכן מוצע להשמיט את סעיף 10(ה1).

החלפת תוכנו של סעיף 10(ה) מיועדת לשים דגש על מתן הכשרה ראויה בחדירה לחומר מחשב, לאור מקומה המרכזי בפיקוח על מאגרי מידע ולצורך הרמוניה עם ההוראות המסדירות חיפושים במחשב בדברי חקיקה אחרים.

סעיף 4 התיקון המוצע לסעיף 17ב מיועד לערוך את ההתאמה המחויבת בניסוחו של הסעיף לאור השינוי בכינוי תפקידו של הרשם.

סעיף 5 סעיף 17 לחוק הגנת הפרטיות מטיל על בעל מאגר מידע, מחזיק במאגר ומנהלו אחריות לאבטחת המידע שבמאגר. סעיף 7 לחוק מגדיר מהן ״אבטחת מידע״ ו- ״שלמות מידע״, וקובע בכך את עקרונות המסגרת לאבטחת מידע במאגר. אמצעי אבטחת המידע צריכים להלום את הסיכונים הנובעים מעיבוד המידע ורגישות המידע המצוי במאגר, בכל מקרה לגופו. בשל השינויים המהירים בטכנולוגיה והמגוון הרחב של סוגי המידע הנאספים ומאפייני הפעילויות אשר בזיקה אליהן המידע נאסף, לא ניתן לקבוע בחקיקה ראשית מסמרות לגבי האמצעים הטכנולוגיים והארגוניים לאבטחת מידע ראויה.

כדי להסדיר בצורה טובה יותר נושא זה, ולקבוע רף מינימאלי להגנה על המידע במקרים המתאימים, מוצע אפוא, כפי שהמליצה גם ועדת שופמן (בסעיף 7.4 לדו״ח הועדה), להסמיך את הרשם לקבוע ״תקינה אישית״ לגבי כל מאגר מידע או סוג של מאגרים כאמור. צו אבטחת המידע יאפשר לרשם להתאים הוראות אבטחת מידע בהתייחס למאגר ספציפי, תוך מתן הכלים להרתיע מי שלא יפעל בהתאם לצו. הפרתו של צו אבטחה היא עילה להטלת עיצום כספי וברשות ציבורית – עשויה הפרתו להגיע עד כדי עבירה פלילית של העובד האחראי על ביצועו, בהתאם לסעיף 23מה.

הסדר דומה למוצע כאן נקבע בחוק שוויון זכויות לאנשים עם מוגבלות, התשנ״ח-1998 בכל הנוגע להוצאת ״צו נגישות״. הסמכות להוציא צווי אכיפה (enforcement notices) שהפרתם מלווה בסנקציה, ביחס לאבטחת מידע, אך גם בנוגע לחובות מהותיות אחרות הנוגעות לניהול מאגרי מידע, מסורה לרשויות הגנת מידע רבות בעולם, למשל באנגליה, באירלנד ובצרפת.

סעיף 6
לפרק ד׳1 המוצע

סימן א' - סעיפים 23ט – 23י – סמכויות פיקוח

סעיף 10(ה1) לחוק הקיים מפרט את הסמכויות המיועדות לפיקוח שגרתי על קיום הוראות החוק – כאשר אין ראיה או יסוד להניח שהופרו אותן הוראות. סעיף 23י המוצע המחליף את סעיף 10 (ה1), מוסיף על סמכויות הפיקוח השגרתי על מאגרי המידע, אמצעי נוסף החיוני לקיום בקרה אפקטיבית של מערכות ממוחשבות – יכולת חדירה לחומר מחשב בעל זיקה ישירה למאגרי המידע.

חדירה לחומר מחשב ללא צו שיפוטי היא אמנם יוצא דופן בחקיקה הישראלית המסדירה סמכויות פיקוח על פעילויות שונות אך לא יוצא מן הכלל: יש לה תקדים בסעיף 17(א)(3) לחוק חתימה אלקטרונית, תשס"א – 2001 ובסעיף 10(3) לחוק שירות נתוני אשראי, תשס"ב – 2002. יחד עם זאת מאליו מובן שכאשר תכלית הפיקוח היא הבנה של אופן השימוש במערכת מחשב, לא ניתן לקיימה ללא יכולת גישה לחומר המחשב. לצורכי הפיקוח על מאגרי המידע המערכת הממוחשבת היא הכלי בה מבוצעת הפרת הדין, ולא רק המדיה בה מאוכסנות הראיות לביצועה. בהפרות של דיני הגנת המידע, "האקדח המעשן" הוא המאגר עצמו, והמחשב או מערכת המחשב בה הוא נמצא. בעבירות הליבה, כלומר אלה שבהן יש מאגר לא חוקי, או שבהן בוצעה פריצה או גישה לא חוקית למאגר, מערכת המחשב היא הראיה המשמעותית ביותר.

הסמכות הנוספת בה מוצע לצייד את המפקחים על מאגרי המידע, היא מוגבלת ומצומצמת לחדירה <u>ל"נתוני מערכת" בלבד, בכפוף לאמור להלן לעניין מידע מדגמי</u>: נתונים טכניים **שאינם כוללים מידע אישי ופרטי אודות אדם**, הדרושים לבירור קיום הוראות החוק במאגר המידע הממוחשב. ביחס לאופן **השימוש במידע**, הדרך לעמוד על כך היא באמצעות התחקות אחר הכללים המוגדרים במערכת המידע, לעניין סוג המידע השמור במערכת המידע, ופעולות העיבוד השונות המבוצעות במידע. ביחס לבחינת **אבטחת המידע**, יש צורך בהתחקות אחר אופן המימוש בפועל של עקרונות אבטחת המידע, למשל באמצעות מורשי הגישה למידע.

כמו כן מוצע להסמיך את המפקחים גם ביכולת לבחון באופן מדגמי כיצד מתנהל ונשמר המידע במאגר. כלומר – לפי סמכות זו לא יוכל המפקח לבקש להעתיק את כל מאגר המידע, אלא בשדות אקראיים לצורך בדיקה מדגמית. סמכות הבדיקה המדגמית היא כלי פיקוח בסיסי וחיוני לעצם קיומו של מנגנון הפיקוח, המוקנה למפקחים גם בדברי חקיקה אחרים.

כדי לצמצם למינימום את הפגיעה האפשרית בזכויות המפוקחים או בזכויות נושאי המידע שבמאגרי המידע במפוקחים, מוצע ללוות את הקניית סמכויות החדירה בכמה

סוגים של איזונים ובלמים. לפי המוצע, הפעלת הסמכות המוגבלת לחדור לנתוני מערכת או לבצע בדיקה מדגמית במאגר, תדרוש היתר מוקדם של רשם מאגרי המידע (אשר כמפורט לעיל יהיה נושא משרה בכיר אשר כישוריו יהלמו כישורים של שופט של בית משפט מחוזי) ותופעל רק במקרים בהם הסמכויות הסטנדרטיות לא הספיקו כדי לקיים את תכלית הפיקוח. כמו כן, סעיף קטן (ג) המוצע גם מגביל מאוד את השימוש במידע אליו עשויים המפקחים להיחשף אגב החדירה לנתוני המערכת או אגב הבדיקה המדגמית.

היקפן המוגבל מלכתחילה של החדירה לנתוני מערכת ושל הבדיקה המדגמית, יחד עם האיזונים והבלמים שהוצגו לעיל, משקפים איזון ראוי בין הזכות לפרטיות ואינטרסים אחרים של המפוקח הספציפי לבין אינטרס הציבור בקיומו של מנגנון פיקוח אפקטיבי על מאגרי המידע אשר יקדם כמובן גם את ההגנה על הזכות לפרטיות של נושאי המידע במאגרי המידע המפוקחים. גם אם לצרכי פיקוח ואכיפה אחרים, חדירה לחומר מחשב ללא צו שיפוטי אכן עשויה להגיע עד כדי פגיעה בזכות הפרטיות במידה העולה על הנדרש, הרי שבהקשר המיוחד של חוק הגנת הפרטיות, ובשים לב לאיזונים שהוצעו, סמכויות החדירה המיוחדות לחומר מחשב שיימסרו למפקחים, עומדות במבחן המידתיות שנקבע בפסיקה על כל רכיביו. כן נקבע כי המידע המדגמי שנאסף יימחק ממאגרי המידע של הממונה כאשר אינו נדרש עוד באופן סביר להמשך הליכי הפיקוח.

סמכויות הפיקוח לפי סימן א', יהיו מסורות כמובן גם למפקחים בהליך הבירור המנהלי לפי סימן ב' ולחוקרים במהלך חקירה פלילית לפי סימן ג'.

סימן ב' - סעיפים 23יא – 23יד – סמכויות בבירור מינהלי

בשנים האחרונות נדון רבות הצורך במציאת מנגנוני אכיפה חלופיים להליך הפלילי באופן כללי. קל וחומר שמנגנון חלופי נדרש לצורך אכיפת חוק הגנת הפרטיות. נוצר צורך להשלים את ההליך הפלילי בכלים אשר יאפשרו תגובה מהירה, אפקטיבית ומידתית להפרות של הוראות החוק שחומרתן לא מגיעה לרמה הגבוהה ביותר.

על כן מוצע לצייד את רשם מאגרי המידע בסל כלי האכיפה המגוון והגמיש המפורט בפרק ד'2, שנדבך מרכזי בהם הוא הסמכת הרשם להטיל עיצום כספי בגין הפרה של הוראות שאינה מגיעה עד כדי עבירה פלילית. מטבע הדברים, צריך גם לצייד את הרשם בכלי בדיקה ובירור חדשים המתאימים לסנקציה החדשה. משום שלא מדובר בפיקוח שגרתי, אלא במקרים בהם קיים יסוד סביר להניח שבוצעה הפרה של הוראות החוק, יש הצדקה וצורך לצייד את המפקחים בסמכויות נרחבות יותר ובהן חיפוש, תפיסה וחדירה לחומר מחשב, מאלה המוקנות להם לצורך הפיקוח השגרתי בסימן א'.

סמכויות אלה ילוו במערך האיזונים והבקרות המקובל. כך לפי סעיף 23יא ככלל ניתן יהיה לברר חשש לביצוע הפרה באמצעות חיפוש או חדירה לחומר מחשב (מעבר לחדירה המדגמית או לנתוני מערכת בלבד, אותן מסדיר סימן א' לפרק ד'1) רק על דרך של קבלת צו שיפוטי. עם זאת, בנסיבות של דחיפות וכורח בהן לא יהיה סיפק לפנות לבית המשפט מבעוד מועד, וביחס למספר מצומצם של הפרות במקרים של יסוד סביר לחשד להפרות שחומרתן ואופיין מחייבות שימוש בסמכויות אלה, ניתן יהיה לפעול ללא צו, ורק באישור כתוב ומנומק של הרשם.

על מנת לאזן בין הצורך לממש את תכליות הפיקוח היעיל לפי החוק עם ההגנה על זכויות המפוקחים ואחרים שמידע אודותם מצוי בחומר המחשב, לפי סעיף 23יג ניתן יהיה רק להעתיק את חומר המחשב, אולם העיון בו יתאפשר רק אם יתקבל אישור של בית משפט לאחר מעשה. החדירה במקום תתאפשר רק אם וככל שהיא נדרשת במישרין לצורך ההעתקה. הצעה זו נועדה לאפשר "הקפאת מצב" פיקוחית, באופן שתמנע העלמת ראיות או העלמת מאגרי מידע לא חוקיים, אולם מעת שהוקפא המצב יש שהות לפנות בבקשה לבית המשפט כדי שיתיר עיון בחומר.

בארגונים רבים, במיוחד בגדולים ובממסדיים שבהם, מערכות המחשב הרלבנטיות לפיקוח על מאגרי המידע, הן מורכבות ביותר וההתמצאות בהן דורשת מידה גבוהה מאוד של ידע ומומחיות, או היכרות ספציפית עם המערכת, שבלעדיהן גם מפקח מוסמך ומיומן עלול להיתקל בקושי ממשי להגיע לחקר האמת. כדי לאפשר פיקוח אפקטיבי, מציע אפוא סעיף 23יד(ג) לאפשר למפקחי הרשות להיעזר בעת הפיקוח במומחים חיצוניים שאינם מפקחים, או במועסקים של או מטעם הארגון המפוקח המכירים היטב את המערכת. כדי להקפיד על פרטיות המפוקחים, מוצע שלגבי מידע אליו יחשפו אגב הסיוע למפקחי הרשות, תחול על המומחים חובת סודיות כאילו היו מפקחים בעצמם.

סימן ג' - סעיף 23טו – סמכויות חקירה

לפי החוק הקיים, לא מוקנות לרשם מאגרי מידע סמכויות חקירה פליליות, ובשל כך במקרים של חשד להפרות חמורות בתחום הפרטיות, יחידת הרשם מחויבת לפנות לסיוע של יחידה משטרתית מתאימה. נושא זה מעורר קשיים מעשים בשל הצורך במומחיות מיוחדת ובשל העומס המוטל כבר כיום על יחידות המשטרה. התוצאה היא שדווקא בעבירות הפליליות המגלמות הפרות חמורות של חוק הגנת הפרטיות בתחום מאגרי מידע, אין כיום מנגנון יעיל המאפשר תגובה מהירה והולמת לחומרת העבירות. סמכויות דומות מוקנות כיום למספר רב של רשויות מתמחות בתחום סמכויותיהן, ובהן רשות ניירות ערך, רשות ההגבלים עסקיים, רשויות המס, וכן יחידות אכיפה ייעודיות נוספות.

בהתאם לכך סעיף 23טו המוצע נועד להסמיך את הרשם בסמכויות חקירה ואכיפה בקשר עם חשד לביצוע עבירות על חוק הגנת הפרטיות במאגרי מידע, מוצע להסמיך את הרשם ואת החוקרים בסמכויות תשאול, תפיסת חפצים, דרישה להתייצב לחקירה, עיכוב, וחדירה לחומר מחשב לפי צו שיפוטי. בנסיבות החריגות המצדיקות ביצוע חיפוש או חדירה לחומר מחשב ללא צו במסגרת הבירור המינהלי (סימן ב' לעיל) – יהיה הרשם רשאי לבצע חיפוש או חדירה כאמור, ללא צו, גם במסגרת חקירה פלילית; אולם, בשל החומרה הרבה של העבירות, בנסיבות בהן לא ניתן יהיה למנוע את שיבוש החקירה בדרך של העתקת חומר מחשב גרידא כמפורט בסעיף 23יג, אפשר יהיה הרשם לחדור לחומר המחשב גם בלא פניה לקבלת הוראות מבית המשפט, להבדיל מן המנגנון הקבוע בסעיף 23יג.

לפרק ד'2 המוצע: עיצום כספי ואכיפה מינהלית

כפי שפורט במבוא ובדברי ההסבר לפרק ד'1, המנגנון הפלילי לבדו אינו מספק פיתרון הולם לאכיפת הוראות חוק הגנת הפרטיות הנוגעות למאגרי מידע. חומרת הענישה הפלילית והסטיגמה שמביאה עימה הרשעה, כמו גם מורכבותם של הליכים אלה, אינם מספקים מענה יעיל ומרתיע לקשת של מעשים שאף שמידת חומרתם אינה הגבוהה ביותר, יש בהם משום איום של ממש על הגנת הפרטיות במאגרי מידע.

בהתאם למגמה העולמית בתחום הגנת הפרטיות במאגרי מידע, ובהתאם למגמה בתחום האכיפה המשלימה על ידי רשויות פיקוח בישראל, מוצע לקבוע הוראות שהפרתן תוביל לסנקציה אזרחית – מינהלית. הוראות אלה נותנות בידי הרשות כלי מידתי ויעיל המאפשר לה לטפל באי ציות לחוק באמצעות מידרג של סנקציות ההולם את הסוגים השונים של ההפרות ואת מידות החומרה השונות הכרוכות בביצוען. מובן כי ככל הליך מינהלי, גם האכיפה המינהלית כפופה לכללי המשפט המינהלי, בכל הנוגע לדיות הראיות הנדרשות להטלת הסנקציה, לזכות השימוע בטרם הטלתה, לזכות עיון ולזכות הערעור לאחר קבלתה. ראה לעניין זה סעיפים 23יז – 23יט המוצעים.

סימן א' - העיצום הכספי

תכליתו של העיצום הכספי איננה ענישה אלא הבטחת חובת הציות להוראות החוק ולהנחיות הרשם. על כן קיומם של כוונה פלילית או יסוד נפשי מיוחד, איננו רלבנטי לקביעת ההפרות והוכחתן. בסעיף 23טז מפורטת רשימה של הוראות החוק אשר לצורך הרתעה והבטחת הציות נדרשת קיומה של סנקציה להפרתן, אם כי לא מתקיימות נסיבות של חומרה יתרה, של כוונה מיוחדות להזיק או לפגוע או של זלזול בהוראות החוק – המצדיקות שימוש בכלים פליליים. ההוראות מחולקות לשלוש קבוצות לפי דרגת חומרה עולה, כאשר ההפרות החמורות ביותר המנויות בסעיף 23טז(ג) מקבילות ביסוד העובדתי

שלהן למעשים ומחדלים המגבשים עבירות לפי פרק ד׳3. דרגת החומרה של כל הפרה נובעת ממידת הסיכון לפגיעה בפרטיות שהיא יוצרת, ובחלק מן ההפרות - ממימושו. רשימת ההפרות המנויה בסעיפים אלה איננה יוצרת חיובים מהותיים יש מאין; כל ההוראות המהותיות שהפרתן תהיה עילה להטלת עיצום, היו קיימות בחוק גם קודם לכן, או שנקבעות בו בתיקון זה.

סכום העיצום הכספי מדורג ונקבע לפי חומרת ההפרה כמפורט בסימן א׳, בשילוב עם סוג המידע ועם גודל המאגר בו או בעטיו בוצעה ההפרה, לפי הקבוע בתוספת. ייחודם של סוגי המידע הכלולים בקבוצה ב׳ שבתוספת הוא ברגישותם הגבוהה במיוחד ובפגיעה החמורה במיוחד שתיגרם מחשיפתם או משימוש לא ראוי בהם. משום שמטרתו של העיצום הכספי היא הרתעתית וכיוון שפוטנציאל הנזק בסוגי מידע אלה הוא גבוה במיוחד, הרי שמוצדק כי עיצום המוטל בגין הפרה בסוגי מידע אלה יהיה גבוה משמעותית מהעיצום שיוטל על הפרה שבוצעה בקשר לסוגי המידע ״הרגילים״ שבקבוצה א׳.

סעיף 23כג מיועד לאפשר להתאים את משטר הסנקציות להתפתחות הטכנולוגית ולמידת הציות להוראות החוק. באישור ועדת החוקה של הכנסת יוכל השר להוסיף לקבוצה ב׳ סוגי מידע נוספים.

לצד ההסמכה של הרשות המנהלית להטיל עיצום כספי, מוצע גם להגביל ולהבנות את שיקול דעתה של הרשות המפקחת ולהעמיד את גובה העיצום הכספי על סכומים קצובים – בהתאם לקריטריונים מובנים וקבועים מראש שייקבעו בחוק, וזאת בשים לב לזכויותיהם של המפוקחים. מסיבה זו הסכום הבסיסי של העיצום הכספי (בהתאמה לסוג המידע ולגודל המאגר) קבוע וקצוב מראש בתוספת, ואילו מנגנון העדכון של הסכום נקוב מראש בסעיף 23כב. בנוסף מוצע להסדיר בצורה ברורה בסעיף 23כ את שיעורה של התוספת על העיצום בגין הפרות חוזרות או נמשכות.

מטרתו העיקרית של העיצום הכספי היא אכיפת ציות על המפוקח, ולצורך השגת תכלית זו ישנה חשיבות לשיקולים שונים המיוחדים לכל הפרה לגופה. על כן לצד הוודאות והגבלת שיקול הדעת שבעיצום כספי בסכום קצוב הקבוע בחוק, יש צורך בהתאמה, במקרים המתאימים של הסנקציה לנסיבות ההפרה והפעולות שננקטו בעקבותה על ידי המפוקח, וכן ביחס לנסיבותיו הקונקרטיות.

סעיף 23כא מגביל את יכולתו של הרשם להטיל עיצום בסכום הנמוך ממה שנקבע בחוק. מאידך מסמיך הסעיף את שר המשפטים לקבוע באישור ועדת החוקה של הכנסת, רשימה מובנית של נסיבות אשר בהתקיימן יהיה הרשם רשאי להפחית את גובה העיצום.

דוגמה לשיקולי הפחתה אפשריים יכולה להיות היותה של ההפרה ראשונה מסוגה אצל המפוקח, שיתוף פעולה עם הרשם במניעת הישנותה, נסיבות אישיות קשות של מפר יחיד, או היעדר פרופורציה בין גובה העיצום לבין מחזור העסקים של המפר.

סעיף 23לו – תיתכן חפיפה בין מעשים או מחדלים המהווים הפרה המקימה עילה להטלת עיצום כספי כמפורט בסימן א' – לבין התנהגויות העולות כדי עבירה פלילית על חוק הגנת הפרטיות. הסעיף קובע שהטלת עיצום כספי לא תקים למפר הגנה של "סיכון כפול" ולא תחסום את הדרך מפני העמדתו לדין פלילי, אם כי העיצום הכספי יוחזר עם הגשת כתב אישום. הוראה דומה נקבעה בסעיף 38ט לחוק להגברת התחרותיות צמצום הריכוזיות וניגודי העניינים בשוק ההון בישראל (תיקוני חקיקה), התשס"ה - 2005.

סימן ב' – התראה מנהלית

סעיף 23כז מקים סעד המחליף עיצום כספי או מקדים אותו. משלוח התראה הוא מעין עיצום כספי "על תנאי" המיועד לעודד ציות של מפוקחים בדרך של מתן תמריץ שלילי לביצוע הפרות עתידיות ותמריץ חיובי לציות. על ההפרה המקורית שבגינה נשלחה ההתראה לא ניתן יהיה להטיל אמנם עיצום כספי, אולם אם ימשיך המפר לעמוד במריו – ניתן יהיה להטיל על ההפרות הנוספות שיבצע עיצום בסכום מוגדל, בהיותן הפרה נמשכת או חוזרת בהתאם לסעיף 23כ. ההתראה היא כלי אכיפה מתון שיתאים במיוחד להפרות ראשונות של המפוקח, או לנסיבות אחרות שיצדיקו יחס מקל. על מנת להבטיח שקיפות ושוויוניות באכיפה ולהגביר את הוודאות, מוצע לעגן את המקרים המתאימים לשליחת התראה בנהלים שיאושרו בידי היועץ המשפטי לממשלה. למרות שעצם משלוח ההתראה אינו מלווה בסנקציה, הרי שיש בה קביעה של הרשם כי המפוקח ביצע הפרה, ולכן מוצע לאפשר למפוקח לבקש את ביטולה.

סימן ג' – התחייבות להימנע מהפרה

ההתחייבות היא אמצעי אכיפה המהווה דרך ביניים בין התראה לבין עיצום כספי, אשר יתאים לשמש כתחליף להטלת עיצום כספי להפרות חמורות יותר מאלו המתאימות יותר לשימוש בהתראה. ההתחייבות היא אמצעי אכיפה גמיש המקנה לרשם שיקול דעת לצקת בו תוכן. התנאים שייקבעו בהתחייבות לא יוגבלו רק לדרישה שלא לחזור על ההפרה שכבר בוצעה או על מעשים נוספים המוגדרים במפורש בחוק כהפרות או עבירות. לרשם יהיה שיקול דעת רחב לקבוע בהתחייבות תנאי רלבנטי וסביר בגדר סמכויותיו לצורך מימוש תכלית החוק, הדרוש לדעתו לצמצום הנזק שנגרם לתיקון הליקויים שנמצאו או להבטחת הציות של המפוקח.

הפרתו של כתב ההתחייבות תוביל לחילוט הערובה שהמציא המפר. אם הפרת כתב

ההתחייבות היא גם הפרה של סימן א', יהיה הרשם רשאי להטיל בגינה עיצום כספי בנוסף על חילוט הערובה, בסכום המוגדל התואם את היותה הפרה נמשכת או חוזרת.

לפרק ד'3 המוצע: עבירות

ככל שאיסוף המידע והשימוש במאגרי מידע הופכים לפעילות יומיומית ורחבת היקף, כך גדלה חשיבות ההרתעה. כפי שצוין כבר לעיל, העבירות שמונה כיום חוק הגנת הפרטיות אינן מכסות את טווח המעשים והמחדלים הפוגעים בפרטיות, אשר אינטרס הציבור הוא למנוע אותן. חלק מן ההתנהגויות המפרות שאינן מכוסות כיום - יטופלו במסגרת הסנקציות המינהליות כפי שמוצע בפרק ד'2 לתזכיר. ביחס להפרות האחרות שהן חמורות יותר ונגועות במחשבה פלילית או משקפות פוטנציאל לנזק רב יותר לציבור - מציע פרק זה להחמיר ולקבוע סנקציות פליליות ברורות ומרתיעות שיציבו סטנדרט ראוי לטיפול במידע, אשר אינו מושרש דיו כיום.

סעיפים 23לז - 23לח קובעים את הסנקציה על עבירות שביסודן כוונה פלילית מפורשת להטעות את הרשם, בקשר ישיר להפעלת הפיקוח על ניהול מאגרי המידע. נסיון החיים והשכל הישר מלמדים כי ככל שהפיקוח יהיה אפקטיבי יותר, עשוי להיות תמריץ להכשילו ולהסתיר נתונים. תופעה זו אינה חדשה בתחום הפיקוח. הכשלה מכוונת של הרשות המפקחת מיועדת לרוב לצורך כיסוי על ביצוע הפרות מהותיות של עקרונות עיבוד המידע, ומשום כך מוצדק להטיל עליהן סנקציה פלילית נאותה.

סעיף 23לט עוסק בפגיעה חמורה נגד נושא המידע עצמו. ההימנעות ממסירת ההודעה לפי סעיף 11 לחוק מתוך כוונה לקבל את המידע במרמה, מפרה את זכותו הבסיסית של נושא המידע שלא תיפגע פרטיותו ללא הסכמתו מדעת (סעיף 1 לחוק). ללא קבלת הפרטים המנויים בסעיף 11 אין לנושא המידע יכולת לגבש הסכמה מדעת, וגם אין אפשרות פרקטית לבחון האם נעשה במידע שימוש בניגוד למטרה לשמה נמסר – עיקרון בסיסי נוסף בהגנת המידע, המעוגן כבר כיום בסעיף 8(ב) לחוק ובסעיף 2(9) ומוצע שהפרתו תיקבע כעבירה לפי סעיף 23מ. עוד מוצע ששימוש במידע ממאגר ללא הרשאה כדין מבעל המאגר, ייקבע כעבירה בסעיף 23מא משום שהוא משקף - או לכל הפחות יוצר סיכון של - הפרה של חובת אבטחת המידע הקבוע בסעיף 17 לחוק, ושימוש במידע בניגוד למטרה לשמה נאסף וללא הסכמתו של נושא המידע.

סעיף 23מד המוצע יוצר תשתית חוקית להטלת אחריות אישית על נושא משרה בתאגיד בגין עבירות אשר יש ביכולתו של נושא המשרה למנוע את ביצוען. הסעיף מטיל על בעל הסמכות בתאגיד את החובה לפקח ולעשות ככל הניתן למנוע ביצוע עבירות בידי התאגיד ובידי עובדיו. חובה זו של נושא המשרה היא נדבך חשוב בתמרוץ התאגיד לציית

להוראות החוק, משום שהיא מונעת מצב בו יתבצעו בתאגיד עבירות "יתומות" שלא ניתן להטיל בגינן אחריות אישית, ומטילה על נושא המשרה את הנטל להוכיח שעשה כל שניתן למנוע את ביצוען.

סעיף 23מה נועד להגביר את הציות להוראות החוק ברשויות הציבוריות. על הרשויות המנהליות ככלל חל המשפט המנהלי המחייב אותן לפעול כדין בכל פעולותיהן. במקרים של חשש להפרה, העיצום הכספי והסנקציות חלופית הנלוות לו אינן האמצעי הראשון המתאים לאכיפת הדין על הרשות הציבורית ועובדיה. מנגד, שימוש בלעדי במשפט הפלילי לצורך אכיפה על המגזר הציבורי עלול להיות לא יעיל וחסר מצד אחד, ולא מידתי ונוקשה יתר על הצורך מן הצד השני. לפיכך מציע הסעיף הסדר דו שלבי מאוזן לפיו תוטל אחריות פלילית על עובד אחראי ברשות ציבורית, רק לאחר שהרשות לא קיימה התראה או צו אבטחת מידע ששלח לה רשם מאגרי המידע, ורק אם העובד האחראי לא עשה ככל שניתן בנסיבות העניין כדי למנוע את ההפרה. גם הדרישה לאישורו של היועץ המשפטי לפני העמדת העובד האחראי לדין, ממתנת את נוקשותו של ההסדר המוצע.

סעיף 7 אכיפת הוראות החוק במישור המינהלי ובמישור הפלילי, הוסדרה מחדש בפרקים ד'2 ו- ד'3 הבאים במקומו של סעיף 31א לחוק העיקרי.

יב. נספח ב' – נייר עמדה בנושא תקנות אבטחת מידע להגנת פרטיות

Ministry of Justice
The Israeli Law, Information & Technology Authority (ILITA)

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

מדינת ישראל
State of Israel

תאריך: 10 בינואר 2010
כ"ד בטבת התש"ע

<u>נייר עמדה בנושא תקנות אבטחת מידע להגנת פרטיות</u>

<u>והזמנה ליום עיון בנושא</u>

הרשות למשפט טכנולוגיה ומידע (להלן - **הרשות**) מפרסמת בזאת להערות הציבור נייר עמדה מטעמה ובו הסדר מוצע בתחום חובות אבטחת מידע על בעל מאגר ומחזיק לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן – **החוק**), לקראת יום עיון בנושא **"אבטחת מידע בהקשר של הגנת הפרטיות במאגרי מידע"**.

יום העיון נערך בשיתוף פעולה עם רשות הגנת המידע הספרדית (AEPD) במסגרת תוכנית ה-twinning המתקיימת עמה, ובו יוצגו גם הגישות של נציב הגנת המידע האישי הספרדי והבריטי בנושא זה. עוד תשתתף ביום העיון נציגה בכירה של איגוד מבקרי המידע הספרדי. ביום העיון יוצג גם נייר עמדה זה, וייערך בו דיון לאור דברי האורחים מחו"ל.

יום העיון ייערך בקריית הממשלה ב- 20.01.2010 בקריית הממשלה, רח' בגין 125, תל-אביב בחדר 101 בשעות 09:00-13:30. לרישום ליום העיון יש להרשם בשליחת דוא"ל עם פרטי הנרשם (שם, תואר תפקיד, ארגון) ל- twinning@justice.gov.il **מספר המקומות מוגבל!**

נייר העמדה מצ"ב, וניתן להורדה גם בכתובת הבאה –

http://www.justice.gov.il/MOJHeb/RashutTech/TwinningProject/Iruim/takanot+avtahat+meida.htm

הערות לנייר העמדה ניתן להעביר לרשות עד יום 15.2.2010 לדוא"ל -

ilita@justice.gov.il

<u>אודות נייר העמדה</u>

נייר העמדה מופץ לציבור בשלב זה על מנת להניע דיון בנושא זה, במסגרת תוכנית העבודה של הרשות, וכחלק ממהלך הסדרה מקיף יותר של תחום זה. הפצתו כעת נעשית לצורך קבלת הערות

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

Ministry of Justice
The Israeli Law, Information & Technology Authority (ILITA)

מדינת ישראל
State of Israel

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

מקדמיות של בעלי עניין לקראת עיון ודיון מול מחלקת ייעוץ וחקיקה במשרד המשפטים, האמונה על החקיקה וחקיקת המשנה בתחום הגנת הפרטיות.

כידוע, הוראות בתחום אבטחת המידע משמשות אדן מרכזי עליו מבוססת ההסדרה בתחום פרטיות במאגרי המידע, משום שהוראות אלה מביאות לצמצום החשש מפני שימוש לרעה או פגיעה במידע.

מטרת נייר העמדה לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בעיבוד מידע אישי במאגרי מידע, בהתבסס על תקנים מקובלים. מטרת יישום העקרונות בהקשר של מאגרי מידע נועד לסייע במימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע, מפני שימוש לרעה הפוגע בפרטיותם. עם זאת, ניתן להניח כי עמידה בעקרונות המוצעים תבטיח כי התנהלות הארגון בתחום המידע באופן כללי תהיה תקינה.

נייר העמדה מציע מנגנונים וכלים פנים ארגונים, שמטרתם הפיכת אבטחת המידע במאגר, לחלק משגרת ניהול המידע בפרט וניהול הארגון בכלל. מטרת המנגנונים לכוון באופן מוחשי וברור יותר לחובותיהם ואחריותם בתחום אבטחת המידע. בשל כך נדרש כי הארגון יקבע נהלים בתחום אבטחת המידע, שיסדירו בצורה מפורטת וברורה יותר היבטים אלה. החובה לקבוע מסמכים המפרטים את הנהלים נגזרת מעקרונות יסוד של אבטחת מידע ושל ניהול תקין, ומאפשרות הנחלה של עקרונות ההתנהלות בתוך הארגון.

בנוסף, הנהלים יאפשרו לארגון גם להציג לצדדים שלישים – לקוחותיו, ספקיו, בתי משפט ורשם מאגרי מידע את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט באמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה.

בשל מגוון הארגונים המעבדים מידע אישי, נייר העמדה הוא מודלורי, בכך שהוא מחיל חובות ברמה עולה וגדלה ככל שהארגון הוא ארגון שפעילות עיבוד המידע שבו, בהקשר החוק, הינה משמעותית יותר. תפיסה זו, של חובות מודלוריות נגזרת ישירות מעקרונות יסוד של אבטחת מידע ומוצאת ביטויה גם במסמכים דומים בעולם.

המסמך חובר על ידי עו״ד יצחק גורדון מהמחלקה המשפטית ברשות, בעזרתם של המתמחים מורן בר, אדם שלשבסקי ויוסי טהר ובהנחיית עו״ד עמית אשכנזי, היועץ המשפטי של הרשות.

בברכה,

יורם הכהן, עו״ד
ראש הרשות למשפט, טכנולוגיה ומידע

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל׳: 03-7634050
פקס: 02-6467064

Ministry of Justice
The Israeli Law, Information & Technology Authority (ILITA)

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

מדינת ישראל
State of Israel

נייר עמדה בנושא

תקנות אבטחת מידע להגנת פרטיות במאגרי מידע

כ"ד בטבת התשי"ע
10 בינואר 2010

Government Campus, 9th floor
125 Begin Road
P.O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

להערות הציבור

מבוא

חוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק), קובע הוראות שונות וחובות המוטלות על בעל מאגר, מחזיק במאגר ומנהל מאגר. אחת החובות המרכזיות היא חובת אבטחת המידע, שמטרתה צמצום החשש מפני שימוש לרעה או פגיעה במידע. סעיף 17 לחוק הגנת הפרטיות קובע כי:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע."

ואילו "אבטחת מידע" מוגדרת בסעיף 3 לחוק באופן הבא:

"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;"

מטרת התקנות המוצעות לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע במאגרי מידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם*. בשונה מאבטחת מידע באופן כללי, שמטרתה להגן על המידע של ארגון כנכס של אותו ארגון, המטרה של ההסדר המוצע הוא מימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע, מפני שימוש לרעה במידע אודותיהם. יחד עם זאת, ניתן לומר כי עמידה בעקרונות המוצעים בתקנות אלה, תבטיח כי ניהול המידע בארגון באופן כללי - יהיה תקין.
התקנות מבקשות לקבוע מנגנונים וכלים פנים-ארגוניים, שמטרתם הפיכת אבטחת המידע במאגר המידע, בהתאם למאפייני המאגר, לחלק משגרת ניהול המידע בפרט וניהול הארגון בכלל. מטרת המנגנונים להמחיש בצורה ברורה יותר את חובותיהם ואחריותם של ארגונים בתחום אבטחת המידע.

המנגנונים המוצעים נחלקים למספר רבדים: ברובד הראשון נדרש בעל המאגר לקבוע מהו המידע המוגן ומהם הסיכונים הקשורים אליו. ברובד השני, נדרש הארגון לייעד נושא משרה בארגון שאבטחת המידע היא חלק מתפקידו, ועליו להיות אחראי בתוך הארגון על כך.
תובנה מקובלת בתחום אבטחת המידע הינה כי:

"מערכות מידע רבות לא נועדו מלכתחילה להיות בטוחות. האבטחה שניתן להשיג באמצעים טכניים היא מוגבלת, והיא זקוקה לתמיכה הולמת של ניהול ונהלים. זיהוי אמצעי הבקרה המתאימים דורש תכנון זהיר ושימת לב לפרטים. ניהול אבטחת המידע בארגון נזקק קודם כל לשיתוף פעולה של כל העובדים. לפעמים יש גם צורך בשיתוף פעולה של ספקים, לקוחות או בעלי מניות, ואף בייעוץ של מומחים שמחוץ לארגון. הכללת אמצעי הבקרה לאבטחת המידע בשלב הגדרות הדרישות והתוכן, תהיה באופן משמעותי זולה יותר ואפקטיבית יותר לעומת הכללתם בשלב מאוחר יותר." [ת"י 7799, מבוא, עמ' 2]

בשל כך נדרש כי הארגון יקבע נהלים בתחום אבטחת המידע, שיסדירו בצורה מפורטת וברורה יותר את ההיבטים האלה. החובה לקבוע מסמכים המפרטים את הנהלים נגזרת מעקרונות יסוד של אבטחת מידע ושל ניהול תקין, ומאפשרת הנחלה של עקרונות אלה בתוך הארגון.

---

* יצוין כי כיום קיימים כבר הסדרים בנושא אבטחת מידע בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986 (להלן – התקנות הקיימות), אך מדובר בהסדרים המחייבים עדכון. לפיכך, בהמשך הדרך, כאשר טיוטת התקנות הנוכחית תבשיל לקראת הפיכתה לתקנות פורמליות, יהיה צורך גם בעריכת תיקונים בתקנות הקיימות, ובכלל זה ביטול של הוראות שיוחלפו בהוראות חדשות במסגרת התקנות המוצעות. בנוסף לכך תידרש התאמה של הוראות תחילה לתקנות, שיאפשרו תקופת היערכות מתאימה להוראות השונות של התקנות.

בנוסף, הנהלים מאפשרים לארגון גם להציג לצדדים שלישיים – לקוחותיו, ספקיו, בתי משפט, רשם מאגרי המידע ורגולטורים אחרים, את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט באמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה.

בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה ככל שהארגון הוא ארגון שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותיות יותר. תפיסה זו, של חובות מודולריות נגזרת ישירות מעקרון היסוד של אבטחת מידע שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטויה גם במסמכים דומים בעולם.

נוסח מוצע לתקנות מכוח חוק הגנת הפרטיות, התשמ"א-1981

לעניין אבטחת מידע במאגרי מידע

הגדרות

1. בתקנות אלה -

"אחראי האבטחה" – מנהל המאגר כהגדרתו בסעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981[27] (להלן – החוק), ואם מונה ממונה על אבטחת מידע כאמור בסעיף 17ב לחוק – גם הממונה;

"חומר מחשב", "מחשב" ו"פלט" – כהגדרתם בחוק המחשבים, התשנ"ה-1995[28].

"עובד" -

(1) ביחס לבעל מאגר - לרבות יחיד המבצע פעולות בקשר למאגר מטעמו של בעל המאגר ועל פי הרשאתו, ולמעט עובד של מחזיק;

(2) ביחס למחזיק - לרבות יחיד המבצע פעולות בקשר למאגר מטעמו של המחזיק ועל פי הרשאתו;

"התקן נייד" - מחשב נייד או התקן נתיק המשמש לאחסון חומר מחשב ;

"מאגרים שחלה עליהם רמת האבטחה הבינונית" - מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה;

"מאגרים שחלה עליהם רמת האבטחה הגבוהה" - מאגרי מידע מן הסוגים המפורטים בתוספת השנייה;

[27] ס"ח התשמ"א, עמ' 128.
[28] ס"ח התשנ"ה, עמ' 366.

"תקן ישראלי" - כמשמעותו בחוק התקנים, התשי"ג-1953[29].

אחריות כוללת לאבטחת המידע במאגר

2. (א) בעל מאגר יגדיר במסמך המחייב גם את עובדי המאגר (להלן – הגדרות המאגר), לכל הפחות, את כל העניינים האלה:

(1) תיאור של סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) לתוספת הראשונה, וכן הערכת הרגישות של כל סוג מידע;

(2) המטרות המותרות של השימוש במידע שבמאגר;

(3) פירוט לעניין העברת מידע מהמאגר מחוץ לגבולות המדינה-ארץ היעד, מטרת ההעברה וזהות הנעבר;

(4) פירוט לעניין ביצוע פעולות עיבוד מידע באמצעות מחזיק;

(5) הסיכונים המרכזיים לפגיעה בשלמות המידע, חשיפתו או שימוש בו שלא כדין, ואופן ההתמודדות איתם.

(ב) בעל מאגר -

(1) יעדכן את הגדרות המאגר בכל שינוי שחל במאגר, הנוגע לעניינים המנויים בתקנת משנה (א) או לעניינים אחרים שהוא כבר כלל בהגדרות המאגר;

(2) יבחן אחת לשנה לפחות, אם יש צורך בעדכון הגדרות המאגר, כאמור בפסקה (1).

(ג) על מנת להפחית את סיכוני אבטחת המידע למידע שבמאגר, יבחן בעל המאגר לפני הקמת מאגר המידע ולכל אורך פעילותו של מאגר המידע, כי המידע הנאסף והנשמר על ידו אינו מעבר לנדרש לצורך מימוש מטרות המאגר.

(ד) בעל מאגר יתכנן, ככל הניתן מראש, את פעילות המאגר ואת מערכותיו באופן שיפחית את סיכוני אבטחת המידע למידע שבמאגר.

ממונה על אבטחת מידע

3. (א) בלי לגרוע מהוראות תקנה 2, מונה ממונה על אבטחת מידע במאגר המידע (להלן – ממונה על אבטחה), יהיה הממונה אחראי על אבטחת המידע במאגר.

[29] ס"ח התשי"ג, עמ' 30.

(ב) זהות הממונה על אבטחה, סמכויותיו ותפקידיו יוגדרו בצורה ברורה על ידי בעל המאגר.

(ג) הממונה על אבטחה יהיה כפוף ישירות לבעל המאגר.

(ד) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה.

נוהל אבטחה

4. (א) אחראי האבטחה יערוך נוהל אבטחת מידע (להלן – נוהל האבטחה) בהתאם לתקנות אלה ובהתאם להגדרות המאגר, ועל בסיס סקר הסיכונים השנתי, ככל שנערך כזה.

(ב) נוהל האבטחה יחייב את כל העובדים שיש להם גישה למערכות המחשוב של המאגר, או לכל מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו כאמור בתקנה 5(א)(5).

(ג) נוהל האבטחה יכלול, בין היתר, התייחסות לכל אלה:

(1) תיאור של רכיבי המערכות כאמור בתקנה 5(א) ותיאור מבנה הרשת שבה פועל המאגר;

(2) קביעת הרשאות גישה למידע במאגר בהתאם לתקנה 8;

(3) הוראות למורשי הגישה למאגר המידע לצורך שמירה על אבטחת המידע במאגר בעת השימוש בו.

(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל האבטחה, בנוסף לאמור בתקנת משנה (ג), התייחסות גם לכל אלה:

(1) הוראות בעניין האבטחה הפיזית והסביבתית של מתקני המאגר כאמור בתקנה 6;

(2) אופן הבקרה על השימוש במאגר המידע, ובכלל זה רישום של הגישה למערכות המחשוב של המאגר;

(3) הוראות לעניין אבטחת מערכות התקשורת אל מערכות המאגר וממנו;

(4) הוראות לעניין ניהול והעברה של אמצעי אחסון והתקנים ניידים;

(5) הוראות לעניין אופן גיבוי המידע ושחזורו;

(6) הוראות לעניין ביצוע ביקורות תקופתיות כדי לוודא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה.

(ה) נוהל האבטחה יהיה עדכני בכל עת, וייבחן מחדש בכל פעם שמתבצעים שינויים מהותיים במערכות המאגר או ככל שיש בכך צורך כתוצאה מהביקורת התקופתית.

מיפוי וביצוע סקר סיכונים

5. (א) בעל מאגר יערוך רשימת מצאי של מכלול רכיבי המערכות המשמשות את המאגר (להלן – מערכות המאגר), ובכלל זה -

(1) מערכות חומרה, רכיבי תקשורת, לרבות ציון של מיקומם הפיזי;

(2) התקנים ניידים, לרבות ציון זהות האדם העושה בהם שימוש;

(3) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ותחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

(4) תוכנות המשמשות לתקשורת אל מערכות המאגר ומהן;

(5) כל מידע או רכיב אחר הנדרש לצורך הפעלת המאגר או לצורך גישה אליו, ושיש לו חשיבות מבחינת אבטחת מידע.

(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); תוצאות סקר הסיכונים יועבר לאחראי האבטחה ולבעל המאגר, אשר ידונו בהם ויבחנו את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעלו לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו.

(ג) רשימת מצאי וסקר סיכונים כאמור בתקנה זו, לפי העניין, ייערכו מדי שנה עד יום 31 בדצמבר.

אבטחה פיזית וסביבתית

6. (א) אחראי האבטחה יבטיח כי המערכות המפורטות בתקנה 5(א) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - ינקוט אחראי האבטחה אמצעים סבירים לבקרה ולתיעוד של הגישה לאתרים שבהם מצויות מערכות המאגר (בתקנות אלה – מתקני המאגר), של הגישות שבוצעו בפועל, ושל הכנסה והוצאה של ציוד אל מתקני המאגר ומהם.

אבטחת מידע בניהול כח אדם

7. (א) קליטת עובדים למשרות המחייבות שימוש במידע ממאגר המידע, תיעשה תוך נקיטת אמצעים סבירים לבירור כי אין חשש להתאמתם לגישה למידע; אמצעים אלה יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקידים שאליהם מיועדים העובדים הנוגעים בדבר, כאמור בתקנה 8.

(ב) בעל מאגר יפעל להדרכת עובדים כאמור בתקנת משנה (א), לקיום החובות לפי תקנות אלה, בטרם יקבלו גישה למידע ממאגר המידע.

(ג) עובדים כאמור בתקנת משנה (א) יחתמו בטרם קבלת גישה למידע ממאגר המידע על התחייבות לשמור על סודיות בנוגע למידע שבמאגר בהתאם להוראות סעיף 16 לחוק, ועל התחייבות לקיים את החובות לפי תקנות אלה.

(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - יקיים בעל המאגר פעילות הדרכה תקופתית, בדבר הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, ובדבר חובות העובדים לפיהם.

ניהול הרשאות גישה

8. (א) הרשאות הגישה של עובדים למאגר המידע ייקבעו על בסיס הגדרת תפקיד; הרשאת הגישה לכל תפקיד תהיה בהיקף ובמידה הנדרשים לביצוע התפקיד בלבד.

(ב) אחראי האבטחה ינהל רישום מעודכן של תפקידים, הרשאות הגישה שנקבעו להם, ועובדים הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).

(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יתקיימו גם כל אלה:

(1) מידור הגישה לחלקים רגישים של מערכות המאגר, ובכלל זה מערכות האחסון של המידע ומנגנוני התיעוד לפי תקנות 10 ו-11, כך שלעובד יחיד לא תהא גישה לכל החלקים הרגישים, אלא אם כן הדבר חיוני לפעילותו של בעל המאגר;

(2) ביצוע פעולות חיוניות לא יהא בשליטתו של עובד אחד בלבד; לעניין זה, קביעת ההרשאות כאמור בתקנת משנה (א) ואפשרות העתקתו של כלל מאגר המידע או חלק מהותי ממנו, ייחשבו כפעולה חיונית.

זיהוי ואימות

9. (א) במאגר המידע יופעלו אמצעים לוידוא כי הגישה למידע במאגר המידע נעשית רק בידי עובד המורשה לכך ובהתאם לרשימת ההרשאות התקפות.

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, אם האמצעים כאמור בתקנת משנה (א) מבוססים על שימוש בסיסמאות, יקבע נוהל האבטחה הוראות לעניין אורך הסיסמה, מספר הניסיונות השגויים, אופן הטיפול בתקלות ובאימות זהות, ותדירות החלפת הסיסמאות שתיקבע בהתאם לתפקיד של מורשה הגישה, ובכל מקרה לא תעלה על ששה חודשים.

(ג) אחראי האבטחה ידאג לביטול ההרשאות של עובד שסיים את תפקידו ולשינוי סיסמאות וקודי גישה למאגר, שהעובד עשוי היה לדעת, מיד עם סיום תפקידו של העובד.

תיעוד גישה

10. (א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה ינוהל מנגנון תיעוד אוטומטי שיתעד כל ניסיון גישה למערכות המאגר (בתקנה זו – מנגנון התיעוד), ובכלל זה את כל הנתונים האלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה והאם הגישה אושרה או נדחתה; אם הגישה אושרה, יישמרו הנתונים המאפשרים זיהוי רכיב המערכת שאליו בוצעה הגישה.

(ב) מנגנון התיעוד לא יאפשר ביטול או שינוי של הפעלתו.

(ג) מנגנון התיעוד יהיה נתון לשליטתו הישירה של אחראי האבטחה, והוא יבחן פעם בחודש לפחות את נתוני התיעוד, ויערוך דו"ח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

(ד) נתוני הרישום של מנגנון התיעוד יישמרו למשך 24 חודשים לפחות.

(ה) אחראי האבטחה יידע את העובדים במאגר בדבר קיומו של מנגנון תיעוד המתעד את ניסיונות הגישה למערכות המאגר.

תיעוד של אירועי אבטחה

11. (א) אחראי האבטחה אחראי לתיעוד אירועים המעלים חשש לפגיעה בשלמות המידע או לשימוש בו בלא הרשאה (להלן - אירועי אבטחה); ככל הניתן יבוסס התיעוד האמור על רישום אוטומטי.

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יוגדרו בנוהל האבטחה הוראות לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ידון בעל המאגר באירועי האבטחה ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהם.

(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור בתקנת משנה (ג) אחת לרבעון לפחות.

ניהול והעברה של מסמכים והתקנים ניידים

12. (א) העתקה של מידע מהמאגר על גבי התקנים ניידים תיעשה באופן המונע שימוש לרעה בהם, ותוך נקיטת אמצעי הגנה סבירים ומקובלים; לעניין זה, שימוש תקין בשיטות הצפנה מקובלות ייחשב כנקיטת אמצעים סבירים.

(ב) התקנים ניידים שמאוחסן בהם מידע מהמאגר, יישאו על גביהם כתובת בולטת לעין: "מידע מוגן לפי חוק הגנת הפרטיות".

(ג) פלט של מידע מהמאגר יופק בלווית כתובת בולטת לעין בכל עמוד: "מכיל מידע מוגן לפי חוק הגנת הפרטיות".

(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יערוך אחראי האבטחה רשימת מצאי של התקנים ניידים המכילים מידע ממאגר המידע, באופן שיאפשר מעקב אחר מיקומם בכל עת, ויקיים מנגנון לתיעוד ולמעקב אחר משלוחים נכנסים ויוצאים של התקנים ניידים; חשש לגישה לא מורשית להתקן נייד או לפגיעה בו, לרבות אובדנו, ייחשב אירוע אבטחה ויחולו לגביו הוראות תקנה 11.

(ה) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, שמירת מידע בהתקנים ניידים, הוצאת התקנים ניידים המכילים מידע מחוץ למתקני המאגר, או עיבוד מידע מחוץ למתקני המאגר, ייעשו רק באישור מראש של אחראי האבטחה, אשר יקבע את רמת האבטחה הנדרשת במצבים אלו.

(ו) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יתויג המידע שבמאגר באמצעים טכנולוגים המאפשרים מעקב אחר העתקה של מידע מהמאגר ואחר השימוש שנעשה בו.

אבטחת תקשורת וניהול מאובטח של מערכות המאגר

13. (א) בעל המאגר יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.

(ב) מערכות המאגר לא יחוברו לרשת האינטרנט או לרשת ציבורית אחרת ללא התקנת אמצעי הגנה סבירים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

(ג) העברת מידע ממאגר המידע ברשת תקשורת אלחוטית, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש באמצעי הצפנה.

(ד) במאגר מידע שניתן לגשת אליו מרחוק באמצעות רשת תקשורת, בנוסף לאמצעי אבטחה כאמור בתקנות משנה (ב) ו-(ג), יש לעשות שימוש באמצעי זיהוי ואימות המאפשרים לזהות באופן סביר את זהות המתקשר ולאמת את ההרשאה שלו לביצוע הפעילות מרחוק ואת היקף ההרשאה.

(ה) אחראי האבטחה ידאג לכך שיתבצעו עדכונים שוטפים של המערכות והתוכנות המשמשות להגנה על המידע במאגר המידע, לרבות חומר המחשב הנדרש לפעולתן.

מיקור חוץ

14. (א) בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירותי עיבוד של המידע שבמאגר המידע, כולו או חלקו, או שירות אחר הכרוך במתן גישה למאגר המידע (להלן - השירות) -

(1) יבחן לפני ביצוע ההתקשרות כאמור, בשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות, האם מוצדק לבצע את השירות באמצעות גורם חיצוני בכלל ובאמצעות הגורם המסוים בפרט;

(2) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה:

(א) המידע שרשאי הגורם החיצוני לעבד;

(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;

(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;

(ד) משך תוקפה של ההתקשרות;

(ה) החובות בתחום אבטחת המידע החלות על הגורם החיצוני לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל המאגר, ככל שקבע;

(ו) חובתו של הגורם החיצוני להחתים את עובדיו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לצורך העיבוד המותר בחוזה וליישם את אמצעי האבטחה הקבועים בהסכם, כאמור בפסקת משנה (ה);

(ז) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - סמכותו של בעל המאגר לפקח על פעילותו של הגורם החיצוני כאמור בפסקה (4).

(3) ירשום בנוהל האבטחה של המאגר את העניינים המנויים בפסקה (2)(א) עד (ה), וכן יפנה בצורה מפורשת להסכם ולנוהל האבטחה של הגורם החיצוני כאמור בתקנת משנה (ב).

(4) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - ינקוט אמצעי בקרה ופיקוח כדי לוודא את עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה.

(ב) גורם חיצוני שהתקשר עם בעל מאגר כאמור בתקנת משנה (א), יחולו עליו הוראות תקנות אלה והוא יערוך נוהל אבטחה כאמור בתקנה 4, בשינויים המחויבים, וירשום בו גם את עניינים המנויים בתקנת משנה (א)(2)(א) עד (ז) ואת זהותו של בעל המאגר.

מחיקת מידע מהמאגר

15. (א) מידע המצוי במאגר מידע שכבר אין בו צורך לתפעולו השוטף של המאגר, יימחק אלא אם קיים צורך על פי דין לשומרו לצרכי גיבוי; גיבוי כאמור יישמר בנפרד באופן שיפחית את סיכוני אבטחת המידע לשימוש לא מורשה בו.

(ב) כל אמצעי אחסון המכיל מידע המיועד למחיקה - יושמד או יימחק על ידי נקיטת אמצעים שנועדו למנוע גישה למידע הכלול בו או שחזור שלו בשלב מאוחר יותר.

ביקורות תקופתיות

16. (א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תיערך פעם בשנתיים לפחות, ביקורת פנימית או חיצונית, שתוודא את עמידתו בהוראות תקנות אלה.

(ב) אם נערכת ביקורת פנימית, לא יהיה המבקר מי שנושא בתפקיד ממונה אבטחה של המאגר.

(ג) דו"ח הביקורת ידווח על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב, ויסתמך גם על ממצאים ממערכות המחשוב של בעל המאגר.

(ד) דוחות הביקורת יועברו לאחראי האבטחה וכן לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהם.

גיבוי, שחזור והתאוששות

17. (א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע אחראי האבטחה -

(1) נהלי עבודה לביצוע גיבויים מדי שבוע, לכל הפחות, אלא אם המידע לא עודכן במהלך אותו זמן;

(2) נהלי התאוששות, כדי להבטיח שבכל עת ניתן יהיה לשחזר את המידע למצבו המקורי ברגע שיתרחש אובדן או הרס.

(ב) אחראי האבטחה יבטיח כי מדי שישה חודשים ייערך אימות של נכונות ההגדרות, הפעולות והיישום של הנהלים עבור יצירת גיבויים ושחזור של המידע, כאמור בתקנת משנה (א).

(ג) במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע לפי תקנה זו, ובכלל זה יתועדו זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

(ד) לשם ביצוע נהלי ההתאוששות כאמור בתקנת משנה (א)(2), נדרש אישור של אחראי האבטחה.

(ה) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יישמר עותק גיבוי של המידע ושל נהלי ההתאוששות כאמור בתקנת משנה (א)(2), אשר מתקיימות גם לגביו דרישות אבטחת המידע לפי תקנות אלה, מחוץ למתקני המאגר, או שייעשה שימוש באמצעים שיבטיחו את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס.

סמכויות הרשם

18. (א) הרשם רשאי לתת הוראות או הנחיות לגבי כלל מאגרי המידע, בכל עניין הנוגע לאבטחת מידע וליישום תקנות אלה, לרבות פירוט של אמצעי האבטחה שיש לנקוט במצבים ובמקרים שונים, תקנים ושיטות אבטחה מקובלים שיש להשתמש בהם.

(ב) הרשם רשאי לפטור סוגי מאגרי מידע או מאגרים מסוימים מחובות אבטחת מידע לפי תקנות אלה, בין היתר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר, או מספר העובדים במאגר.

(ג) הרשם רשאי להורות כי עמידה בהוראות תקן מקובל או בהנחיות של רשות מוסמכת בעניין אבטחת מידע, תפטור מתחולת תקנות אלה כולן או חלקן; לעניין זה -

"רשות מוסמכת" - רשות בישראל המוסמכת על פי דין לתת הנחיות בעניין אבטחת מידע;

"תקן מקובל" – תקן אבטחת מידע שהוא תקן ישראלי או תקן של גוף מוכר שאיננו ישראלי, שהרשם אישר לעניין זה.

תחולה

19. (א) על מאגרי מידע שאינם מאגרים שחלה עליהם רמת האבטחה הבינונית או רמת האבטחה הגבוהה - יחולו הוראות תקנות אלה, למעט תקנות 4(ד), 5(ב), 6(ב), 7(ד), 8(ג), 9(ב), 10(א), 11(ב) עד (ד), 12(ד) עד (ו), 14(א)(2)(ז) ו-(4), 16(א) ו-17(א)ו-(ה).

(ב) על מאגרים שחלה עליהם רמת האבטחה הבינונית - יחולו הוראות תקנות אלה, למעט תקנות 5(ב), 8(ג), 11(ד), 12(ו) ו-17(ה).

(ג) על מאגרים שחלה עליהם רמת האבטחה הגבוהה - יחולו בנוסף להוראות התקנות החלות על מאגרים שחלה עליהם רמת האבטחה הבינונית - גם הוראות תקנות 5(ב), 8(ג), 11(ד), 12(ו) ו-17(ה).

(ד) הוראות תקנות אלה יחולו גם על מחזיק של מאגר, בשינויים המחויבים, ובכל מקום שכתוב "בעל המאגר" יראו כאילו כתוב "המחזיק של מאגר".

פטור מתחולה

20. על אף הוראות תקנות אלה, על מאגר מידע אשר בבעלות יחיד שאינו תאגיד אשר רק לו יש גישה אל המאגר, יחולו הוראות תקנות 2(ג) ו-(ד), 5(א), 6(א), 9(א), 12(א), 13 ו- 15 בלבד.

תוספת ראשונה

(תקנה 1)

1. מאגרי מידע שחלה עליהם רמת האבטחה הבינונית:

(1) מאגר מידע המשמש לשרותי דיוור ישיר או למכירה של מידע באופן אחר;

(2) מאגר מידע שבבעלות גוף ציבורי כמשמעותו בסעיף 23 לחוק;

(3) מאגר מידע הכולל מידע שהוא אחד מאלה:

(א) מידע על צנעת חייו האישים של אדם;

(ב) מידע רפואי או נפשי;

(ג) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000[30];

(ד) מידע כלכלי, לרבות מידע אודות הרגלי הצריכה של אדם;

(ה) מידע אודות דעות פוליטיות ואמונות דתיות;

(ו) מידע אודות נטיות, הרגלים ומעשים מיניים;

(ז) מידע אודות עברו הפלילי של אדם;

(ח) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח – 2007[31];

(ט) מידע שהוא מאפיין אנושי פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת– ומשמש לזיהוי.

2. על אף האמור בפרט 1(3) לתוספת זו, מאגר מידע המקיים אחד מאלו, יראו אותו כאילו אינו מאגר שחלה עליו רמת האבטחה הבינונית, ויחולו לגביו הוראות תקנה 19(א):

(1) המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ד), (ז), (ח) או (ט) לתוספת זו, אך ורק אודות העובדים או הספקים של בעל מאגר המידע, ובלבד שהמידע נדרש למטרות ניהול העסק בלבד;

(2) מאגר המידע מפורסם לכלל הציבור לפי סמכות כדין;

(3) מספר המועסקים אצל בעל המאגר אינו עולה על 10.

3. מחזיק במאגרי מידע השייכים לחמישה בעלים שונים לפחות, יחולו לגביו הוראות תקנה 19(ב) ויראו אותו כמחזיק במאגר שחלה עליו רמת האבטחה הבינונית, אף אם מאגרי המידע שבהחזקתו אינם מאגרים כאמור בפרט 1 לתוספת זו; הוראות פרט זה לא יחולו לגבי מאגרי מידע שמתקיים בהם האמור בפרט (2)(1) או (2) לתוספת זו.

[30] ס"ח התשס"א, עמ' 62
[31] ס"ח התשס"ח, עמ' 72.

תוספת שניה

(תקנה 1)

מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה:

(1) מאגר מידע כאמור בפרט (1) לתוספת הראשונה, שיש בו מידע אודות 100,000 אנשים ומעלה.

ד ב ר י ה ס ב ר

תקנה 1 – הגדרות

ההגדרות העיקריות בתקנות המוצעות הן אלה:

"אחראי האבטחה" – חובות אבטחת המידע השוטפות, מוטלות על מנהל המאגר כהגדרתו בסעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק), ואם מונה ממונה על אבטחת מידע כאמור בסעיף 17ב לחוק – גם על הממונה.

"עובד" – מטרת ההגדרה להתמקד בחובות של מי שיש לו גישה למידע במסגרת פעילותו בארגון, ולצורך כך המבחן הוא פונקציונאלי וגמיש. משום כך המוקד אינו דיני העבודה, אלא מכלול בעלי ההרשאות לגישה למאגר שגישתם למידע נקבעת בידי הארגון בעל המאגר, ובכלל זה עובד שמתקיימים ביחס אליו יחסי עובד-מעביד וגם עובד קבלן. מאחר שתקנות אלה חלות גם על מחזיק במאגר שקיבל את המאגר לעיבוד מבעל המאגר (כאמור בתקנה 19(ד) המוצעת), לכן גם ביחס למחזיק יחולו ההוראות האמורות של ההגדרה "עובד", בשינויים המחויבים, לעניין "עובד" של המחזיק.

"**מאגרים שחלה עליהם רמת האבטחה הבינונית**" – מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה. מאגרים אלה הינם מאגרים בעלי רגישות בינונית, שנקבעה בהתאם לשילוב של פרמטר כמותי (היקף המועסקים) ופרמטר מהותי (סוג המידע המעובד). הפרמטר הארגוני נבחר כפרמטר כמותי מוביל משום שהיקף מורשי הגישה הלגיטימיים למידע בארגון, הם שקובעים במידה רבה את היקף החשיפה של המידע, ובהתאם לכך מהווים אינדיקציה למידת הסיכון שבתפעול המאגר, ולצורך בהתמודדות עם סיכון זה באמצעות כלים בתחום אבטחת המידע.

"מאגרים שחלה עליהם רמת האבטחה הגבוהה" – אלה הם מאגרים שרגישותם נקבעה בהתאם לשילוב של פרמטרים כמותיים (היקף המועסקים והיקף המידע במאגר), מהותי (סוג המידע המעובד) וכמותי (היקף המידע). ההנחה היא כי סיכונים מערכתיים, לאוכלוסיות גדולות, ממוקדים במאגרים מסוג זה;

תקנה 2 – אחריות כוללת לאבטחת המידע במאגר

תקנות משנה (א) ו-(ב)

מטרת התקנה לקבוע כי בעל מאגר המידע צריך להכיר את פעילות עיבוד המידע המבוצעת על ידו, האפיון של המידע המצוי במאגר, דרגות הרגישות שלו, ולבחון את הסיכונים השונים לפעילות זו ואופן ההתמודדות איתם. הגדרה ברורה של הנהלת הארגון בנושא זה משמשת נקודת מוצא חיונית לקבלת החלטות ומימוש האחריות הניהולית של בעל המאגר. לצורך כך על בעל המאגר להגדיר מהם האיומים על המידע, ומהם הנזקים והפגיעות שיגרמו לנושאי המידע, בשל תקלה או פריצת אבטחת מידע.

על הארגון להגדיר את הדברים במסמך אחיד גם על מנת לוודא תיאום בין נושאי המשרה השונים בתוך הארגון, בהקשר לחובותיהם השונות לפי תקנות אלה (כגון מנהל מערכות המידע, מנהל משאבי אנוש, קב"ט וכדומה).

בהתאם לסעיף 9 לחוק, נדרש כיום בעל מאגר לכלול חלק מפרטים אלה בבקשת רישום המאגר, ובכלל זה בהתאם להוראות סעיף 9(ב) לחוק:

"

(1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל;
(2) מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע;
(3) סוגי המידע שיכללו במאגר;
(4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה."

ולפי הוראת 9(ד) לחוק, על בעל מאגר ומחזיק לעדכן את רשם מאגרי המידע (להלן – הרשם) בדבר שינויים בפרטים אלה.

תקנות משנה (ג) ו-(ד)

מטרת הוראות אלה לקבוע כי יש לנקוט אמצעים סבירים בכל השלבים של תפעול מערכות מאגר המידע, ובכלל זה בשלב המקדמי של עיצובן, להפחית את סיכוני אבטחת המידע. בהקשר זה התקנה נועדה לבטא גם תובנה מקובלת, שעדיף להטמיע את שיקולי אבטחת המידע בעת עיצוב המערכת. במסגרת זו על בעל המאגר, בין היתר, לבחון האם המידע הנאסף והנשמר על ידו אינו מעבר לנדרש לצורך מימוש מטרות המאגר, וכן לשקול אם מטרות המאגר מאפשרות שימוש במידע בדרך שתאפשר שמירה על האנונימיות של נושא המידע (אנונימיזציה).

תקנה 3 – ממונה על אבטחת מידע

לפי סעיף 17ב לחוק נדרשים גופים מסוימים, בנוסף לאחריותם לפי סעיף 17 למנות גם "ממונה אבטחה" שהינו בעל הכשרה מתאימה. ביחס לגופים אלה, נקבע כי החובות המנויות בתקנות למנהל מאגר, יחולו בנוסף על הממונה.

נקודה משמעותית שיש לתת עליה את הדעת היא להגדיר מהם הכלים והסמכויות לממונה על אבטחה בתוך הארגון על מנת שיוכל לממש את חובות הארגון בתחום זה. דברים אלה נכונים גם לגבי ממונה על אבטחה שמונה בידי בעל מאגר, אפילו אם חלה עליו חובה למנות ממונה לפי סעיף 17ב לחוק.

תקנה 4 – נוהל אבטחה

התקנה מחייבת את אחראי האבטחה לערוך נוהל אבטחה ארגוני. מטרתו של הנוהל היא לייצר מדיניות אבטחה ארגונית, לקבוע כללים ונהלים המחייבים את כל עובדי הארגון, וליצור מודעות לסוגיית אבטחת המידע במאגרי הארגון ולחשיבות העמידה בכללים שנקבעו. קיום של נוהל אחיד ומחייב מאפשר אחידות בסדרי העבודה מול מאגרי המידע, נגישות להוראות במקרה של ספק, ומאפשר קיום תשתית להתחייבות כל עובד לעמוד בתנאיה.

נוהל האבטחה ייערך ברמת פירוט ובהיקף משתנה בהתאם לסוג הארגון. ברמה הבסיסית נדרש נוהל זה לכלול מיפוי של מערכות המידע של הארגון, פירוט ההרשאות למערכות המידע ואופן השמירה על הוראות אלה. במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, ובהתאם לחובות המהותיים החלים לעניין רמות אלה, יידרש הנוהל לכלול הוראות נוספות.

על הנוהל להיות מעודכן ותואם בכל עת, הן את מצב המערכת והן את התקנות.

תקנה 5 – מיפוי וביצוע סקר סיכונים

תקנת משנה (א)

גוף המבקש לגשת לאבטחת המידע המצוי במאגר המידע שלו, צריך קודם כל למפות את רכיבי מערכות המידע שלו, כדי שניתן יהיה להגן עליהם בצורה יעילה בעזרת אמצעי אבטחה מתאימים.

לכן בשלב הראשון נדרש בעל מאגר לערוך רשימה מסודרת של כל רכיבי מערכות המחשב המשמשות להפעלת מאגר המידע או הקשורות אליו, לרבות ציוד מחשב וציוד תקשורת (רכיבי החומרה), ותוכנות מחשב (רכיבי התוכנה), כמפורט להלן:

- מערכות החומרה כוללות בין היתר: מחשבי שולחן, שרתי מחשב, תחנות עבודה, מדפסות, אמצעי מיתוג ובקרה כגון - התקני חומת-אש פיזיים, ראוטרים, מתגים, ומודמים, התקנים ניידים המתחברים לרשת כמו מחשבים ניידים, מחשבי כף יד, ואמצעי זיכרון ניידים.
- מערכות התוכנה כוללות בין היתר: מערכות הפעלה של המחשבים, יישומים (אפליקציות) לגישה לנתונים שבבסיסי הנתונים במאגר, יישומים לעיבוד נתונים, יישומי תקשורת נתונים ומערכות הגנה כגון: אנטי-וירוס, חומת-אש (פיירוול) ותוכנות אנטי-רוגלות.

קיומה של רשימה מסודרת של רכיבי החומרה ורכיבי התוכנה, מסייעת לאחראי על האבטחה במאגר, לבצע מעקב מתמיד אחר מצאי רכיבי המערכת, ללא החמצת התייחסות לאף אחד מהרכיבים. התמונה הכללית המתקבלת מהרשימה המלאה מעניקה לאחראי "מבט על" המאפשר זיהוי נקודות תורפה וסיכונים ונקיטת אמצעים אבטחה הולמים לטיפול בהם.

מעבר לעריכת רשימת רכיבי מערכות המחשב, יש צורך לציין את מיקומם הפיזי של כל אחד מרכיבי החומרה. למיפוי של מיקום הרכיבים השונים יש חשיבות רבה, מאחר שהוא מדגיש את מקומו של כל רכיב בתוך המערכת הכללית, ואת היחס בינו לבין הרכיבים האחרים. מיפוי זה מאפשר זיהוי של תהליכי העבודה במערכת, ובמקרה של ליקוי אבטחה, מאפשר לזהות את מקורו ואת תחומי השפעתו.

תקנת משנה (ב)

התקנה קובעת כי במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה, אין להסתפק בדרישות תקנת משנה (א), אלא יש לבסס את אבטחת המידע על מסמך מקיף ומעמיק יותר – "סקר הסיכונים". הכוונה בביטוי "סקר סיכונים" לסקר הנערך בידי בעל מקצוע בעל הכשרה מתאימה במטרה לזהות ולדרג את רמת הסיכון הקיימת בכל אחת ממערכות המחשוב שבמאגר המידע, על סמך מאפייני סיכון שייקבעו.

תוצאות סקר הסיכונים יועבר לאחראי האבטחה ולבעל המאגר, אשר ידונו בהם ויבחנו את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעלו לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו.

תקנת משנה (ג)

התקנה קובעת כי המיפוי והסקר האמורים בתקנות משנה (א) ו-(ב) יבוצעו בתדירות של פעם בשנה קלנדרית לפחות. מערכות תוכנה וחומרה נתונים באופן מתמיד לאפשרויות שדרוג, עדכון, ושינוי רכיבים. כל שינוי כזה במערכת החומרה או התוכנה, משפיע באופן ישיר על רכיבים אחרים

במערכת בהיותם תלויים ברכיב שהשתנה או שהוא תלוי בהם. ההשפעה של כל שינוי עלולה לייצר סיכוני אבטחה חדשים, או ליצור שינוי במבנה המערכת, המחייב התייחסות בראי אבטחת המידע.

בנוסף, איומי אבטחה נוצרים חדשות לבקרים, עם גילוי פרצות או חשיפות במערכות נפוצות. לכן, יש צורך לקיים בחינה חוזרת של מבנה המערכת ורכיביה, כדי להפיק תמונת מצב עדכנית ונאמנה למקור. ובמאגרי מידע המחויבים בסקר סיכונים, קיים צורך לעדכן את סקירת הסיכונים במערכת בהתאם לשינויים שנעשו. קביעת תדירות החובה לביצוע הבדיקות נותנת מענה למעקב אחר השינויים שחלו במערכת בזמן שחלף מאז הבדיקה האחרונה.

תקנה 6 – אבטחה פיזית וסביבתית

התקנה מחייבת שמירה על מידור פיזי של מערכות החומרה הקשורות לניהול מאגרי המידע. המערכות ימצאו במקום מוגן, שכניסה אליו מתאפשרת רק לעובדים בעלי הרשאה מתאימה, בהתאם לסיווגם הביטחוני.

הקפדה על אבטחה פיזית של המערכות מונעת גישה של גורמים לא מורשים אל מערכות המידע. מניעת גישה זו חשובה מאוד לאור העובדה כי הגדרות הליבה של המערכת ואמצעי ההגנה הלוגיים שלה ניתנים לשינוי ועדכון בשיטות שונות המתאפשרות על ידי הגישה הפיזית. גישה פיזית אף עלולה לאפשר גניבת אמצעי האחסון הפיזיים ובכך שימוש לא מורשה במידע.

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יש לתעד את הכניסות והיציאות של העובדים אל מתקני המאגר, וכן לתעד הכנסת ציוד אל המתקנים, והוצאת ציוד מהם. תיעוד מלא מאפשר מעקב ובקרה במקרה של כשל אבטחתי. באמצעות התיעוד ניתן להצביע על גורם הכשל, ולנקוט באמצעי פתרון מתאימים.

תקנה 7 – אבטחת מידע בניהול כח אדם

הגורם האנושי הינו גורם סיכון משמעותי בתחום אבטחת מידע. תובנה מקובלת המבוססת על לימוד של אירועי אבטחה, מלמדת כי שיעור גבוה של אירועי אבטחה נובע מהתנהלות כוח האדם בארגון.

כחלק ממערך הצעדים הננקטים על מנת לשמור על אבטחת המידע שבמאגר, יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע, עובדים המתאימים לעבודה זו, מבחינת אמינותם ויושרם. את רמת הסיווג הנדרש יש להתאים לרגישות המידע במאגרים, ולאופי הארגון שבו מתעתד המועמד לעבוד.

בשלב הבא, לאחר שהוחלט כי המועמד אכן מתאים לעבודה הנוגעת למאגרי המידע, יש להבהיר לעובד החדש, בטרם יקבל גישה למאגרים, את חובותיו לפי חוק הגנת הפרטיות, ולפי התקנות. את הבהרת חובותיו ניתן לממש בצורה של הדרכה מובנית לעובדים חדשים, שתועבר על ידי אחראי אבטחת המידע, או על ידי גורם מתאים אחר, ורצוי אף באמצעות חוברת מידע בסיסית המבהירה נושא זה. מובן כי היקף העיסוק בנושא משתנה בין ארגונים בהתאם לתפקיד.

טרם קבלת הגישה למאגר, ולאחר הבהרת החובות לפי חוק לעובד החדש, יחתום העובד על התחייבות לשמירת סודיות בקשר למידע אליו הוא נחשף במסגרת עבודתו עם מאגרי המידע של הארגון, התחייבות זו תואמת להוראות סעיף 16 לחוק.

בנוסף על האמור לעיל, על מנת לרענן את חשיבות אבטחת המידע ואת החובות הנובעות ממנה, מוצע כי במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יחוייב בעל המאגר לערוך פעילויות הדרכה תקופתיות. פעילויות ההדרכה יכללו סקירה של מסמכי האבטחה המחייבים בארגון: הגדרות המאגר, נוהל האבטחה, והחובות לפי התקנות.

יש לוודא כי עובדים מודעים לסיכון שגורמים שונים ינסו לרמות או להונות אותם על מנת לגרום להם להוציא מידע מהמאגר בדרכי מרמה, ואת חובתם לבדוק כי מידע המופק מהמאגר ניתן למי שזכאי לכך.

תקנה 8 – ניהול הרשאות גישה

התקנה מחייבת לוודא כי הגישה למידע במאגר תתאפשר רק לאותו עובד אשר קיים צורך לאפשר את גישתו למידע בהתאם להגדרת תפקידו. פעולה זו מתבצעת על ידי ניהול הרשאות גישה. לכל עובד מוצמדת רמת הרשאה המתאימה לתפקידו, והמאפשרת לו את היקף הגישה למידע על פי רמת הרשאתו. הקצאת ההרשאות תבוסס על גישת "צריך לדעת" שמשמעותה: אם העובד לא צריך גישה למידע מסוים לצורך עבודתו, אזי לא נאפשר לו את הגישה לאותו מידע.

לרוב, כאשר עובד מבצע כניסה למחשב האישי שלו, הוא נדרש להקיש שם משתמש וסיסמא, או לספק אמצעי זיהוי אחר. באמצעותו המערכת מזהה אותו, ומאפשרת לו את הגישה בהתאם לרמת ההרשאה שנקבעה לו מראש.

בנוסף, במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יש ליישם תובנות מתקדמות יותר בתחום אבטחת המידע, הדורשות פיצול הסמכות לבצע פעולות קריטיות במערכות רגישות או חיונית בין שני אנשים, באופן שמפחית את איומי האבטחה.

תקנה 9 – זיהוי ואימות

תקנת משנה (א)

כדי לאמת שמי שניגש למידע במאגר המידע הינו אכן עובד מורשה, יש לוודא כי תשויך זהות פיזית להרשאה כפי שהוגדרה במערכות המחשב של המאגר. זאת כדי למנוע גישה של גורמים עוינים מחוץ לארגון או שימוש לרעה מתוך הארגון.

קיימים מספר מנגנונים המאפשרים אימות זהות של משתמש: שם משתמש וסיסמה, אמצעי חומרה פיזי (כגון כרטיס חכם), זיהוי ביומטרי, או שילוב של שניים או יותר מהאמצעים הללו.

תקנת משנה (ב)

במאגרי מידע שחלה עליהם רמת אבטחת המידע הבינונית או הגבוהה, על הארגון לקבוע נוהל אבטחה לעניין השימוש בסיסמאות, בהתאם לרגישות התפקידים וההרשאות.

הנוהל יקבע קריטריונים ל"חוזק" סיסמאות. סיסמה "חזקה" היא סיסמא שקשה לפרוץ אותה, הואיל והיא ארוכה, מורכבת ממחרוזת תווים אקראית, ומשלבת סוגים שונים של תווים. לעומתה, סיסמה חלשה תהיה לרוב קצרה, בעלת היגיון פנימי (כמו רצף מספרים), או קשורה לבעלים שלה (כמו מספר הטלפון, תאריך לידה או מספר תעודת זהות). הקריטריונים יחייבו את העובדים ליצור סיסמה מספיק חזקה לצרכי הגישה שלהם למידע.

כמו כן, יקבע הנוהל את מספר הניסיונות להזנת סיסמה שגויה לפני שהמערכת חוסמת את אותו משתמש מגישה למערכת. חסימה זו מיועדת למנוע מצב של פיצוח הסיסמה על ידי ניסיונות חוזרים ונשנים של צירופים שונים.

כדי למנוע התחזות לעובד ועקיפת מנגנוני ההגנה, וכן במקרה של משתמש שנחסם, הנוהל יקבע מי אחראי לברר ולאפשר גישה העוקפת את מנגנוני ההגנה.

בנוסף נדרש שהנוהל יקבע מדיניות החלפת סיסמאות. התקנה מחייבת כי החלפת הסיסמאות תתבצע לפחות פעם בשנה. בעת גישה למידע רגיש, החלפת הסיסמה היא אמצעי חיוני לשימוש לא נאות בסיסמה, שהרי גם במקרה שהסיסמה תיחשף באופן כלשהו, טווח הנזק יצומצם לזמן שיחלוף עד להחלפתה בלבד.

במערכות רבות קיימות סיסמאות ברירת מחדל לכניסה להגדרות המערכת. (דוגמא נפוצה לכך היא ראוטר אלחוטי ביתי, שבו סיסמת ברירת היא "Admin", וכך גם שם המשתמש). על אחראי האבטחה לוודא את עדכון הסיסמאות, על מנת למנוע ממי שאינו מורשה גישה להגדרות רכיבי המערכת.

תקנת משנה (ג)

במקרה של עזיבת עובד את מקום העבודה, או שינוי בתפקידו, התקנה מחייבת את אחראי האבטחה לעדכן את רשימת הרשאות הגישה בארגון. במקרה של עזיבת העובד יש לבטל את ההרשאות המוקצות לו, וכן לשנות את הסיסמאות הכלליות שהשתמש בהם. במידה וחל שינוי בתפקידו של העובד, יש לעדכן את הרשאותיו בהתאם להרשאות המוקצות לאותו תפקיד חדש, ולבטל את הרשאותיו הקודמות. בהתאם לעדכונים הללו, אחראי האבטחה יעדכן גם את רשימת ההרשאות שערך לפי תקנה 8(ב), על מנת לקבל תמונה עדכנית של מצב ההרשאות בארגון.

תקנה 10 – תיעוד גישה

תקנת משנה (א)

במאגרי מידע שחלה עליהם רמת אבטחת המידע הבינונית או הגבוהה, מחייבת התקנה את אחראי האבטחה להפעיל מנגנון המתעד את הכניסות למערכת, את ניסיונות הכניסה למערכת, ואת הפעולות שבוצעו לאחר הכניסה למערכת. כל פעולה שכזאת תתועד בצמוד לזהותו של מבצע הפעולה, לזמן של ביצוע הפעולה, והמשאב הספציפי כלפיו כוונה הפעולה.

תקנת משנה (ב)

על המנגנון להיות עצמאי, לפעול באופן רציף, ללא אפשרות התערבות חיצונית, כולל התערבות של מפעילו. באופן כזה, תישמר אמינותו של המנגנון, ואמינות התיעוד. בהתקני Firewall פיזיים למשל, משולב מנגנון כזה במערך הניהול של ההתקן.

תקנת משנה (ג)

התקנה מחייבת את אחראי האבטחה לבחון את נתוני התיעוד שהפיק המנגנון מדי חודש. על אחראי האבטחה מוטלת החובה לבחון את התיעוד באופן מקצועי ומעמיק. עליו להתייחס לא רק לניסיונות כניסה שהמערכת דחתה, אלא אף לניסיונות כניסה שאושרו – תוך בחינת הלגיטימיות של האישור בניסיון למצוא כניסות לא מורשות למערכת. במידה והבחינה אכן גילתה ליקויים, על אחראי האבטחה לערוך דו"ח מסודר המפרט את הליקויים שנמצאו, ואת הצעדים שננקטו.

תקנת משנה (ד)

התקנה מחייבת לשמור את נתוני התיעוד האמור לפחות שנתיים. באופן כזה תתאפשר בחינה מדוקדקת של התיעוד במקרה של אירוע נקודתי שהתגלה בטווח של עד שנתיים מאוחר יותר.

תקנת משנה (ה)

התקנה מחייבת את אחראי האבטחה ליידע את עובדיו בדבר קיום התיעוד של פעולות הגישה שלהם למערכת. יידוע זה נועד להבטיח את מודעותו של העובד למעקב אחר פעולותיו, וממילא בעל גישה למערכת לא יבצע פעולות שאינן מורשות ביודעו כי פעולתו מתועדת.

תקנה 11 – תיעוד של אירועי אבטחה

תקנת משנה (א)

מטרת תקנה זו ליצור "זיכרון ארגוני" ביחסי לאירועי אבטחה, על מנת להפיק מהם לקחים. מוצע ככלל מנחה שנועד להקל על תחקור כאמור, להתבסס ככל הניתן על רישומים אוטומטים במערכות המידע של הארגון. מוצע כי אחראי האבטחה או צוותו יעשו שימוש ברישומים סטנדרטים, ובמידת הצורך ובהתאם לארגון, גם יוטמעו בארגון מנגנונים ייעודים המנהלים רישום אוטומטי אודות פעילות ברשת הארגון.

תקנת משנה (ב)

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, ייקבעו נהלי דיווח מסודרים אודות אירועי אבטחה לגורמים המוסמכים.

תקנות משנה (ג) ו-(ד)

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, מחייבת התקנה את אחראי האבטחה לדווח לבעל המאגר על אירועי האבטחה שזוהו על פי הוראות התקנות הקודמות. בעל המאגר ידון בדיווחי אחראי האבטחה, ועל פיהם יבחן האם יש צורך לעדכן את הגדרות המאגר או נוהל האבטחה. במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה ייערך דיון כאמור אחת לרבעון.

במקרים בהם נתוני אירועי האבטחה (כגון: כניסה בלתי מורשית למאגר, ניסיונות חדירה חיצוניים חוזרים ונשנים, שימוש חריג של עובד בהרשאתו לצורך גישה למשאבים יחודיים) מצביעים על כמות גדולה של אירועים, או על חומרתם המיוחדת, מתעורר הצורך לבחון את נהלי האבטחה, ובהתאם, לעדכן את המסמכים המיישמים את המדיניות. לכן, מטילה התקנה את החובה על בעל המאגר, לשקול את עדכון המסמכים בדונו על ממצאי אחראי אבטחת המידע מידי רבעון.

תקנה 12 – ניהול והעברה של מסמכים והתקנים ניידים

כללי

התקנים ניידים, כוללים לעניין תקנות אלה: מחשבים ניידים ומחשבי כף-יד, ואמצעי אחסון נתיקים כגון: תקליטורים, כונני פלאש למיניהם, כונני גיבוי ניידים וכיו"ב. התקנים אלה, מעצם טבעם כניידים, דורשים התייחסות מיוחדת, מאחר שככלל מדובר בהתקנים קטנים יחסית, הניתנים להעברה ממקום למקום, ולפיכך קיים סיכון כי מידע עלול לדלוף החוצה באופן לא מורשה על ידי שימוש בהם. כדי למנוע מצב כזה, יש לנקוט במספר צעדים לפי הוראת התקנה:

תקנת משנה (א)

מוצע לחייב נקיטה באמצעי הגנה סבירים על המידע המצוי על ההתקן הנייד, על מנת להקשות על שימושו בידי מי שאינו מורשה במקרה של אובדן ההתקן או גניבתו. קיימים שיטות שונות להגן על מידע בהתקנים ניידים. התקנה קובעת, כי הצפנת המידע על ההתקן הנייד, על ידי שימוש נכון בשיטות הצפנה מקובלות (לדוגמה, שימוש בתוכנה המשתמש בשיטות הצפנה כמו: PGP), תיחשב נקיטת אמצעים סבירים.

תקנות משנה (ב) ו-(ג)

מוצע לחייב כי התקנים ניידים שמאוחסן בהם מידע מהמאגר, וכן פלט של מידע מהמאגר יישאו על גביהם כתובת בולטת לעין שתתריע כי המסמך או ההתקן הנייד מכילים מידע מוגן לפי חוק הגנת הפרטיות.

תקנת משנה (ד)

כדי לאפשר לאחראי אבטחת המידע לפקח על ההתקנים הניידים הנמצאים בשימוש העובדים, ועל השימוש בהם, מוצע לחייב את אחראי האבטחה לערוך רשימה של ההתקנים הניידים המשמשים לשמירת מידע שנשלף ממאגר המידע, ואת פרטי העובד המחזיק בהם. כמו כן מחויב

אחראי האבטחה לקיים מנגנון לתיעוד ולמעקב אחר משלוחים נכנסים ויוצאים של התקנים ניידים. באופן כזה, מתאפשר מעקב אחר מיקומם של ההתקנים. כמובן, שיש לאסור על שימוש בהתקנים ניידים שאינם מופיעים ברשימה שערך אחראי האבטחה, לצורך שמירת מידע ממאגרי המידע של הארגון, כאמור בתקנת משנה (ה).

במקרה של אבדן או גניבה של התקן נייד המופיע ברשימה, או פגיעה בו, על אחראי האבטחה להתייחס למקרה כמקרה של אירוע אבטחה, ומוטלת עליו החובה לנקוט באמצעים לפי תקנה 11. דהיינו, תיעוד מקרה האבטחה, ודיווח לבעל המאגר במסגרת שאר אירועי האבטחה המדווחים לו.

תקנת משנה (ה)

התקנה אוסרת על שימוש בהתקנים ניידים, לאחסון מידע ממאגר המידע, באופן עצמאי על ידי עובד, ללא שקיבל על כך אישור מראש מאחראי האבטחה. עובד המעוניין להשתמש בהתקן נייד לצרכים אלו, חייב לפנות אל אחראי האבטחה, שישקול את הסיכון שבשימוש מול הצורך, ויחליט האם לאשר את השימוש בהתקן. בנוסף יעדכן האחראי את הרשימה שהכין לפי תקנת משנה (ד).

תקנת משנה (ו)

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יתויג המידע שבמאגר באמצעים טכנולוגים המאפשרים מעקב אחר העתקה של מידע מהמאגר ואחר השימוש שנעשה בו.

תקנה 13 – אבטחת תקשורת וניהול מאובטח של מערכות המאגר

תקנת משנה (א)

ברשת מחשבים ארגונית, ניתן לגשת מכל מחשב ברשת לכל מחשב אחר ברשת. גם אם מאגר המידע נמצא על מחשב אחד בלבד, הנעול בחדר מיוחד, אין זה אומר כי המאגר מוגן מפני גישה לא מורשית. העובדה כי המחשב מחובר ברשת לשאר המחשבים, גורמת סיכון של כניסה למחשב באמצעות הרשת.

התקנה מחייבת את בעל המאגר להפריד ככל האפשר בין המערכות המשמשות את מאגר המידע, כמו השרת שעליו מותקן המאגר, ותחנות הקצה בעלות גישה למאגר, משאר מערכות המחשבים הארגוניות. זאת, על מנת למנוע קישוריות בלתי רצויה, אל מחשבים או מערכות אשר לא נזקקים להשתמש במאגר המידע. קישוריות זו, עלולה לגרום שימוש לא נאות במאגר המידע.

קיימות מספר שיטות להפרדה זו, וביניהם: מערכת חומת אש פנימית, מערכת לחלוקת רשתות, ועוד.

תקנת משנה (ב)

בהמשך לסכנות שנמנו בתקנה הקודמת, במידה ומערכות המידע המשמשות את מאגר המידע מחוברות לרשת האינטרנט, נוצר סיכון של גישה חיצונית מתוך רשת האינטרנט – אל מערכות המידע של הארגון.

אכן, תובנה מקובלת היא כי:

> **"ארגונים ומערכות המידע ורשתות התקשורת שלהם עומדים יותר ויותר מול איומי אבטחה שמקורם בקשת רחבה של גורמים המסתייעים במחשבים, כגון איומי הונאה, ריגול, חבלה, ונדליזם, וכן מול איומי שרפה או הצפה, נזקים שמקורם בתקיפה של וירוסים, פריצה למחשבים ובמניעת שירות, הפכו להיות יותר שכיחים ויותר נועזים, והתחכום שלהם גדל כל העת.**
>
> **...**
>
> **קישור בין רשתות ציבוריות ופרטיות והשימוש המשותף במשאבי מידע, מקשה יותר ויותר על בקרת הגישה. המגמה לבזר את שירותי המחשוב החלישה את האפקטיביות של בקרה מרכזית מקצועית." [ת"י 7799, מהמבוא, עמ' 2].**

על מנת להקטין את הסיכון למינימום, התקנה מחייבת, כי במידה והמערכות מתחברות לרשת האינטרנט, יש להתקין על גבי המערכות אמצעי הגנה סבירים מפני חדירה לא מורשית, או תוכנות מזיקות. אמצעי ההגנה הנפוצים היום כוללים: תוכנת אנטי-וירוס עדכנית, תוכנת אנטי-רוגלות עדכנית, תוכנת חומר אש, והתקן חומת אש פיזי.

מאחר שמערכות מידע רבות ביותר מתחברות לרשת האינטרנט, כולל בארגונים קטנים, חלה תקנה זו על מכלול מעבדי המידע, משום שבעידן הנוכחי חובה עליהם להגן על המידע המצוי ברשתותיהם מפני האיומים הכרוכים בחיבור לרשת האינטרנט.

תקנת משנה (ג)

העברת מידע באמצעות רשת האינטרנט עלולה להיות חשופה להתחקות ומעקב על ידי גורם זר המעוניין בהעתקת המידע ובשימוש בו. מידע הנשלח באמצעות רשת האינטרנט, עובר בדרכו, עד הגיעו ליעדו, תחנות רבות, אשר איננו מסוגלים להבטיח את רמת האבטחה בהן. לכן, התקנה מחייבת להצפין את המידע הנשלח באמצעות האינטרנט או רשת ציבורית אחרת.

תקנת משנה (ד)

מטרת תקנת משנה ד' לוודא כי הסיכונים שנוצרים בעת אפשרות של גישה מרחוק של עובדי הארגון, ספקיו ולקוחות, למערכות הארגון, ימצאו פתרון, ולא תהיה פגיעה ברמת האבטחה הכוללת בשל כך. לצורך כך נדרש הארגון לשמור על מנגונים שיבטיחו כי רק מורשים יגשו למידע.

תקנת משנה (ה)

מאחר שאיומי אבטחה נוצרים באופן שוטף, ומתגלות חולשות ופגימויות חדשות מעת לעת, יש צורך בניטור ועדכון שוטף של מערכות ההגנה.

תקנה 14 - מיקור חוץ

כללי

מטרת התקנה להבהיר את חובות בעל המאגר בעת ביצוע פעולות במיקור חוץ, באמצעות מחזיק. מאחר שפעולת מיקור חוץ יוצרת סיכונים מיוחדים משל עצמה, על בעל המאגר להתמודד עם סיכונים אלה בעת ביצוע פעולת מיקור חוץ. בהתאם לכך, על בעל המאגר להגדיר את דרישות האבטחה בעת פעולת מיקור החוץ, כחלק בלתי נפרד מהגדרת שירות מיקור החוץ עצמו. על פי ההסדר המוצע, מעטפת אבטחת המידע של בעל המאגר תוחל גם על המחזיק, תוך יישום ושימוש בכלים משפטים מתאימים למימושה. על המחזיק תחול חובה לעמוד במסגרת זו.

בהקשר זה, הדעת נותנת כי קבלת שירות של מיקור חוץ מוסדרת בחוזה המסדיר את ההיבטים העסקים והמסחריים של השירות – מטרת התקנה להבהיר כי במסגרת זו יש להתמודד עם הסיכונים לאבטחת המידע הקשורים במיקור החוץ, ולהסדירם בהסכם, כמפורט להלן:

תקנת משנה (א)

ראשית, מחויב בעל המאגר לבחון מראש את התועלת בהתקשרות עם הגורם החיצוני, מול הסיכונים של אבטחת המידע הכרוכים בהתקשרות זו. תוך שימת הדגש הראוי על זהות הגורם המועמד להתקשרות, והערכת מידת אמינותו.

אם התקבלה ההחלטה כי יש הצדקה להתקשרות זו, יש להתייחס במפורש בהסכם ההתקשרות בין הצדדים, לסוגיית אבטחת המידע. ההתייחסות תכלול את סוג המידע אליו רשאי הגורם החיצוני לגשת, ובאמצעות אילו מערכות; סוג העיבוד אותו הגורם החיצוני רשאי לבצע, ציון מפורש של משך תקופת ההתקשרות, חובות אבטחת המידע של הגורם החיצוני, והתחייבות עובדיו לעמוד בהן. כמו כן, במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה יכלול ההסכם גם הסכמה בדבר סמכותו של בעל המאגר לפקח על פעילותו של הגורם החיצוני, על מנת לבחון שהוא אכן מקיים את דרישות האבטחה שנקבעו בהסכם.

לאחר עריכת ההסכם בין הצדדים, מחייבת התקנה את עדכון נוהל האבטחה של בעל המאגר, תוך ציון ההרשאות שניתנו לגורם החיצוני, והפניה למסמך שנחתם בין הצדדים. עדכון זה מעלה את מודעות אחראי האבטחה ושאר העובדים של בעל המאגר, למגבלות המוטלות על הגורם החיצוני, ובאופן זה, מאפשר פיקוח יעיל יותר על ביצוע פעילותו בתחום המוגדר לו, כפי שמחייבת התקנה.

תקנת משנה (ב)

התקנה מבהירה כי הוראות התקנות חלות על הגורם החיצוני עצמו, וכי הוא חייב לערוך נוהל אבטחה משלו, תוך מגבלותיו בגישה ובעיבוד של נתוני המאגר של מזמין השירות.
מטרת התקנה היא, להבהיר את תחולת הסטנדרטים האמורים בתקנות, ומוחלים כבר על הארגון מזמין השירות (בעל המאגר), גם על הגורם החיצוני, נותן השירות. זאת, על מנת לשמור על רמת אבטחה מהימנה, ולמנוע זליגת המידע או חדירה אליו, דרך מערכות הגורם החיצוני.

תקנה 15 – מחיקת מידע מהמאגר

תקנת משנה (א)

בתקנה זו מוצע לחייב מחיקת מידע שכבר אין בו צורך לפי מטרות המאגר. מחיקה זו מסייעת מראש להקטנת הסיכון שבשימוש לרעה במידע, הן על ידי משתמש פנימי והן על ידי משתמש חיצוני. ככל שקיים צורך לגיטימי בשימור המידע לצרכי ארכיון, יש לשמרו בנפרד על מנת למזער את סיכוני האבטחה הנשקפים מגישה לא מורשית אליו.

תקנת משנה (ב)

התקנה קובעת שיש למחוק את המידע מאמצעי אחסון המיועד למחיקה, או להשמיד את אמצעי האחסון עצמו, באופן שלא יאפשר אחזור של המידע בעתיד.

מחיקה "רגילה" של מידע מחשב, לרוב אינה מחיקה אמיתית של המידע מאמצעי האחסון, אלא היא רק סימון של אותו מקום שהתפנה בעקבות ה"מחיקה" – כמקום הפנוי לשימוש. על ידי שימוש בתוכנות ייעודית, ניתן לאתר את המקום שבו אוחסן המידע מראש (שעתה מסומן כ"פנוי"), ולקרוא ממנו את המידע, כל עוד לא נכתב על גבי אותו מקום מידע חדש. מחיקה רגילה כזו, אינה מספיקה לעניין עמידה בהוראות התקנה. כאן יש דרישה למחיקה אקטיבית, שאינה מסתפקת בסימון המקום כמחוק, אלא בכתיבה של מידע אקראי לאותו מקום בנוסף לכך, באופן שלא יתאפשר שיחזור של המידע המקורי שנשמר שם. קיימות תוכנות רבות המאפשרות מחיקה כזו (wipe), ויש להשתמש בהן.

תקנה 16 – ביקורות תקופתיות

תקנת משנה (א)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תחול חובת עריכת ביקורת, פעם בשנתיים, שבמסגרתה ייבחנו מדיניות האבטחה במאגר, קיומם של אמצעי אבטחה ומימושם – תוך בחינה האם מאגר המידע עומד בתנאי התקנות. הביקורת יכולה להיות פנימית – באמצעות עובדי הארגון, או חיצונית – באמצעות גורם חיצוני.

תקנת משנה (ב)

אם הביקורת היא ביקורת פנימית, חשוב לוודא כי עורך הביקורת אינו ממונה האבטחה בארגון, כדי לוודא כי הארגון מבצע בקרה בלתי תלויה. באופן כזה יוכל גם הארגון להציג תוצרים אלה, במידת הצורך, לבעלי מניותיו, לקוחותיו, בתי משפט והרשם.

תקנת משנה (ג)

דוח הביקורת יכלול את מסקנותיו לגבי יעילות אמצעי האבטחה והתאמתם לתקנות, וכן את מסקנותיו לגבי ליקויי אבטחה, אם נמצאו, והצעות לפתרונם. כמקובל, על דוח כאמור להסתמך על ממצאים ישירים ממערכות המידע.

תקנת משנה (ד)

התקנה קובעת, כי דוחות הביקורת יועברו למנהל המאגר, לאחראי האבטחה, ויידונו על ידי בעל המאגר. מטרת התקנה, לחייב את התייחסות הגורמים המחליטים לדו"ח שהופק. התקנה אף מחייבת את בעל המאגר לבחון את הצורך בעדכון הגדרות המאגר או נוהל האבטחה, בעקבות ממצאי הדו"ח.

תקנה 17 – גיבוי שחזור והתאוששות

מערכות מחשב, עלולות לקרוס באופן פתאומי בעטיים של גורמים שונים: התיישנות המערכת, תקלה טכנית, התקפה יזומה על ידי גורם זר, וירוס אלים ועוד. במקרה של אבדן המידע השמור במערכת, שחזור המידע כרוך בהשקעת משאבים רבים, ולעיתים אף אינו אפשרי. כמו כן, גם אם השחזור אפשרי, המערכת מושבתת עד לשחזור המידע מההתקנים שניזוקו.

לפיכך מוצע בתקנה זו כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה תהיה חובה לקבוע מדיניות של שמירת גיבויים למידע השמור במערכת, וקביעת נהלי התאוששות מתאימים במקרה של קריסת מאגר המידע, או מחיקתו.

תקנה זו מחייבת את אחראי האבטחה לקבוע נהלי גיבוי לביצוע גיבויים מדי שבוע ("גיבוי" משמעותו: יצירת עותק נוסף של המידע המגובה, עדכני לאותו זמן שבו נוצר הגיבוי). אם נמחק המאגר או שהמערכת קורסת, ניתן לגשת לאותו גיבוי, ולהפיק ("לשחזר") ממנו את המידע האבוד. כמו כן, על אחראי האבטחה לקבוע נהלים לשחזור המערכת במקרה של אבדן המידע.

ביצוע נהלי השחזור מצריך אישור מראש של אחראי האבטחה, והליך השחזור יתועד ברישום אירועי האבטחה לפי תקנה 11.

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, חלה דרישה נוספת שלפיה עותק גיבוי של המידע ושל נהלי השחזור יישמר במיקום פיזי אחר מאשר מיקום המאגר עצמו. מטרת הוראה זו היא למנוע מצב של הרס נרחב אשר יפגע במאגר המידע ובגיבויים השמורים באותו מקום, כך שלא תהיה אפשרות שחזור. התקנה משאירה פתח ליישום פתרונות טכנולוגיים אחרים, במקום האחסון הפיזי המרוחק, ובלבד שהם יאפשרו את אותה רמת ביטחון בשחזור המידע במקרה הרס או אבדן.

תקנה 18 – סמכויות הרשם

תקנת משנה (א)

התקנות מציגות מסגרת בסיסית המכילה את העקרונות לאבטחת המידע במאגרי מידע. הרשם רשאי לפרט את העקרונות שהוצגו בתקנות, ולהתוות באופן מעשי את דרך המימוש המתאימה לעקרונות הללו, בהתאם לנסיבות המשתנות, להתפתחויות הטכנולוגיות ולתקני אבטחת המידע המשתנים. הרשם רשאי לתת הנחיות לגבי כלל מאגרי המידע, לגבי חלק מהם או לגבי מאגרים מסוימים, לפי הצורך.

תקנת משנה (ב)

לעתים ישנם מאגרי מידע שבשל גודלם, היקף פעילותם, מספר העובדים המועסקים בהם או בשל סוג המידע הכלול בהם, יש מקום להקל את דרישות אבטחת המידע המוטלות עליהם לפי התקנות המוצעות. לפיכך מוצע לתת לרשם סמכות לפטור סוגי מאגרי מידע או מאגרים מסוימים מחובות אבטחת המידע לפי התקנות, על בסיס אמות המידה האמורות.

תקנת משנה (ג)

ישנם תקני אבטחת מידע שונים, בין שהם תקנים ישראליים ובין שהם תקנים זרים או הוראות

של רשויות מוסמכות בתחום זה, אשר עמידה בתנאיהם מהווה החלה של רמת אבטחת מידע ראויה, שיש בה כדי להתמודד באופן ראוי עם הסיכונים הקשורים בתחום זה, אף אם אינם תואמים במדויק את הוראות תקנות אלה. לפיכך מוצע לתת לרשם סמכות להורות שעמידה בהוראות תקן מקובל או בהנחיות של רשות מוסמכת בעניין אבטחת מידע, תפטור מתחולת התקנות כולן או חלקן.

תקנה 19 – תחולה

כאמור לעיל במבוא לטיוטת התקנות, בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה, ככל שמאגר המידע הוא מאגר שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותיות יותר. לפיכך רמות האבטחה לפי התקנות המוצעות מחולקות לשלוש קבוצות שונות של מאגרי מידע כאמור לעיל בדברי ההסבר לתקנה 1. תפיסה זו, של חובות מודולריות נגזרת כאמור ישירות מעקרון היסוד של אבטחת מידע, שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטויה גם במסמכים דומים בעולם.

תקנה 20 – פטור מתחולה

מוצע כי מאגר מידע אשר רק לאדם אחד יש גישה אליו והוא בעל המאגר, אזי יהיה בעל המאגר פטור מהוראות התקנות, בשל הסיכון הנמוך יותר הנובע מכך שאין צורך לנהל ולפקח אחר המורשים למאגר. זאת למעט מספר הוראות בסיסיות של אבטחת מידע שיש להחיל על כל מאגר מידע שהוא, והן:

- אחריות כללית לאבטחת המידע במאגר מידע ולנקיטת אמצעים סבירים להפחית את סיכוני אבטחת המידע, ובין היתר, לבחון האם המידע הנאסף והנשמר במאגר אינו מעבר לנדרש לצורך מימוש מטרות המאגר.
- עריכת רשימת מצאי של רכיבי המערכת.
- **א**בטחה פיזית וסביבתית בסיסית (נעילת דלתות וכד').
- קיום מנגנון זיהוי ואימות בכניסה למאגר (שם משתמש וסיסמה, וכד').
- יישום אמצעי הגנה סבירים בעת העברת התקנים ניידים.
- אבטחת תקשורת, אינטרנט, דוא"ל וכו' (התקנת FIREWALL, אנטי-וירוס ועדכונים שוטפים וכיו"ב).
- מחיקת מידע מיותר, וכן שלאחר המחיקה לא ניתן יהיה לשחזרו מהמאגר או מאמצעי האחסון.

יג. נספח ג' – הצעת פרופ' עדי שמיר להגנת המידע במאגר הביומטרי

31 international conference of data protection and privacy commissioners

Adding Privacy To Biometric Databases:

The Setbase Approach

Adi Shamir
Computer Science Dept
The Weizmann Institute
Israel

1

Adding Privacy To Biometric Databases: Using Random Graphs to Identify People

- Many governments (including in Israel) plan to issue new ID cards in the near future
- They are facing strong public opposition mainly due to privacy concerns
- The five possible solutions:

No universal ID card	Printed/ laminated ID card	Smart ID card, no biometrics	Biometric ID card, no DB	Biometric ID card + database

2

The Planned Transition in Israel

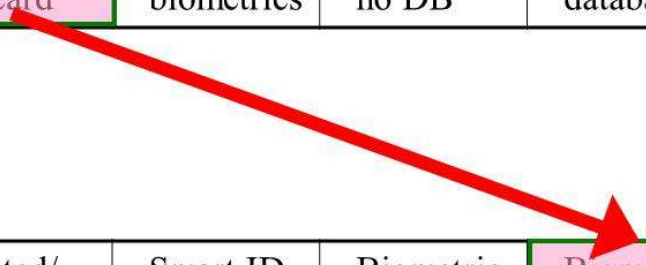
No universal ID card	Printed/ laminated ID card	Smart ID card, no biometrics	Biometric ID card, no DB	Biometric ID card + database

No universal ID card	Printed/ laminated ID card	Smart ID card, no biometrics	Biometric ID card, no DB	Biometric ID card + database

3

The Planned Transition in Israel

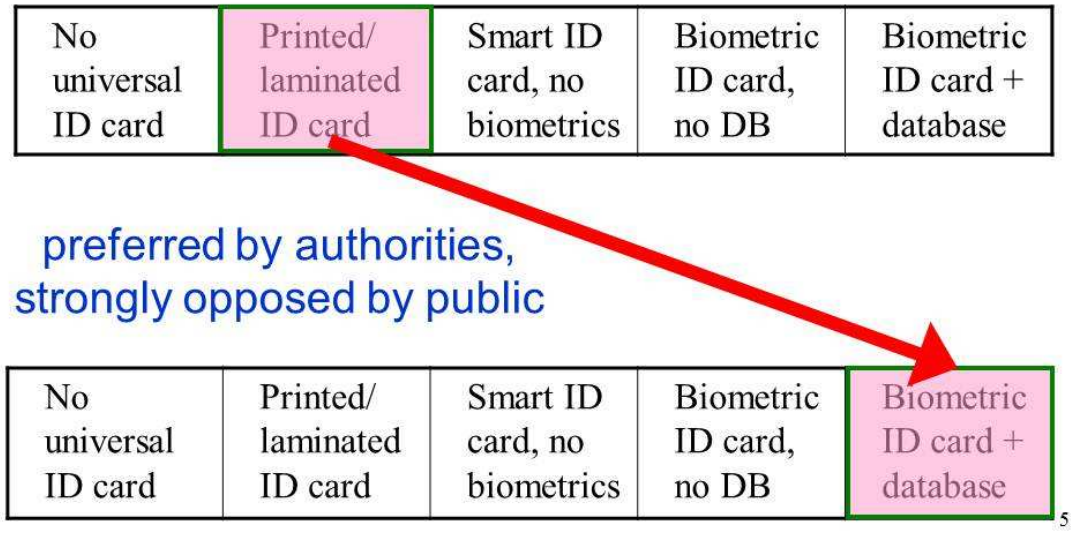
No universal ID card	Printed/ laminated ID card	Smart ID card, no biometrics	Biometric ID card, no DB	Biometric ID card + database



No universal ID card	Printed/ laminated ID card	Smart ID card, no biometrics	Biometric ID card, no DB	Biometric ID card + database

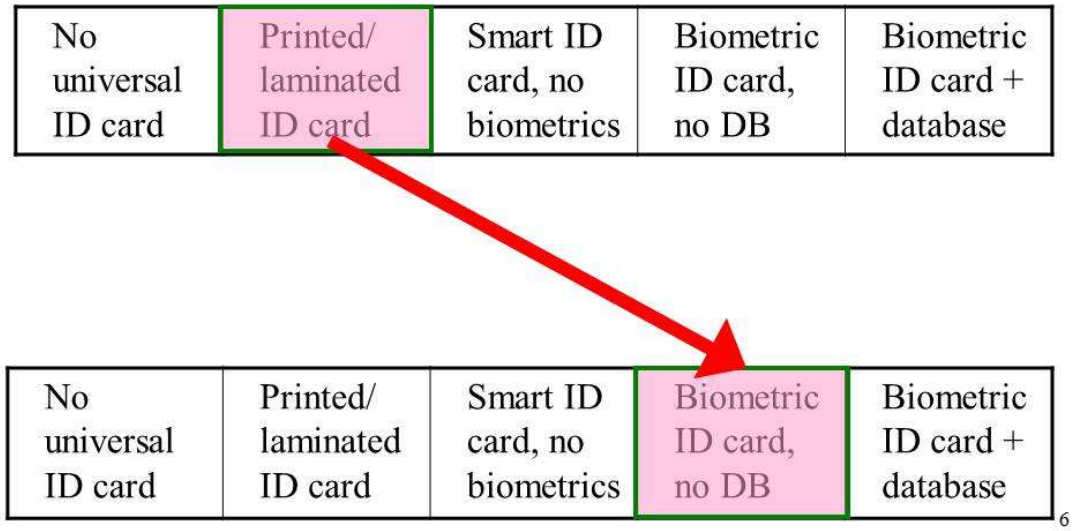
4

The Planned Transition in Israel



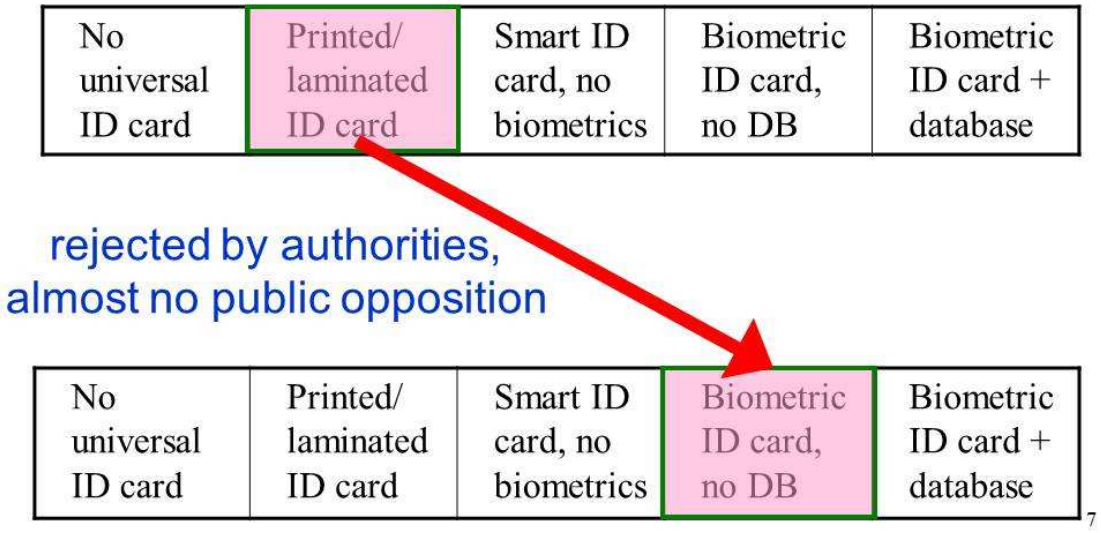
5

The Planned Transition in Israel



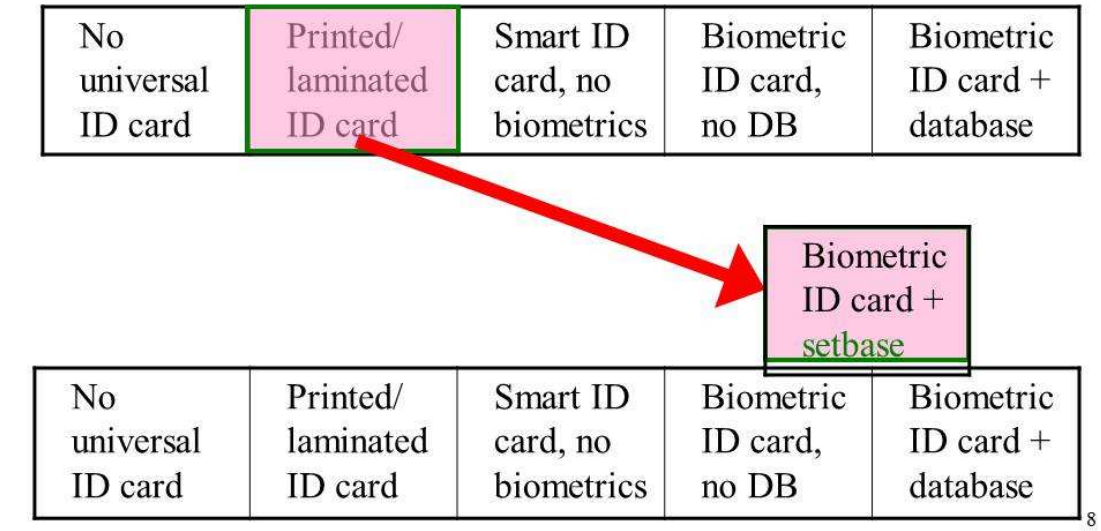
6

The Planned Transition in Israel



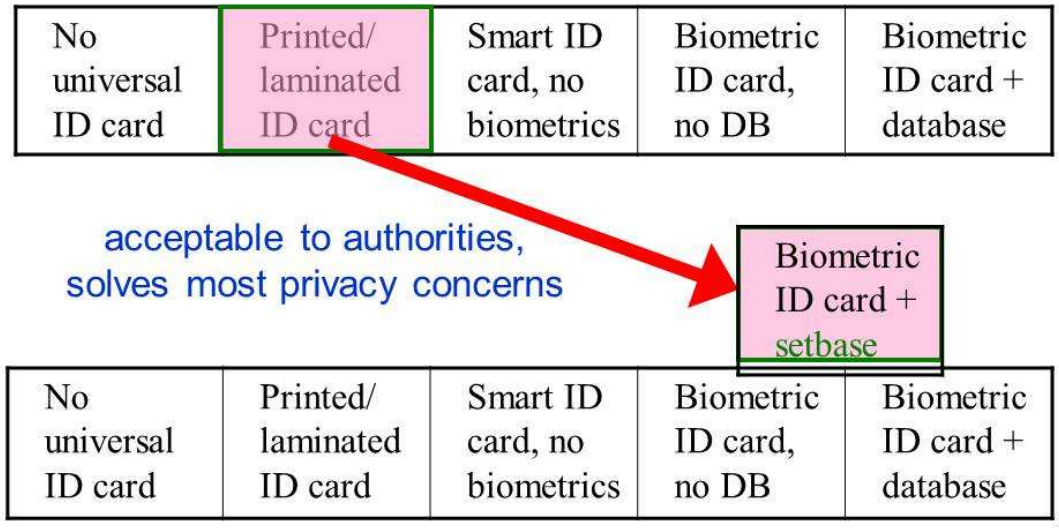
7

My Proposal: A Biometric Setbase



8

My Proposal: A Biometric Setbase



9

The Official Reasons for Creating a Biometric Database in Israel:

- Major reason: Preventing double issuing of official ID cards to criminals and crooks
- Minor reason: Identifying paperless bodies and solving major crimes – in very rare cases

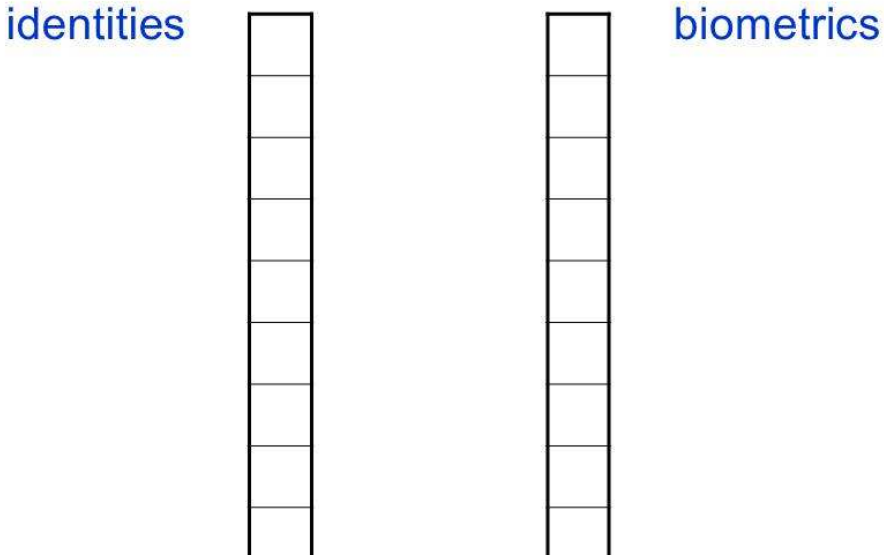
10

The Main Counterarguments of Privacy Advocates:

- Irreversibility: After the biometrics are collected for one purpose, there will be mission creep
- Mistrust of government: Legal protections are insufficient to prevent possible future misuse
- Insufficiency of Cryptographic Protection: Future governments can force the disclosure of keys
- Potential dangers: identifying troublemakers, entrapping innocents, leakage to outside entities

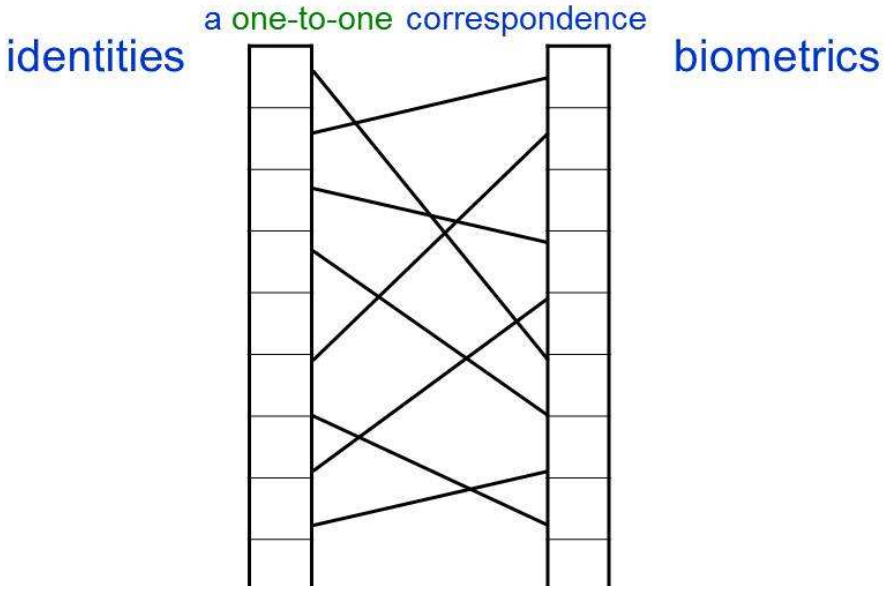
11

A Standard Biometric Database:



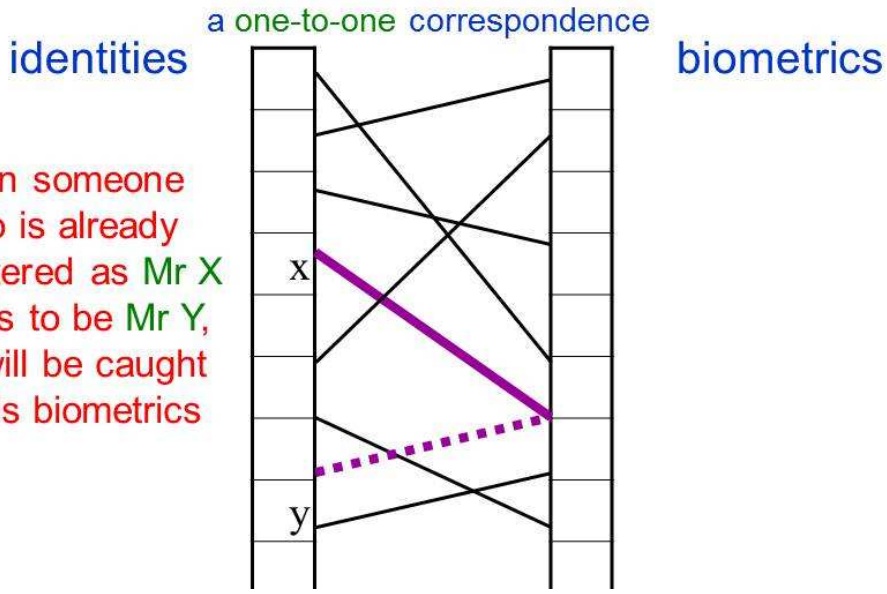
12

A Standard Biometric Database:



13

A Standard Biometric Database:



14

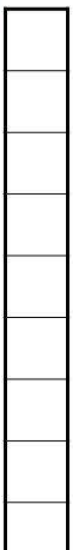
The Main Observation Behind Setbases:

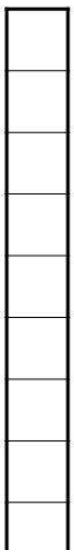
- The database should have:
  - insufficient information to identify a person via his biometrics as Mr X
  - sufficient information to disprove a wrong claim that he is Mr Y
- This separation should remain true even if:
  - the law changes after the database is set up
  - everyone colludes with the government

15

Using Setbases Instead of Databases:

file cabinet with all the N identities

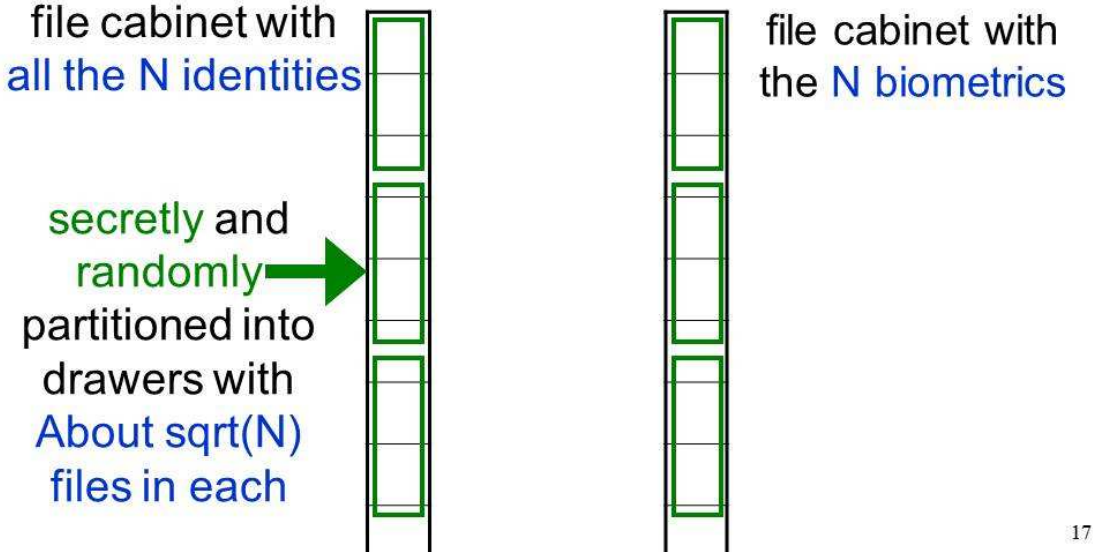




file cabinet with all the N biometrics

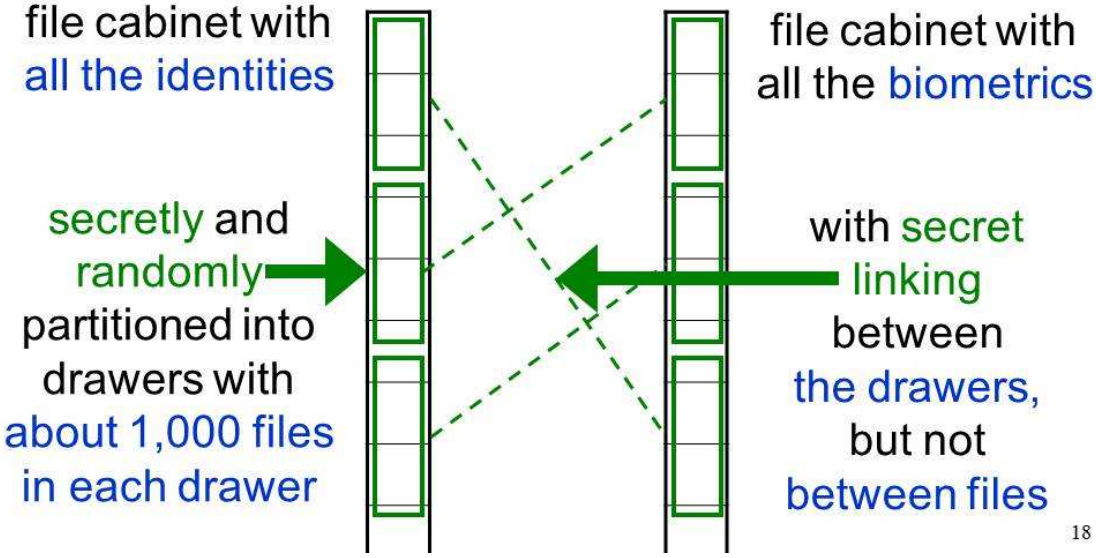
16

Using Setbases Instead of Databases:



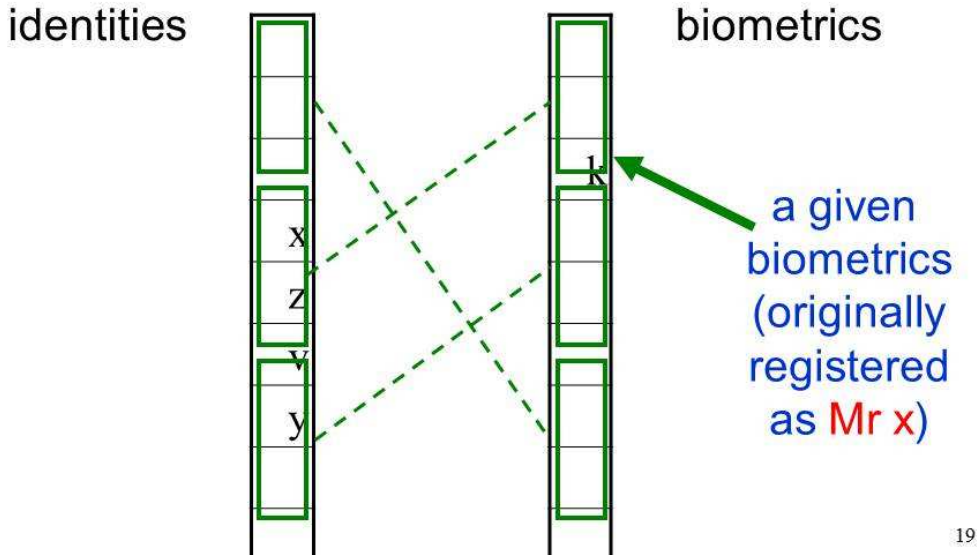
17

Using Setbases Instead of Databases:



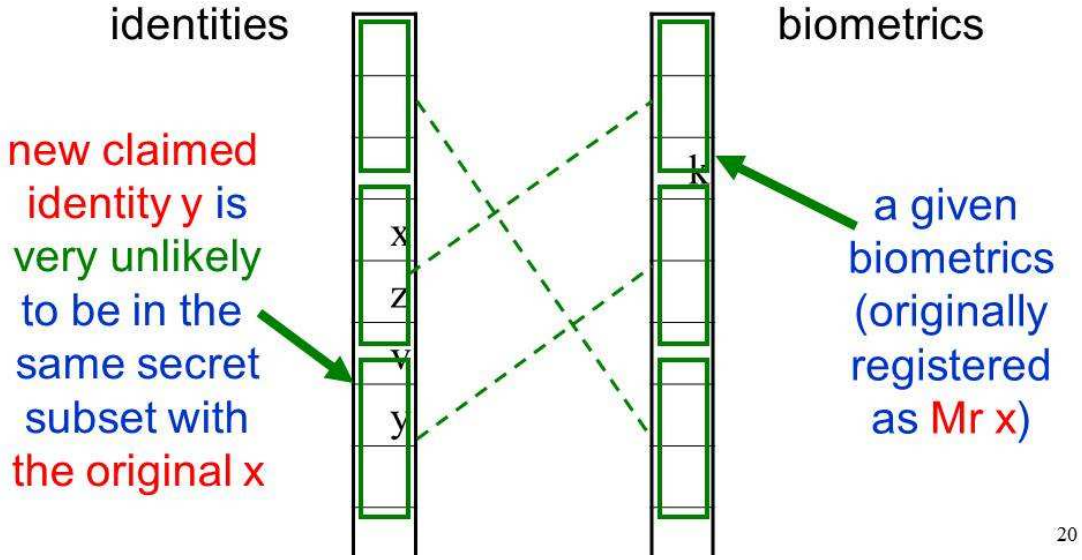
18

Using Setbases Instead of Databases: How to catch cheaters



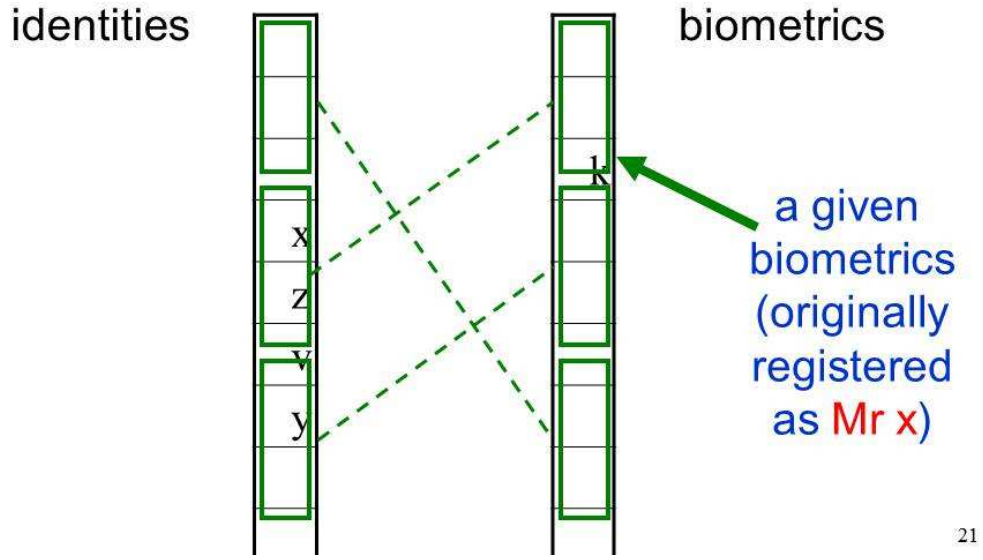
19

Using Setbases Instead of Databases: How to catch cheaters



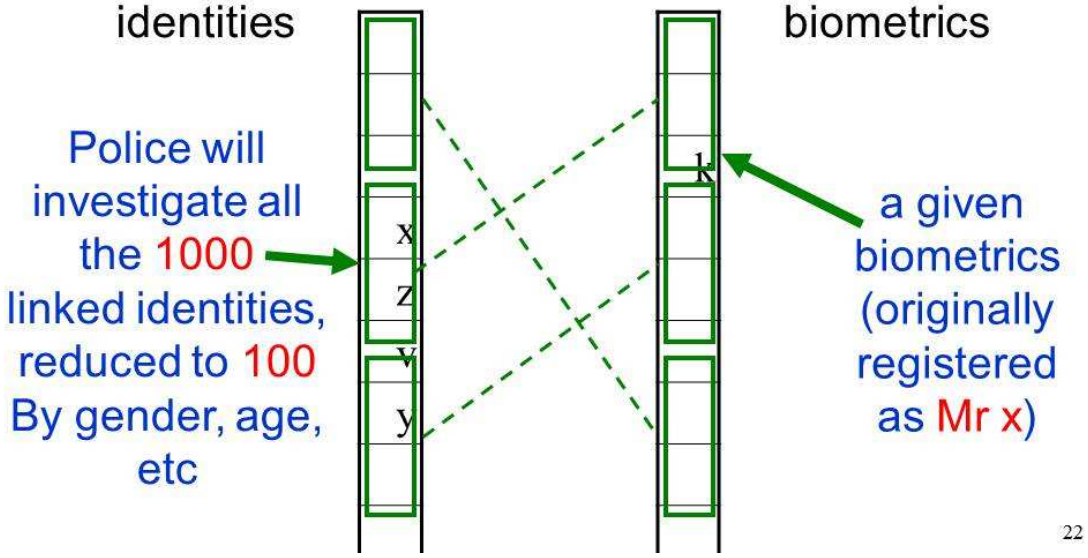
20

Using Setbases Instead of Databases: How to Identify Paperless Bodies



21

Using Setbases Instead of Databases: How to Identify Paperless Bodies

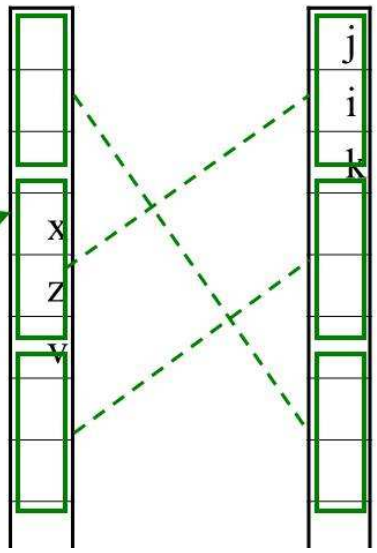


22

Using Setbases Instead of Databases: Even Fully Leaked Data Cannot Entrap

identities

someone with full access to the data wants to entrap x by planting his fingerprints in a crime scene



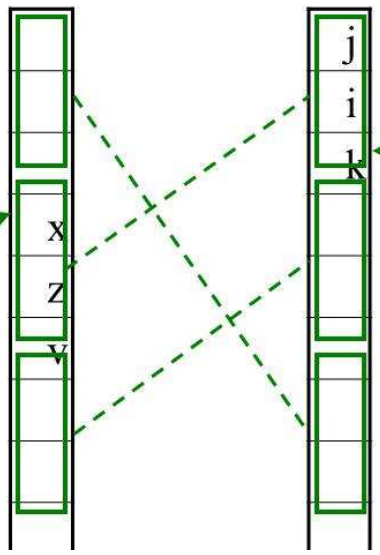
biometrics

23

Using Setbases Instead of Databases: Even Fully Leaked Data Cannot Entrap

identities

someone with full access to the data wants to entrap x by planting his fingerprints in a crime scene

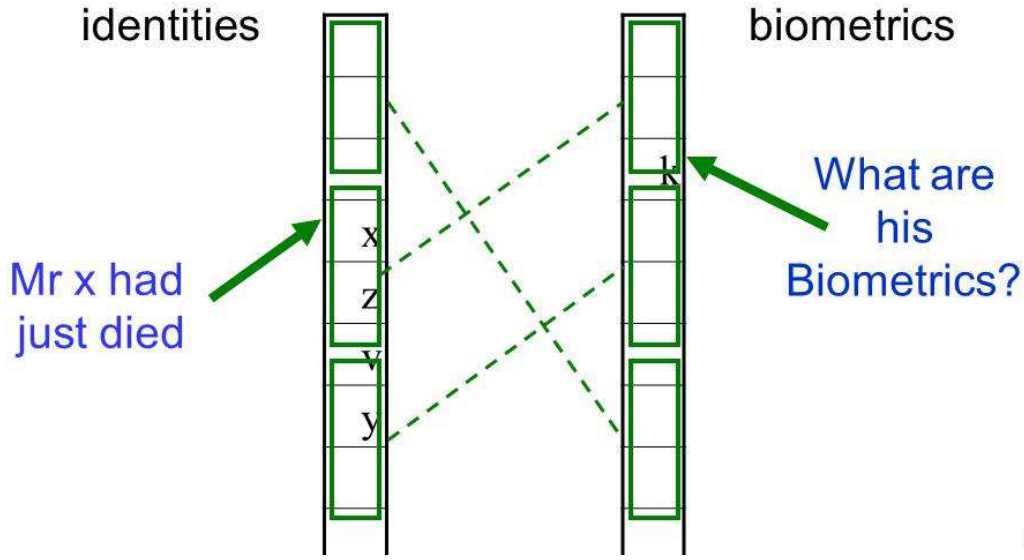


biometrics

planting one fingerprint has probability of 1/1000 to succeed; planting multiple fingerprints will raise alarm

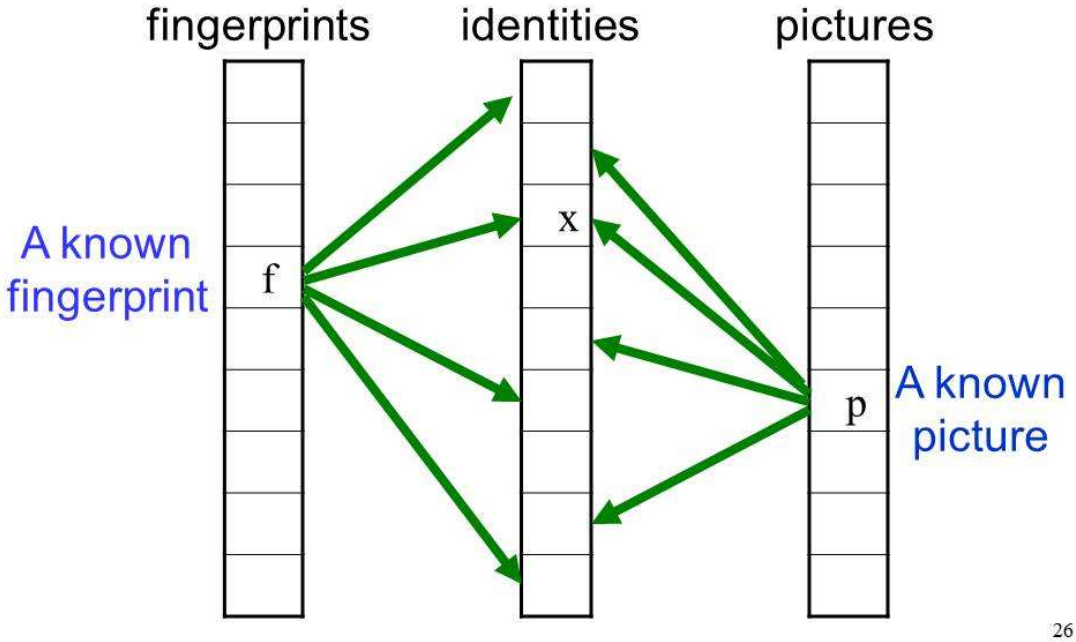
24

Real life Problems Are More Complicated: Can We Eliminate People who Die or Emigrate?



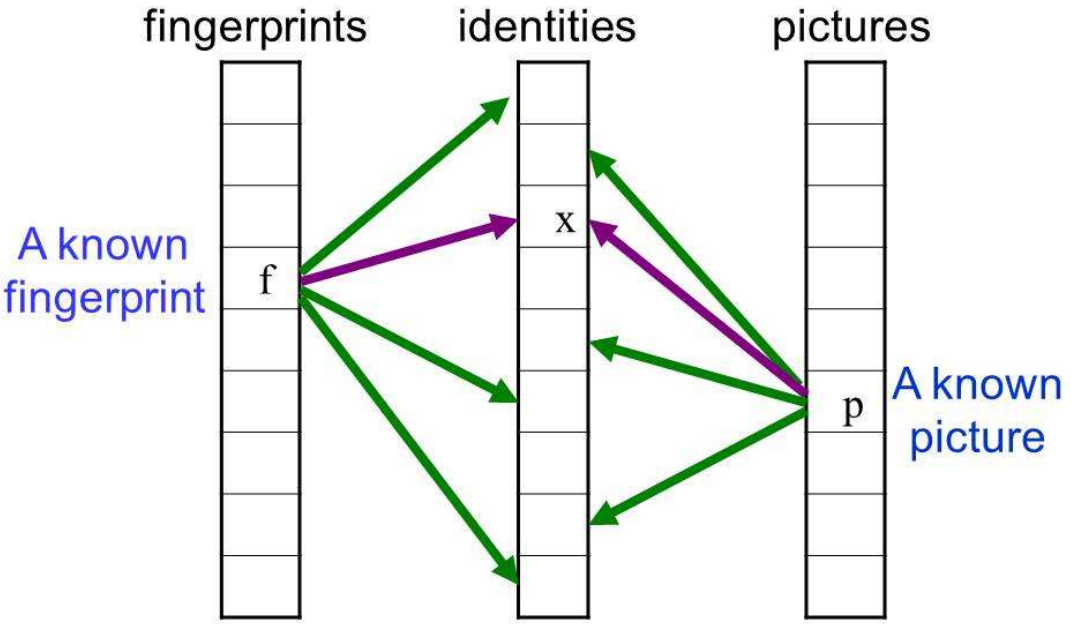
25

Real life Problems Are More Complicated: How to Deal With Multiple Biometrics?



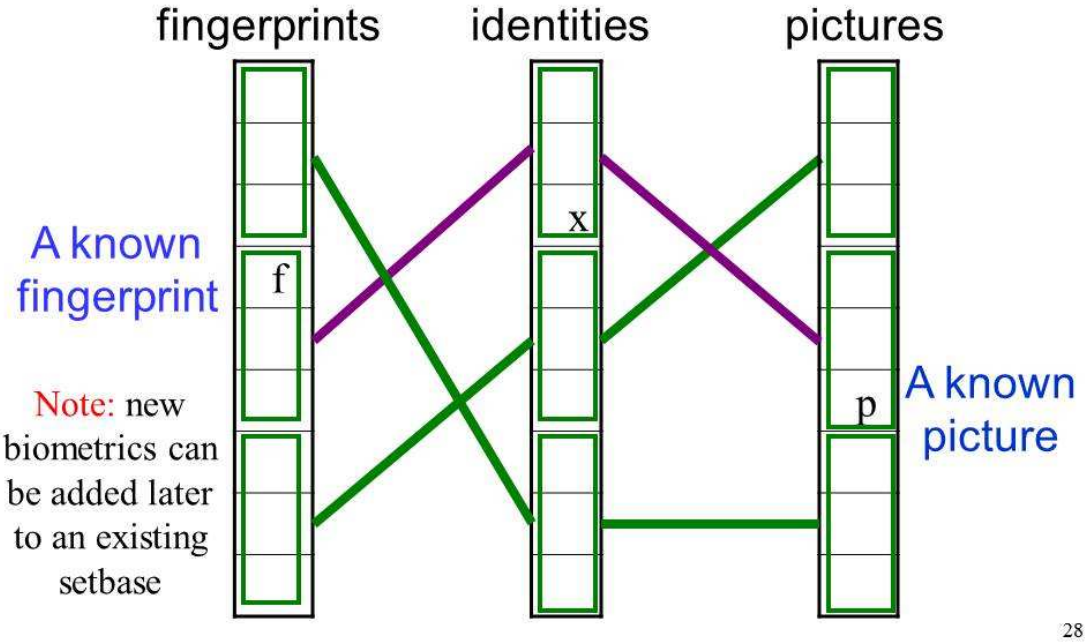
26

Real life Problems Are More Complicated: Multiple Biometrics Can Identify a Person



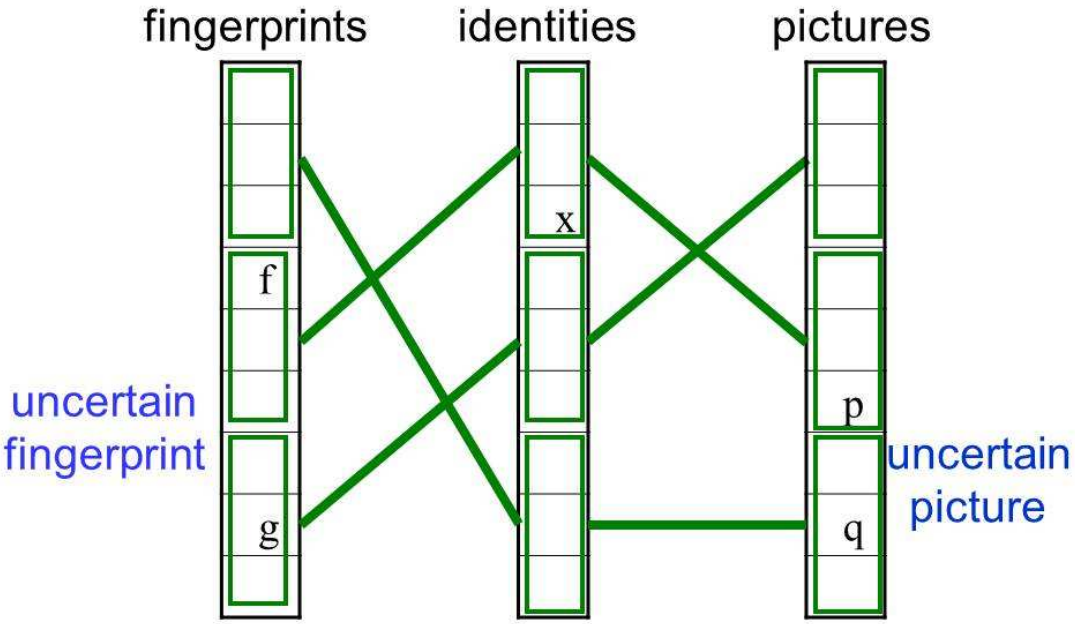
27

Real life Problems Are More Complicated: Correct Implementation of Hypergraph Setbases



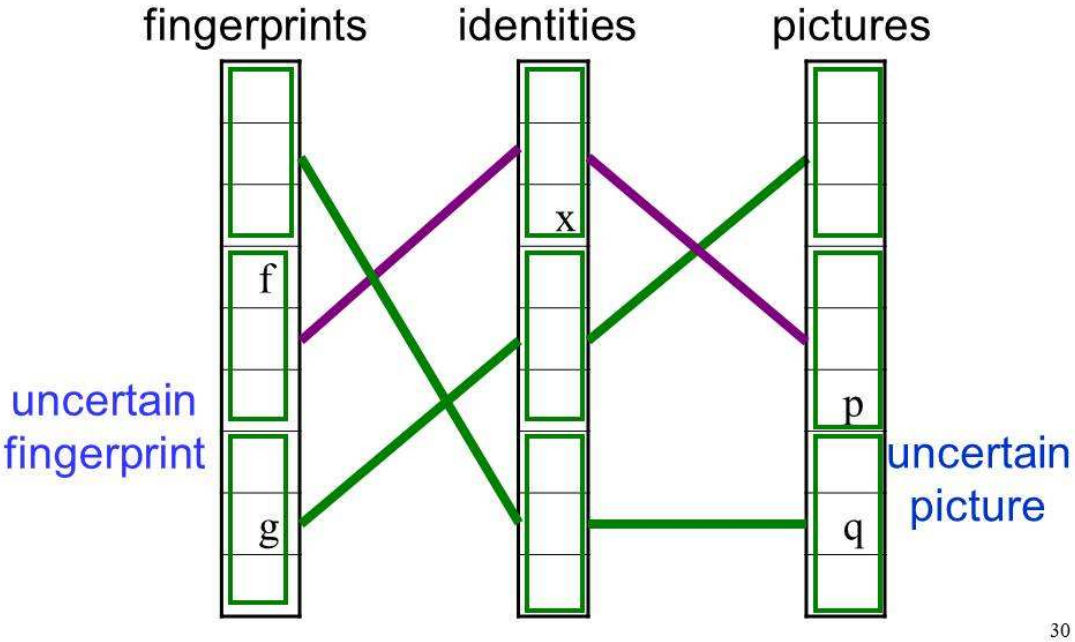
28

Real life Problems Are More Complicated: The Advantages of Hypergraph Setbases



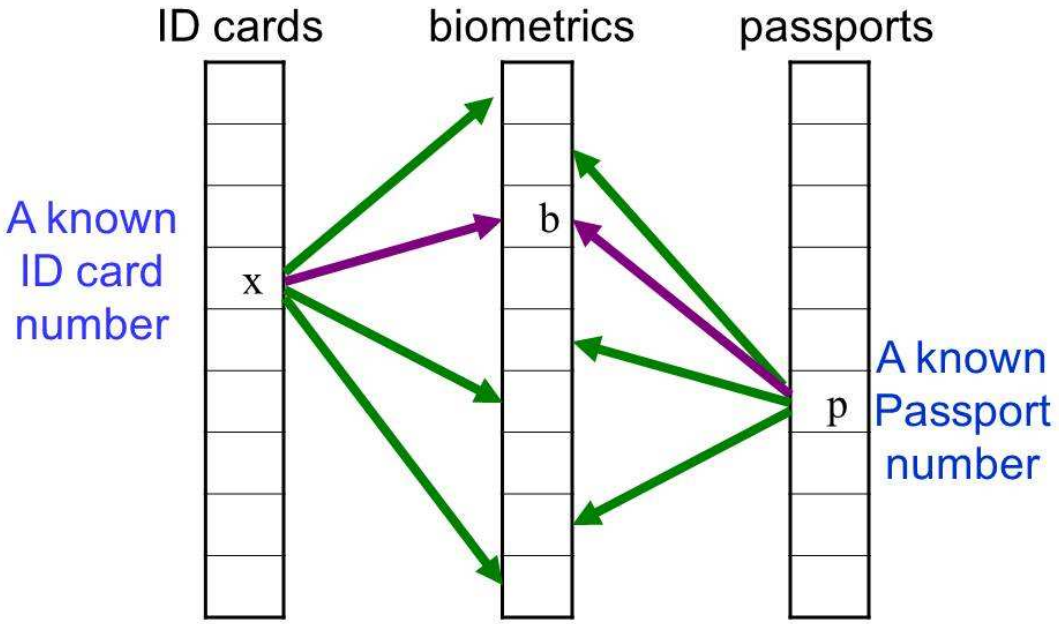
29

Real life Problems Are More Complicated: The Advantages of Hypergraph Setbases



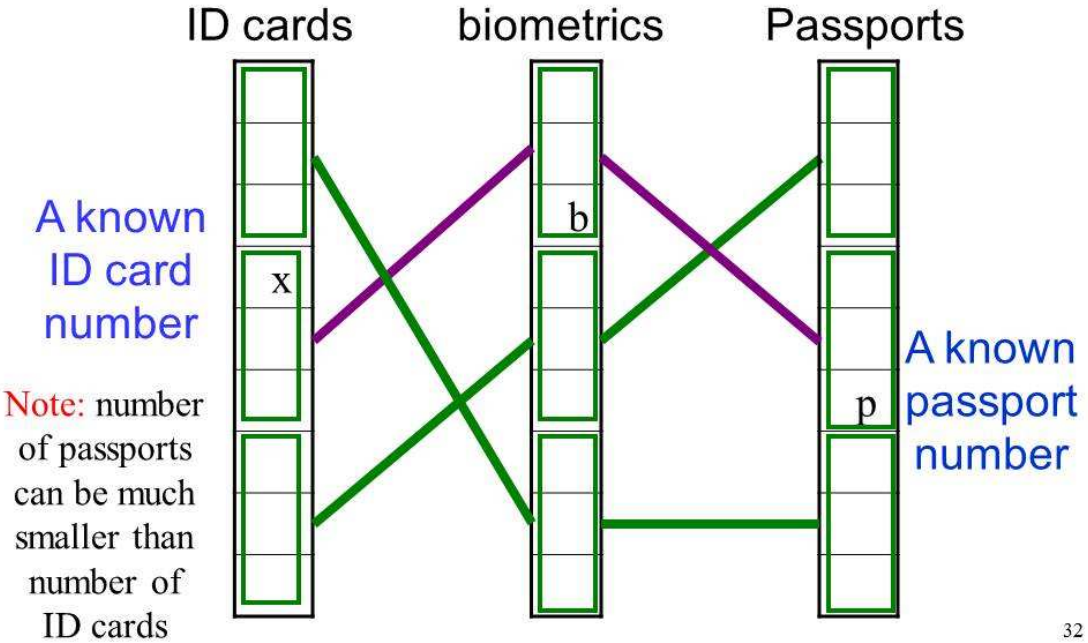
30

Real life Problems Are More Complicated: The Dual Problem of Multiple Card Types



31

Real life Problems Are More Complicated: The Dual Problem of Multiple Card Types



32

Summary of Setbases:

- Like any other privacy enhancing technique, setbases are a compromise between the conflicting demands for privacy and functionality
- Double issuing can be prevented at almost no additional cost and with very high probability
- Individuals can be identified from their biometrics, but only by a long, expensive and highly visible police investigation, and can't be easily entrapped
- This privacy protection cannot be eliminated by changing the law or expropriating the crypto keys

33

יד. נספח ד' – סקרים אודות תפיסת הפרטיות בציבור הישראלי ובמגזר העסקי בישראל



מטרות ושיטה

מטרות	בחינת רמת המודעות הקיימת בארץ לסוגיית ה"פרטיות" ובחינת הבנת המשמעות של חוק הגנת הפרטיות בארץ
מי	529 גברים ונשים בגילאי 18 ומעלה, מתוכם: 450 יהודים ו-79 ערבים ישראלים במדגם ארצי, אקראי, ומייצג של אוכלוסיה זו.
מתי	במהלך חודש ספטמבר 2009
כיצד	סקר יעודי טלפוני באמצעות מערכת סקרים ממוחשבת CATI הראיונות נערכו בעברית ובערבית.
ניתוח	הניתוח נערך בקרב כלל המדגם וכן על פי חיתוכים סוציו-דמוגרפים.

2



<u>תפיסות ביחס למידע אישי והגנה על הפרטיות:</u>

- בישראל, קיימת תפיסה שהמידע האישי אינו מוגן כראוי, וחמור יותר שמערכת החקיקה אינה מסוגת להתמודד עם הסוגייה:
  - 70% מהציבור סבורים כי המידע האישי אינו מוגן כראוי, ועוד 5% ציינו לא יודע.
  - במקביל, החקיקה בישראל נתפסת בשיעור נמוך (34%) כמסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים בעוד ש- 58% מהציבור סבורים שהיא אינה מסוגלת.

<u>מידת הבטחון של הציבור בנושא מידע אישי בידי ארגונים וחברות</u>

- הציבור מוטרד במידה רבה מנושא ההגנה על המידע האישי:
  - כמחצית מהציבור מדווחים כי הם מוטרדים מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי לגבי אנשים.
  - מבין הגופים שנבחנו עד כמה הציבור בוטח בהם שישתמשו במידע אודותיו רק למטרות למענן הוא נמצא אצלן. לגבי רוב הגופים, כמחצית מהציבור אינו בוטח בהם בנושא, כשחוסר הבטחון העיקרי הוא לגבי חברות סקרים (62%) ועמותות וארגונים שלא למטרות רווח (57%). הבטחון הגדול ביותר הוא ברופאים ונותני שירותים רפואיים.
  - 50% מהציבור מדווחים, שכאשר הם מוסרים פרטים לגוף כלשהו הם **תמיד** שואלים לשם מה הם נדרשים. 27% נוספים **בדרך כלל** שואלים.

מודעות לחוק הגנת הפרטיות וזכויותיו

- רוב הציבור (79%) סבור שמודעות הציבור לתחום ההגנה על מידע אישי נמוכה. בפועל, המודעות סבירה, למעט המודעות לרשם מאגרי המידע שהיא אכן נמוכה:
  - 64% מהציבור מאשרים כי ידוע להם שמי שאוסף עליהם מידע צריך לזהות עצמו, ולהציג את מטרת השימוש במידע, כדי שיוכל לשמור אותו במאגר מידע.
  - 81% מהציבור סבורים כי נדרשת הסכמתם לשם שימוש במידע אודותיהם.
  - 76% מהציבור סבורים כי החוק בישראל מאפשר להם לתבוע בהליך משפטי פיצויים בשל הפרת חוק הגנת הפרטיות.
  - 44% מהציבור סבורים כי ישנה הוראה חוקית המאפשרת להם לעיין במידע אודותיהם שנמצא בידי אחר.

יחידת רשם מאגרי המידע

- מעמד יחידת רשם מאגרי מידע בתודעת הציבור נמוך:
  - < רק 25% מהציבור מודע ליחידת רשם מאגרי המידע
  - < 15% מהציבור (כ- 60% מהמודעים ליחידה) סבורים שהיחידה מוסמכת לברר ולטפל בתלונות של אנשים בנושא זה.
  - < רק 4% מהציבור (כ-15% מהמודעים ליחידה) יצרו בעבר קשר עם הרשם או הרשות, כשאין נושא בולט לגביו יצרו קשר.

ShiluvMillwardBrown

הגנה על מידע אישי ושימוש באינטרנט:

- העברת מידע באמצעות האינטרנט אינה נתפסת כבטוחה. למרות זאת, שיעור בלתי מבוטל משתמשים באינטרנט לצרכים אלו:
  - 69% מהציבור מודאגים מהשארת מידע אישי באינטרנט
  - רק 22% מהציבור סבורים כי העברת מידע על ידם באמצעות האינטרנט בטוחה יחסית, 70% אינם סבורים כך.
  - עם זאת, רק 8% מהציבור בודקים **תמיד** מהי מדיניות שמירת הפרטיות של האתר אליו גלשו ו-18% מהציבור (19% מגולשי האינטרנט) בודקים **בדרך כלל**. כחמישית מהציבור בודקים **לעיתים רחוקות** ו-42% מהציבור (44% מגולשי האינטרנט) **כלל לא** בודקים.
  - 57% מהציבור (60% מגולשי האינטרנט) שמעו על כלים או טכנולוגיות המגבילים או מונעים איסוף מידע מהמחשב האישי ע"י גורמים זרים.
  - רק ל-35% מהציבור (כ-60% מהמודעים לכלים) יצא להשתמש בכלים אלו.
  - עיקר החסמים לשימוש בכלים אלו הם חסמים טכניים – חוסר מודעות לאופן התקנתם וחוסר מודעות לאופן השימוש בהם.

ShiluvMillwardBrown



הצגה גראפית של ממצאים ומסקנות

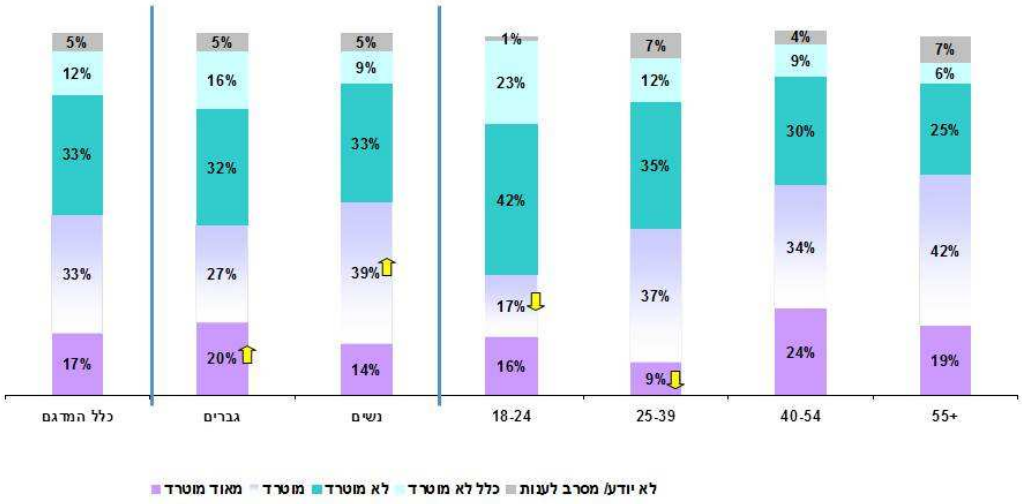
ShiluvMillwardBrown



תפיסות ביחס למתן מידע אישי והגנת הפרטיות

ShiluvMillwardBrown

המידה בה מוטרד הציבור מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי - בדיקה נעזרת



- כמחצית מהציבור מוטרד מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי לגבי אנשים.
- נשים מוטרדות יותר מגברים, ככל שעולה הגיל מוטרד הציבור יותר.

Q1. [Q1] מידע פרטי על אנשים נשמר בידי גופים ציבוריים ופרטיים. האם אתה מוטרד מהאופן בו מֻגָנים ארגונים אלה על המידע אודותיך ⇧⇩ **הבדל מובהק**

9

ShiluvMillwardBrown

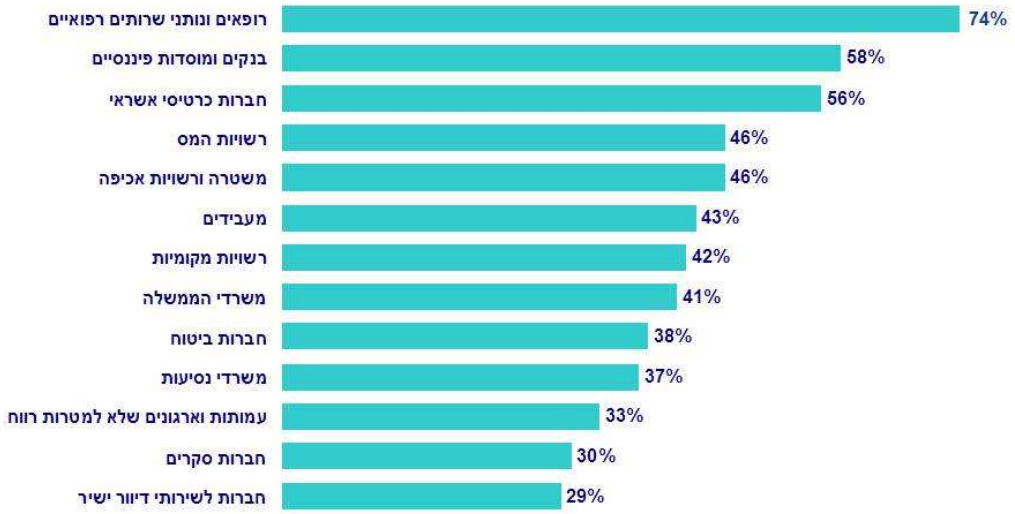


עד כמה הציבור בוטח בארגונים וחברות בנושא מידע אישי

ShiluvMillwardBrown

תפיסת הבטחון בהגנת מידע פרטי בגופים ציבוריים ופרטיים - נעזר

% מצייני בוטח בקרב כלל המדגם



- הבטחון הגדול ביותר הוא ברופאים ונותני שירותים רפואיים.
- חוסר הבטחון העיקרי הוא בחברות לדיוור ישיר, חברות סקרים ועמותות וארגונים שלא למטרות רווח.
- הציבור לא בוטח ברשויות ממשלתיות כגון: מס, משטרה, רשויות מקומיות ומשרדי ממשלה.

11 Q2-Q14 [Q2]. האם אתה בוטח ב... שיעשו שימוש במידע אודותיך אך ורק למטרות למענן הוא נמצא אצלן?

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת ניתוח סוציו דמוגרפי

	רופאים ונותני שירותים רפואיים		בנקים ומוסדות פיננסיים		חברות כרטיסי אשראי	
	בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
% מהמדגם	74	23	58	39	56	39
מין						
גברים	73	24	57	42	60	36
נשים	74	23	58	37	52	42
גיל						
18-24	76	22	66	34	57	41
25-39	78	19	57	39	56	39
40-54	73	24	57	42	61	35
55+	66	30	51	41	48	42
השכלה						
יסודי או תיכון ללא בגרות	71	26	54	42	49	38
תיכון עם בגרות	78	21	69	30	68	29
על תיכוני או אקדמאי	74	23	54	42	54	43
סרב לענות	56	33	61	39	56	39
אזור מגורים						
ירושלים	69	25	52	40	58	32
מרכז	65	31	52	43	52	44
צפון	79	19	60	39	58	36
דרום	81	17	68	31	60	37
שרון	75	24	55	45	47	47
משלח יד						
עצמאי	71	27	51	47	56	40
שכיר	74	23	59	40	58	39
ללא מקצוע	75	22	59	35	52	38

- בקרב מי שאינו בוטח ברופאים ונותני שירותים רפואיים ייצוג גבוה לגילאי +55 ולתושבי אזור המרכז.
- ככל שיורד הגיל עולה הביטחון בבנקים ובמוסדות פיננסיים. כמו כן בטחון רב יותר בקרב בעלי השכלה תיכונית עם בגרות ובקרב תושבי הדרום.
- גברים בוטחים יותר מנשים בנושא שמירה על מידע אישי בחברות כרטיסי האשראי. בקרב הבוטחים ייצוג גבוה לקבוצת הגיל 40-54 ולבעלי השכלה תיכונית עם בגרות.

הבדל מובהק

12

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת ניתוח סוציו דמוגרפי

		רשויות המס		משטרה ורשויות אכיפה		מעבידים	
		בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
	% מהמדגם	46	50	46	48	43	45
	מין						
	גברים	46	52	47	49	41	50
	נשים	45	47	45	46	45	40
	גיל						
	18-24	44	55	50	46	47	44
	25-39	51	42	47	46	49	42
	40-54	42	53	47	47	42	48
	+55	43	50	39	52	32	46
	השכלה						
	יסודי או תיכון ללא בגרות	37	55	48	44	52	38
	תיכון עם בגרות	46	52	45	50	45	45
	על תיכוני או אקדמאי	48	47	46	48	40	47
	סרב לענות	39	50	33	44	39	44
	אזור מגורים						
	ירושלים	40	51	46	43	43	37
	מרכז	48	49	44	54	38	48
	צפון	45	50	48	47	44	49
	דרום	46	48	46	44	52	35
	שרון	45	51	45	45	39	49
	משלח יד						
	עצמאי	44	53	40	53	38	44
	שכיר	46	51	47	49	45	46
	ללא מקצוע	46	46	47	43	42	44

- בקרב בעלי השכלה על תיכונית או אקדמאית גבוה יותר הבטחון ברשויות המס.
- ככל שיורד הגיל עולה הביטחון במשטרה וברשויות האכיפה.
- ייצוג גבוה לבוטחים במעבידים בקרב הגילאים 18-39. ככל שעולה ההשכלה יורד הבטחון במעביד. כמו כן, בקרב הבוטחים במעבידים, ייצוג גבוה לתושבי הדרום.

הבדל מובהק

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת ניתוח סוציו דמוגרפי

		רשויות מקומיות		משרדי הממשלה		חברות ביטוח	
		בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
	% מהמדגם	42	51	41	53	38	54
	מין						
	גברים	36	59	39	56	38	59
	נשים	48	43	43	49	38	50
	גיל						
	18-24	47	50	46	50	51	43
	25-39	45	44	49	44	40	54
	40-54	38	56	34	62	30	63
	+55	37	54	34	56	32	55
	השכלה						
	יסודי או תיכון ללא בגרות	47	43	41	52	43	45
	תיכון עם בגרות	52	43	41	55	52	43
	על תיכוני או אקדמאי	36	56	42	52	31	63
	סרב לענות	39	50	22	61	39	39
	אזור מגורים						
	ירושלים	42	40	32	55	38	42
	מרכז	45	52	34	60	38	54
	צפון	45	51	50	47	38	57
	דרום	40	48	46	48	44	51
	שרון	27	63	33	57	27	71
	משלח יד						
	עצמאי	40	52	37	62	33	63
	שכיר	42	51	41	53	38	57
	ללא מקצוע	44	49	43	48	40	45

- נשים בוטחות יותר ברשויות המקומיות וגם בעלי השכלה תיכונית מלאה ומטה.
- בקרב קבוצות הגיל 18-39, בעלי השכלה על תיכונית או אקדמאית ובקרב תושבי הצפון והדרום. הבטחון במשרדי הממשלה גבוה יותר .
- בקרב הגילאים 18-39, בעלי השכלה תיכונית מלאה ומטה ותושבי הדרום ייצוג גבוה יותר לבוטחים בחברות הביטוח.

הבדל מובהק

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת
ניתוח סוציו דמוגרפי

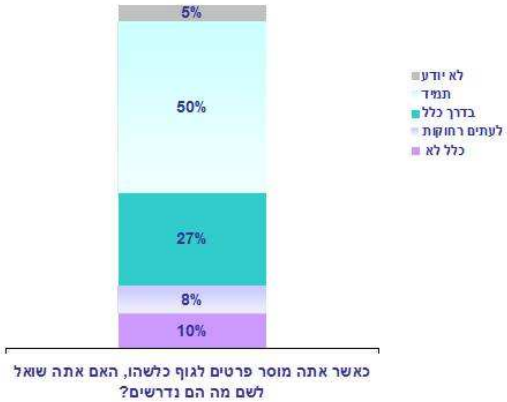
	משרדי נסיעות		עמותות וארגונים		חברות סקרים		חברות לשירותי דיוור ישיר	
	בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
% מהמדגם	37	53	33	57	30	62	29	56
מין								
גברים	33	61	35	58	33	61	30	56
נשים	41	45	30	57	27	63	29	56
גיל								
18-24	47	47	49	47	40	56	41	49
25-39	38	54	33	56	34	59	31	54
40-54	34	54	24	65	25	65	24	59
55+	29	57	26	61	21	69	22	61
השכלה								
יסודי או תיכון ללא בגרות	38	47	34	52	38	47	38	46
תיכון עם בגרות	47	45	42	52	33	62	38	50
על תיכוני או אקדמאי	33	59	30	61	27	68	24	61
סרב לענות	39	44	17	67	22	50	22	56
אזור מגורים								
ירושלים	43	34	40	51	34	58	35	40
מרכז	31	58	30	61	30	62	23	62
צפון	40	54	35	54	35	63	39	51
דרום	45	49	37	52	32	56	23	59
שרון	24	67	20	76	24	73	18	69
משלח יד								
עצמאי	33	60	32	60	23	74	30	66
שכיר	34	56	29	61	31	62	27	58
ללא מקצוע	44	45	39	50	32	58	33	47

- בקרב נשים וכל שיורד הגיל הבטחון במשרדי נסיעות גבוה יותר. כמו גם, בקרב בעלי השכלה תיכונית, תושבי האזורים ירושלים, צפון ודרום ובקרב לא מקצועיים.
- בקרב גילאי 18-39, בעלי השכלה תיכונית מלאה, תושבי האזורים: ירושלים, צפון ודרום ובקרב לא מקצועיים הבטחון בעמותות וארגונים גבוה יותר .
- הבטחון בחברות סקרים יורד עם הגיל ועם ההשכלה.
- הבטחון בחברות לשירותי דיוור ישיר יורד עם הגיל. כמו כן, הוא נמוך יותר בקרב בעלי השכלה על תיכונית ואקדמאית. הבטחון בחברות אלו גבוה יותר בקרב תושבי ירושלים והצפון.

הבדל מובהק

ShiluvMillwardBrown

מתן פרטים אישיים והגנת הפרטיות - נעזר
כלל המדגם



- מרבית הציבור מדווח כי אינו נותן פרטים אישיים מבלי לברר את הסיבה: 50% ישאלו תמיד לשם מה הם נדרשים בעוד ש-27% נוספים ישאלו בדרך כלל.
- בקרב המשיבים תמיד ייצוג גבוה לגילאי 40 ומעלה וייצוג נמוך לתושבי אזור ירושלים.

Q32. כאשר אתה מוסר פרטים לגוף כלשהו, האם אתה שואל לשם מה הם נדרשים?



הגנה על הפרטיות בישראל

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת

כלל המדגם



- הציבור מוטרד בנושא ההגנה על המידע האישי והמודעות לתחום: כשלושה רבעים מהציבור חושבים שהמידע האישי אינו מוגן כראוי.
- כשני שליש מהציבור חושבים שהחקיקה בישראל אינה מסוגלת להתמודד עם התגברות העברת המידע האישי.

Q15-18. [Q3] אקריא בפניך דעות שציינו אנשים שונים, עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים

18

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת ניתוח סוציו דמוגרפי

	בישראל המידע האישי מוגן כראוי		מודעות הציבור לתחום ההגנה על מידע אישי נמוכה	
	מסכים	לא מסכים	מסכים	לא מסכים
% מהמדגם	24	70	79	17
מין				
גברים	27	68	80	15
נשים	22	72	77	18
גיל				
18-24	37	62	77	21
25-39	25	67	74	20
40-54	19	74	87	9
55+	17	78	77	17
השכלה				
יסודי או תיכון ללא בגרות	35	60	73	21
תיכון עם בגרות	31	67	77	18
על תיכוני או אקדמאי	19	74	82	14
סרב לענות	11	78	61	28
אזור מגורים				
ירושלים	20	72	72	18
מרכז	23	74	79	18
צפון	30	65	82	13
דרום	22	69	74	20
שרון	20	75	80	14
משלח יד				
עצמאי	16	78	86	8
שכיר	22	74	80	17
ללא מקצוע	32	60	73	19

- ההסכמה לתפיסה לפיה המידע האישי בישראל מוגן כראוי יורדת עם העליה בגיל וככל שעולה רמת ההשכלה.
- בקרב הגילאים 40-54 בולטת יותר הסכמה לתפיסה לפיה מודעות הציבור לתחום ההגנה על מידע אישי נמוכה. עצמאיים ושכירים מסכימים יותר לתפיסה זאת מול חסרי מקצוע.

הבדל מובהק

19

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת ניתוח סוציו דמוגרפי

	אני מודאג מהשארת מידע אישי כגון שם, כתובת, תאריך לידה וכו' באינטרנט		החקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים	
	מסכים	לא מסכים	מסכים	לא מסכים
% מהמדגם	69	28	34	58
מין				
גברים	66	32	35	59
נשים	72	25	33	57
גיל				
18-24	65	35	46	48
25-39	68	30	32	59
40-54	75	23	30	61
55+	68	25	30	63
השכלה				
יסודי או תיכון ללא בגרות	63	34	42	53
תיכון עם בגרות	69	28	38	56
על תיכוני או אקדמאי	71	27	31	61
סרב לענות	72	22	22	61
אזור מגורים				
ירושלים	72	23	35	49
מרכז	68	30	25	72
צפון	64	33	43	49
דרום	74	24	35	54
שרון	75	22	29	69
משלח יד				
עצמאי	73	26	23	66
שכיר	73	26	36	59
ללא מקצוע	62	33	36	52

- בקרב נשים בולטת דאגה רבה יותר מהשארת מידע אישי באינטרנט. כך גם בקרב קבוצת הגיל 40-54 ובקרב שכירים.
- ככל שיורד הגיל עולה ההסכמה עם התפיסה לפיה החקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים.
- ההסכמה לתפיסה יורדת ככל שעולה רמת ההשכלה ובקרב עצמאים.

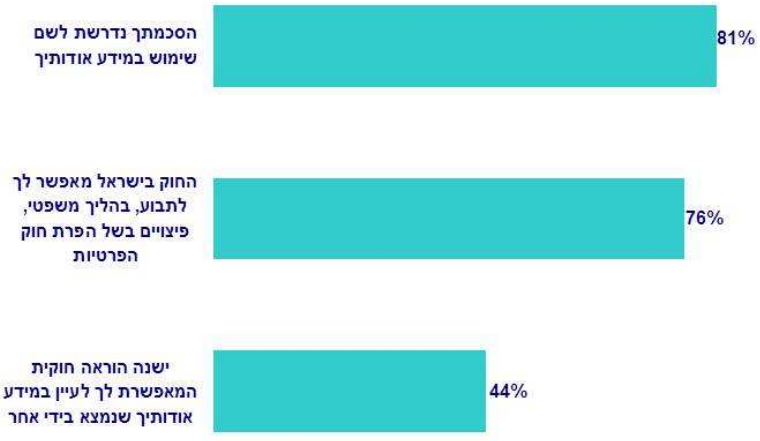
הבדל מובהק

20



תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת

% מצייני נכון בקרב כלל המדגם



- נושא מתן הסכמה לשימוש במידע אישי ואפשרות תביעת פיצויים בשל הפרת חוק הפרטיות ידועים אצל מרבית הציבור, יחד עם זאת, פחות ממחצית מהציבור מודעים להוראה החוקית המאפשרת עיון במידע אישי הנמצא בידי אחר.

Q24-26. [Q6] אקריא לך מספר משפטים הקשורים להגנת מידע אישי, לגבי כל אחד מהם אנא ציין האם למיטב ידיעתך הוא נכון או לא נכון

22

ShiluvMillwardBrown

תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת ניתוח סוציו-דמוגרפי

	הסכמתך נדרשת לשם שימוש במידע אודותיך		ישנה הוראה חוקית המאפשרת לך לעיין במידע אודותיך שנמצא בידי אחר		החוק בישראל מאפשר לך לתבוע, בהליך משפטי, פיצויים בשל הפרת חוק הפרטיות	
	נכון	לא נכון	נכון	לא נכון	נכון	לא נכון
% מהמדגם	81	14	44	33	76	11
מין						
גברים	78	17	38	38	73	16
נשים	84	12	50	28	78	7
גיל						
18-24	84	11	47	39	78	14
25-39	81	14	49	31	83	9
40-54	78	18	37	35	73	8
55+	81	13	43	28	67	16
השכלה						
יסודי או תיכון ללא בגרות	75	16	43	42	71	15
תיכון עם בגרות	83	11	49	34	76	15
על תיכוני או אקדמאי	83	14	43	30	77	8
סרב לענות	67	17	39	33	78	11
אזור מגורים						
ירושלים	85	9	38	32	74	9
מרכז	74	21	48	27	79	11
צפון	81	14	41	39	74	15
דרום	83	12	54	31	78	11
שרון	94	6	39	33	75	2
משלח יד						
עצמאי	85	14	45	33	64	19
שכיר	80	15	44	32	81	7
ללא מקצוע	81	12	44	36	72	15

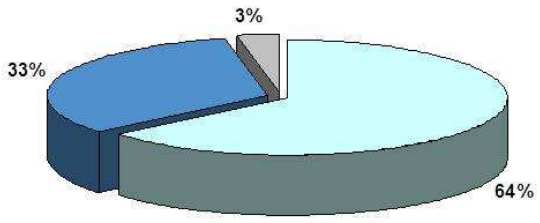
- בקרב נשים שכיחה יותר התפיסה כי נדרשת הסכמה לשימוש במידע אישי. תפיסה זו שכיחה יותר בקרב גילאי 18-24, בעלי השכלה תיכונית מלאה ומעלה ותושבי השרון.
- נשים סבורות יותר כי קיימת הוראה חוקית המאפשרת לעיין במידע אישי הנמצא בידי אחר. התפיסה שכיחה יותר בקרב גילאי 25-39 ובקרב תושבי המרכז והדרום.
- בקרב גילאי 18-39 שכירים נפוצה יותר הסברה לפיה החוק מאפשר לתבוע בהליך משפטי פיצויים בשל הפרת חוק הפרטיות.

הבדל מובהק

ShiluvMillwardBrown

מודעות למשמעות החוק בנושא איסוף מידע – נעזר

כלל המדגם



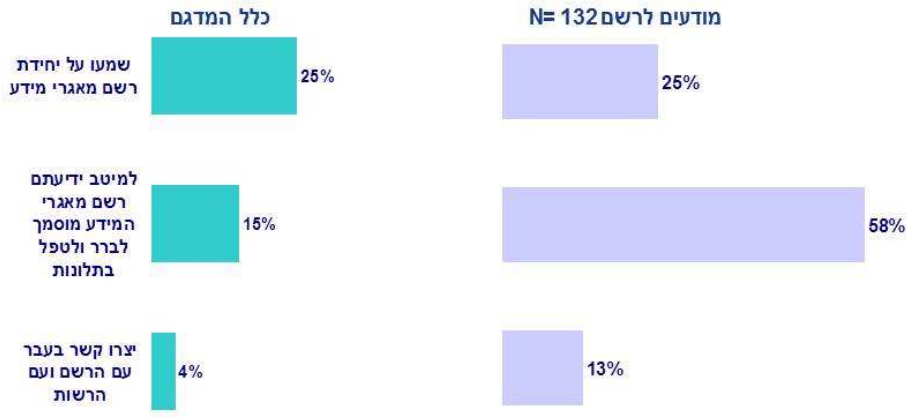
- כשני שליש מהציבור מודעים למתחייב מחוק הגנת הפרטיות בנושא איסוף המידע.
- בקרב מי שאינו מודע ייצוג גבוה לבעלי השכלה יסודית או תיכונית ללא בגרות.

Q23. [Q5] האם ידוע לך כי מי שאוסף עליך מידע צריך לזהות עצמו בפניך ולהציג את מטרת השימוש במידע כדי שיוכל לשמור אותו במאגר מידע?



רשם מאגרי המידע

מודעות לרשם מאגרי המידע, לתחומי טיפולו ויצירת קשר עם הרשם - נעזר



- מודעות נמוכה ליחידת רשם מאגר המידע ותפקידיה. יחד עם זאת מעל מחצית מהמודעים סבורים כי רשם מאגרי המידע מוסמך לברר ולטפל בתלונות וכחמישית מהמודעים יצרו קשר בעבר עם הרשם ועם הרשות.

Q19. האם שמעת כי במשרד המשפטים, ברשות למשפט טכנולוגיה ומידע קיימת יחידת רשם מאגרי המידע שאחראית על אכיפת חוק הגנת הפרטיות בתחום מאגרי המידע?
Q20. האם למיטב ידיעתך רשם מאגרי מידע מוסמך לברר ולטפל בתלונות של אנשים בנושא זה?
Q21.האם יצרת קשר בעבר עם הרשם או הרשות? ואם כן באיזה עניין?

26

ShiluvMillwardBrown

מודעות לרשם מאגרי המידע ולסמכויותיו – בדיקה נעזרת נתונים סוציו דמוגרפיים

	האם שמעת כי במשרד המשפטים קיימת יחידת רשם מאגרי מידע שאחראית על אכיפת החוק בתחום מאגרי מידע		האם למיטב ידיעתך רשם מאגרי מידע מוסמך לברר ולטפל בתלונות של אנשים בנושא זה (בקרב המודעים N=132)	
	כן	לא	כן	לא
% מהמדגם	25	72	58	20
מין				
גברים	30	68	51	24
נשים	20	76	69	15
גיל				
18-24	30	69	66	20
25-39	22	73	61	14
40-54	23	73	66	22
55+	27	71	38	28
השכלה				
יסודי או תיכון ללא בגרות	19	77	61	33
תיכון עם בגרות	26	69	55	23
על תיכוני או אקדמאי	25	72	60	17
סרב לענות	44	50	50	13
אזור מגורים				
ירושלים	17	82	64	27
מרכז	31	68	61	7
צפון	23	71	60	28
דרום	26	70	50	33
שרון	22	75	55	18
משלח יד				
עצמאי	27	70	55	25
שכיר	23	74	60	19
ללא מקצוע	27	68	58	20

- מודעות גבוהה יותר ליחידת רשם מאגרי המידע בקרב גברים ובקרב תושבי המרכז.
- בקרב נשים, מודעות רבה יותר לסמכויותיו של רשם מאגרי המידע. בקרב קבוצת הגיל +55 מודעים פחות לסמכויותיו של הרשם.

הבדל מובהק

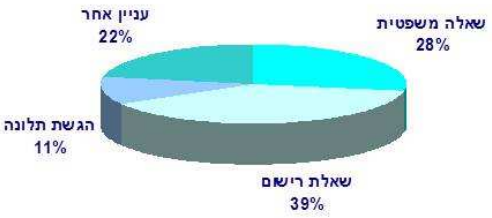
ShiluvMillwardBrown

רשם מאגרי המידע - יצירת קשר ושביעות רצון – נעזר

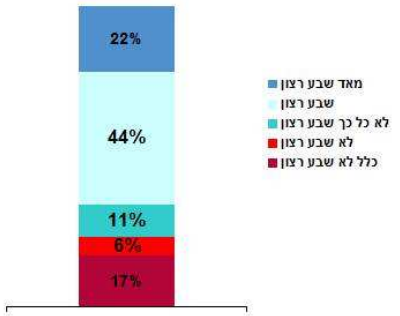
בקרב יוצרי הקשר עם הרשם

***N=18**

נושאים ליצירת הקשר



שביעות רצון מהשירות



האם יצרת קשר בעבר עם הרשם או הרשות? ואם כן באיזה עניין?
עד כמה אתה שבע רצון מהשירות שניתן לך על ידי הרשם / הרשות

- שני שליש מהפונים לרשם הביעו שביעות רצון מהשירות שקיבלו.

Q21 [Q4d] האם יצרת קשר בעבר עם הרשם או הרשות? ואם כן באיזה עניין?
Q22 עד כמה אתה שבע רצון מהשירות שניתן לך על ידי הרשם / הרשות?

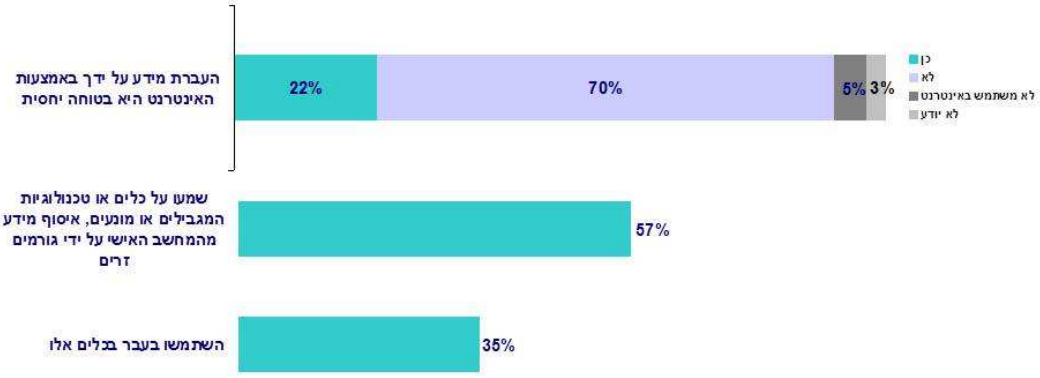
* תא סטטיסטי קטן



הגנה על מידע אישי באינטרנט

תפיסות לגבי שימוש באינטרנט והגנת הפרטיות - נעזר

כלל המדגם



- שימוש באינטרנט להעברת מידע אישי אינו נתפס כבטוח.
- רמת מודעות בינונית לטכנולוגיות המגבילות איסוף מידע מהמחשב האישי, יחד עם זאת, רק כשליש מהציבור השתמשו בהן.

Q27 [Q7a] האם לדעתך העברת מידע על ידך באמצעות האינטרנט היא בטוחה יחסית?
Q28 .[Q7b] האם שמעת על כלים או טכנולוגיות המגבילים או מונעים, איסוף מידע מהמחשב שלך על ידי גורמים זרים לדוגמא: פיירוול או מסנן עוגיות (cookies blocker) ?
Q29 [Q7c] האם יצא לך להשתמש בעבר בכלים אלו?

ShiluvMillwardBrown

תפיסות לגבי שימוש באינטרנט והגנת הפרטיות – בדיקה נעזרת נתונים סוציו דמוגרפיים

	האם לדעתך העברת מידע על ידך באמצעות האינטרנט היא בטוחה יחסית ?		האם שמעת על כלים או טכנולוגיות המגבילים או מונעים, איסוף מידע מהמחשב שלך ע"י גורמים זרים? N=503	
	כן	לא	כן	לא
% מהמדגם	22	70	60	35
מין				
גברים	29	64	66	31
נשים	15	75	55	38
גיל				
18-24	23	72	63	36
25-39	30	62	65	31
40-54	19	75	62	34
55+	13	72	46	40
השכלה				
יסודי או תיכון ללא בגרות	11	74	37	53
תיכון עם בגרות	26	65	51	45
על תיכוני או אקדמאי	25	70	70	25
סרב לענות	17	67	59	35
אזור מגורים				
ירושלים	17	72	52	36
מרכז	30	61	66	31
צפון	19	72	55	38
דרום	23	72	67	30
שרון	14	80	53	39
משלח יד				
עצמאי	22	70	69	31
שכיר	24	71	64	33
ללא מקצוע	19	68	49	39

- העברת מידע באמצעות האינטרנט נתפסת בטוחה יותר בקרב: גברים, גילאי 18-39, בעלי השכלה תיכונית מלאה ומעלה ובקרב תושבי המרכז.
- בקרב גברים, בעלי השכלה תיכונית מלאה ומעלה ותושבי המרכז והדרום שמעו יותר על טכנולוגיות המגבילות או מונעות איסוף מידע מהמחשב האישי.

הבדל מובהק

ShiluvMillwardBrown

הרגלי גלישה באינטרנט והגנת הפרטיות - נעזר

בקרב גולשי האינטרנט
N=503



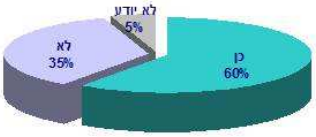
- כשני שליש מהגולשים באינטרנט אינם נוהגים לבדוק את מדיניות שמירת הפרטיות של האתרים אליהם הם גולשים: 44% אינם בודקים כלל ו-21% בודקים לעתים רחוקות. יחד עם זאת, פחות מעשירית מגולשי האינטרנט בודקים תמיד מהי מדיניות שמירת הפרטיות של האתר אליו גלשו. כחמישית בודקים בדרך כלל.
- בקרב הבודקים תמיד ייצוג גבוה לתושבי הצפון. בקרב הבודקים בדרך כלל ייצוג גבוה לבעלי השכלה על תיכונית ואקדמאית, לתושבי הדרום והשרון ולשכירים.

Q31. האם כאשר אתה גולש באינטרנט אתה בודק מהי מדיניות שמירת הפרטיות של האתר/החברה אליה גלשת?

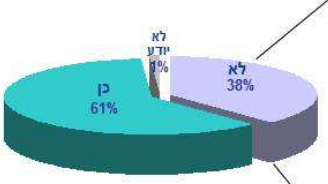
ShiluvMillwardBrown

תפיסות לגבי שימוש באינטרנט והגנת הפרטיות - נעזר

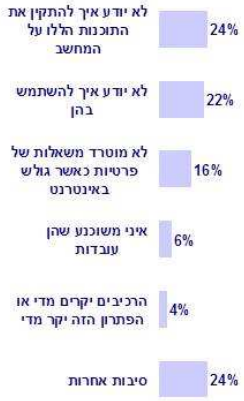
מודעות לטכנולוגיות
בקרב משתמשי האינטרנט
N=503



שימוש בטכנולוגיות
בקרב המודעים לכלים אלו
N=302



סיבות לחוסר שימוש
בקרב מי שלא השתמש בכלים אלו בעבר
N=116



- חסמים טכנולוגיים מהווים סיבה עיקרית לחוסר שימוש באמצעים טכנולוגיים המגבילים את איסוף המידע מהמחשב האישי.

Q28. [Q7b] האם שמעת על כלים או טכנולוגיות המגבילים או מונעים, איסוף מידע מהמחשב שלך על ידי גורמים זרים לדוגמא: פיירוול או מסנן עוגיות (cookies blocker) ?
Q29. [Q7c] האם יצא לך להשתמש בעבר בכלים אלו?
Q30. [Q8] מבין הסיבות הבאות, מהי הסיבה העיקרית לכך שלא השתמשת בכלים או טכנולוגיות המגבילים את איסוף המידע מהמחשב שלך, למרות שידעת על קיומם:

33

ShiluvMillwardBrown



נספח

ShiluvMillwardBrown

המידה בה מוטרד הציבור מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי - בדיקה נעזרת נתונים סוציו דמוגרפיים

	מאד מוטרד	מוטרד	לא מוטרד	כלל לא מוטרד	לא יודע	סה"כ N
% מהמדגם	17	33	33	12	5	529
מין						
גברים	20	27	32	16	5	260
נשים	14	39	33	9	5	269
גיל						
18-24	16	17	42	23	1	116
25-39	9	37	35	12	7	162
40-54	24	34	30	9	4	142
55+	19	42	25	6	7	109
השכלה						
יסודי או תיכון ללא בגרות	10	25	41	16	7	97
תיכון עם בגרות	12	29	36	21	3	117
על תיכוני או אקדמאי	20	37	30	8	4	297
סרב לענות	28	33	17	6	17	18
אזור מגורים						
ירושלים	12	26	40	14	8	65
מרכז	19	34	32	11	4	149
צפון	15	33	34	14	5	171
דרום	16	31	31	14	8	93
שרון	25	41	27	6		51
משלח יד						
עצמאי	19	33	33	12	3	73
שכיר	18	34	32	12	4	291
ללא מקצוע	15	30	35	14	7	165

Q1. מידע פרטי על אנשים נשמר בידי גופים ציבוריים ופרטיים. האם אתה מוטרד מהאופן בו מֻגָנִים ארגונים אלה על המידע אודותיך

ShiluvMillwardBrown

תפיסת הבטחון בהגנת מידע פרטי בגופים ציבוריים ופרטיים – % מציינים בוטח בכל קטגוריה - בדיקה נעזרת נתונים סוציו דמוגרפיים

	רופאים ונותני שרותים רפואיים	בנקים ומוסדות פיננסיים	חברות כרטיסי אשראי	רשויות המס	משטרה ורשויות אכיפה	מעבידים	רשויות מקומיות	סה"כ
% מהמדגם	74	58	56	46	46	43	42	529
מין								
גברים	73	57	60	46	47	41	36	260
נשים	74	58	52	45	45	45	48	269
גיל								
18-24	76	66	57	44	50	47	47	116
25-39	78	57	56	51	47	49	45	162
40-54	73	57	61	42	47	42	38	142
55+	66	51	48	43	39	32	37	109
השכלה								
יסודי או תיכון ללא בגרות	71	54	49	37	48	52	47	97
תיכון עם בגרות	78	69	68	46	45	45	52	117
על תיכוני או אקדמאי	74	54	54	48	46	40	36	297
סרב לענות	56	61	56	39	33	39	39	18
אזור מגורים								
ירושלים	69	52	58	40	46	43	42	65
מרכז	65	52	52	48	44	38	45	149
צפון	79	60	58	45	48	44	45	171
דרום	81	68	60	46	46	52	40	93
שרון	75	55	47	45	45	39	27	51
משלח יד								
עצמאי	71	51	56	44	40	38	40	73
שכיר	74	59	58	46	47	45	42	291
ללא מקצוע	75	59	52	46	47	42	44	165

Q2-Q14 אקריא לך רשימה של ארגונים. לגבי כל אחד מהם אנא ציין האם אתה בוטח או לא בוטח בארגון שיעשה שימוש במידע אודותיך אך ורק למטרות למענן הוא נמצא אצלם

ShiluvMillwardBrown

תפיסת הבטחון בהגנת מידע פרטי בגופים ציבוריים ופרטיים – % מצייני בוטח בכל קטגוריה - בדיקה נעזרת
נתונים סוציו דמוגרפיים

	משרדי ממשלה	חברות ביטוח	משרדי נסיעות	עמותות וארגונים שלא למטרות רווח	חברות סקרים	חברות לשרותי דיוור ישיר	סה"כ
% מהמדגם	41	38	37	33	30	29	529
מין							
גברים	39	38	33	35	33	30	260
נשים	43	38	41	30	27	29	269
גיל							
18-24	46	51	47	49	40	41	116
25-39	49	40	38	33	34	31	162
40-54	34	30	34	24	25	24	142
55+	34	32	29	26	21	22	109
השכלה							
יסודי או תיכון ללא בגרות	41	43	38	34	38	38	97
תיכון עם בגרות	41	52	47	42	33	38	117
על תיכוני או אקדמאי	42	31	33	30	27	24	297
סרב לענות	22	39	39	17	22	22	18
אזור מגורים							
ירושלים	32	38	43	40	34	35	65
מרכז	34	38	31	30	30	23	149
צפון	50	38	40	35	30	39	171
דרום	46	44	45	37	32	23	93
שרון	33	27	24	20	24	18	51
משלח יד							
עצמאי	37	33	33	32	23	30	73
שכיר	41	38	34	29	31	27	291
ללא מקצוע	43	40	43	39	32	33	165

Q2-Q14 אקריא לך רשימה של ארגונים. לגבי כל אחד מהם אנא ציין האם אתה בוטח או לא בוטח בארגון שיעשה שימוש במידע אודותיך אך ורק למטרות למענן הוא נמצא אצלם

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	מסכים	לא מסכים	מסרב לענות לא יודע	סה"כ N
% מהמדגם	24	70	5	529
מין				
גברים	27	68	5	260
נשים	22	72	6	269
גיל				
18-24	37	62	1	116
25-39	25	67	8	162
40-54	19	74	7	142
55+	17	78	5	109
השכלה				
יסודי או תיכון ללא בגרות	35	60	5	97
תיכון עם בגרות	31	67	3	117
על תיכוני או אקדמאי	19	74	6	297
סרב לענות	11	78	11	18
אזור מגורים				
ירושלים	20	72	8	65
מרכז	23	74	3	149
צפון	30	65	4	171
דרום	22	69	10	93
שרון	20	75	6	51
משלח יד				
עצמאי	16	78	5	73
שכיר	22	74	4	291
ללא מקצוע	32	60	8	165

Q15. אקריא בפניך דעות שציינו אנשים שונים, עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים: בישראל המידע האישי מוגן כראוי

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת נתונים סוציו דמוגרפיים

	מסכים	לא מסכים	מסרב לענות לא יודע	סה"כ N
% מהמדגם	79	17	5	529
מין				
גברים	80	15	4	260
נשים	77	18	5	269
גיל				
18-24	77	21	3	116
25-39	74	20	6	162
40-54	87	9	4	142
55+	77	17	6	109
השכלה				
יסודי או תיכון ללא בגרות	73	21	6	97
תיכון עם בגרות	77	18	5	117
על תיכוני או אקדמאי	82	14	4	297
סרב לענות	61	28	11	18
אזור מגורים				
ירושלים	72	18	9	65
מרכז	79	18	3	149
צפון	82	13	4	171
דרום	74	20	5	93
שרון	80	14	6	51
משלח יד				
עצמאי	86	8	5	73
שכיר	80	17	3	291
ללא מקצוע	73	19	8	165

Q16. אקריא בפניך דעות שציינו אנשים שונים, עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים: מודעות הציבור לתחום ההגנה על מידע אישי נמוכה

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת נתונים סוציו דמוגרפיים

	מסכים	לא מסכים	מסרב לענות לא יודע	סה"כ N
% מהמדגם	69	28	3	529
מין				
גברים	66	32	2	260
נשים	72	25	3	269
גיל				
18-24	65	35		116
25-39	68	30	2	162
40-54	75	23	2	142
55+	68	25	7	109
השכלה				
יסודי או תיכון ללא בגרות	63	34	3	97
תיכון עם בגרות	69	28	3	117
על תיכוני או אקדמאי	71	27	2	297
סרב לענות	72	22	6	18
אזור מגורים				
ירושלים	72	23	5	65
מרכז	68	30	2	149
צפון	64	33	2	171
דרום	74	24	2	93
שרון	75	22	4	51
משלח יד				
עצמאי	73	26	1	73
שכיר	73	26	1	291
ללא מקצוע	62	33	5	165

Q17. אקריא בפניך דעות שציינו אנשים שונים, עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים: אני מודאג מהשארת מידע אישי כגון שם, כתובת, תאריך לידה וכו' באינטרנט

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת נתונים סוציו דמוגרפיים

		מסכים	לא מסכים	מסרב לענות לא יודע	סה"כ N
	% מהמדגם	34	58	8	529
	מין				
	גברים	35	59	6	260
	נשים	33	57	10	269
	גיל				
	18-24	46	48	6	116
	25-39	32	59	9	162
	40-54	30	61	9	142
	55+	30	63	6	109
	השכלה				
	יסודי או תיכון ללא בגרות	42	53	5	97
	תיכון עם בגרות	38	56	7	117
	על תיכוני או אקדמאי	31	61	8	297
	סרב לענות	22	61	17	18
	אזור מגורים				
	ירושלים	35	49	15	65
	מרכז	25	72	3	149
	צפון	43	49	9	171
	דרום	35	54	11	93
	שרון	29	69	2	51
	משלח יד				
	עצמאי	23	66	11	73
	שכיר	36	59	5	291
	ללא מקצוע	36	52	12	165

Q18. אקריא בפניך דעות שציינו אנשים שונים. עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים: החקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים

ShiluvMillwardBrown

מודעות לרשם מאגרי המידע – בדיקה נעזרת נתונים סוציו דמוגרפיים

		כן	לא	מסרב לענות לא יודע	סה"כ N
	% מהמדגם	25	72	3	529
	מין				
	גברים	30	68	2	260
	נשים	20	76	4	269
	גיל				
	18-24	30	69	1	116
	25-39	22	73	4	162
	40-54	23	73	4	142
	55+	27	71	3	109
	השכלה				
	יסודי או תיכון ללא בגרות	19	77	4	97
	תיכון עם בגרות	26	69	4	117
	על תיכוני או אקדמאי	25	72	2	297
	סרב לענות	44	50	6	18
	אזור מגורים				
	ירושלים	17	82	2	65
	מרכז	31	68	1	149
	צפון	23	71	5	171
	דרום	26	70	4	93
	שרון	22	75	4	51
	משלח יד				
	עצמאי	27	70	3	73
	שכיר	23	74	3	291
	ללא מקצוע	27	68	4	165

Q19. האם שמעת כי במשרד המשפטים, קיימת יחידת רשם מאגרי מידע שאחראית על אכיפת חוק הגנת הפרטיות בתחום מאגרי המידע?

ShiluvMillwardBrown

מודעות לסמכויות רשם מאגרי המידע – בדיקה נעזרת
נתונים סוציו דמוגרפיים בקרב המודעים ליחידת רשם מאגרי מידע במשרד המשפטים

	כן	לא	מסרב לענות לא יודע	סה"כ N
%	58	20	21	132
מין				
גברים	51	24	24	78
נשים	69	15	17	54
גיל				
18-24	66	20	14	35
25-39	61	14	25	36
40-54	66	22	13	32
+55	38	28	34	29
השכלה				
יסודי או תיכון ללא בגרות	61	33	6	18
תיכון עם בגרות	55	23	23	31
על תיכוני או אקדמאי	60	17	23	75
סרב לענות	50	13	38	8
אזור מגורים				
ירושלים	64	27	9	11
מרכז	61	7	33	46
צפון	60	28	13	40
דרום	50	33	17	24
שרון	55	18	27	11
משלח יד				
עצמאי	55	25	20	20
שכיר	60	19	21	67
ללא מקצוע	58	22	20	45

Q20. האם למיטב ידיעתך רשם מאגרי מידע מוסמך לברר ולטפל בתלונות של אנשים במושא זה?

43

ShiluvMillwardBrown

יצירת קשר עם יחידת רשם מאגרי מידע - בדיקה נעזרת בקרב המודעים ליחידת רשם מאגרי מידע
נתונים סוציו דמוגרפיים

	כן בשאלת רישום	כן להגשת תלונה	כן שאלה משפטית	כן בעניין אחר	לא	לא יודע מסרב לענות	סה"כ
%	7	2	5	4	86	1	132
מין							
גברים	8	1	8	5	83		78
נשים	6	2		2	89	2	54
גיל							
18-24	3			6	89	3	35
25-39	6	3	6	6	81		36
40-54	19	3	13	3	75		32
+55					100		29
השכלה							
יסודי או תיכון ללא בגרות	6	6	6		83		18
תיכון עם בגרות				6	94		31
על תיכוני או אקדמאי	9		7	4	84	1	75
סרב לענות	13	13			75		8
אזור מגורים							
ירושלים		9		18	73		11
מרכז	9	2	2	4	85		46
צפון	8		13	3	83	3	40
דרום	4				96		24
שרון	9				91		11
משלח יד							
עצמאי	5	5	5	5	80		20
שכיר	12	1	6	4	81	1	67
ללא מקצוע			2	2	96		45

Q21 האם יצרת קשר בעבר עם הרשם או עם הרשות? ואם כן באיזה עניין

44

ShiluvMillwardBrown

שביעות רצון מהשירות שניתן ביחידת רשם מאגרי מידע - בקרב יוצרי הקשר עם הרשם או הרשות
נתונים סוציו דמוגרפיים

	מאד שבע רצון	שבע רצון	לא כל כך שבע רצון	לא שבע רצון	כלל לא שבע רצון	סה"כ
%	22	44	11	6	17	18
מין						
גברים	23	31	15	8	23	13
נשים	20	80				5
גיל						
18-24	33	67				3
25-39	14	43			43	7
40-54	25	38	25	13		8
55+						
השכלה						
יסודי או תיכון ללא בגרות	33		33		33	3
תיכון עם בגרות		100				2
על תיכוני או אקדמאי	18	45	9	9	18	11
סרב לענות	50	50				2
אזור מגורים						
ירושלים		67	33			3
מרכז	14	57		14	14	7
צפון	50		17		33	6
דרום		100				1
שרון		100				1
משלח יד						
עצמאי	50	25	25			4
שכיר	17	50	8	8	17	12
ללא מקצוע		50			50	2

Q22 האם יצרת קשר בעבר עם הרשם או עם הרשות? ואם כן באיזה עניין

* תא סטטיסטי קטן

ShiluvMillwardBrown

מודעות לסמכויות רשם מאגרי המידע – בדיקה נעזרת
נתונים סוציו דמוגרפיים בקרב המודעים ליחידת רשם מאגרי מידע במשרד המשפטים

	כן	לא	מסרב לענות לא יודע	סה"כ N
% מהמדגם	64	33	3	529
מין				
גברים	62	35	3	260
נשים	65	32	3	269
גיל				
18-24	67	28	4	116
25-39	60	39	1	162
40-54	65	33	2	142
55+	63	31	6	109
השכלה				
יסודי או תיכון ללא בגרות	56	40	4	97
תיכון עם בגרות	74	25	2	117
על תיכוני או אקדמאי	62	35	3	297
סרב לענות	67	22	11	18
אזור מגורים				
ירושלים	63	32	5	65
מרכז	62	36	1	149
צפון	67	29	4	171
דרום	61	37	2	93
שרון	59	35	6	51
משלח יד				
עצמאי	70	27	3	73
שכיר	62	36	3	291
ללא מקצוע	64	32	4	165

Q23. האם ידוע לך כי מי שאוסף עליך מידע צריך לזהות עצמו בפניך ולהציג את מטרת השימוש במידע כדי שיוכל לשמור אותו במאגר מידע?

ShiluvMillwardBrown

תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	נכון	לא נכון	מסרב לענות לא יודע	סה"כ N
% מהמדגם	81	14	5	529
מין				
גברים	78	17	6	260
נשים	84	12	4	269
גיל				
18-24	84	11	4	116
25-39	81	14	4	162
40-54	78	18	4	142
55+	81	13	6	109
השכלה				
יסודי או תיכון ללא בגרות	75	16	8	97
תיכון עם בגרות	83	11	6	117
על תיכוני או אקדמאי	83	14	2	297
סרב לענות	67	17	17	18
אזור מגורים				
ירושלים	85	9	6	65
מרכז	74	21	5	149
צפון	81	14	5	171
דרום	83	12	5	93
שרון	94	6		51
משלח יד				
עצמאי	85	14	1	73
שכיר	80	15	4	291
ללא מקצוע	81	12	7	165

Q24. אקריא לך מספר משפטים הקשורים להגנת מידע אישי, לגבי כל אחד מהם אנא ציין האם למיטב ידיעתך הוא נכון או לא נכון: הסכמתך נדרשת לשם שימוש במידע אודותיך

ShiluvMillwardBrown

תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	נכון	לא נכון	מסרב לענות לא יודע	סה"כ N
% מהמדגם	44	33	22	529
מין				
גברים	38	38	23	260
נשים	50	28	22	269
גיל				
18-24	47	39	15	116
25-39	49	31	19	162
40-54	37	35	28	142
55+	43	28	28	109
השכלה				
יסודי או תיכון ללא בגרות	43	42	14	97
תיכון עם בגרות	49	34	17	117
על תיכוני או אקדמאי	43	30	27	297
סרב לענות	39	33	28	18
אזור מגורים				
ירושלים	38	32	29	65
מרכז	48	27	25	149
צפון	41	39	20	171
דרום	54	31	15	93
שרון	33	39	27	51
משלח יד				
עצמאי	45	33	22	73
שכיר	44	32	24	291
ללא מקצוע	44	36	20	165

Q25. אקריא לך מספר משפטים הקשורים להגנת מידע אישי, לגבי כל אחד מהם אנא ציין האם למיטב ידיעתך הוא נכון או לא נכון: ישנה הוראה חוקית המאפשרת לך לעיין במידע אודותיך שנמצא בידי אחר

ShiluvMillwardBrown

תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	נכון	לא נכון	מסרב לענות לא יודע	סה"כ N
% מהמדגם	76	11	13	529
מין				
גברים	73	16	11	260
נשים	78	7	15	269
גיל				
18-24	78	14	9	116
25-39	83	9	8	162
40-54	73	8	18	142
55+	67	16	17	109
השכלה				
יסודי או תיכון ללא בגרות	71	15	13	97
תיכון עם בגרות	76	15	9	117
על תיכוני או אקדמאי	77	8	14	297
סרב לענות	78	11	11	18
אזור מגורים				
ירושלים	74	9	17	65
מרכז	79	11	10	149
צפון	74	15	12	171
דרום	78	11	11	93
שרון	75	2	24	51
משלח יד				
עצמאי	64	19	16	73
שכיר	81	7	12	291
ללא מקצוע	72	15	13	165

Q26. אקריא לך מספר משפטים הקשורים להגנת מידע אישי. לגבי כל אחד מהם אנא ציין האם למיטב ידיעתך הוא נכון או לא נכון: החוק בישראל מאפשר לך לתבוע בהליך משפטי פיצויים בשל הפרת חוק הגנת הפרטיות

ShiluvMillwardBrown

תפיסות לגבי שימוש באינטרנט והגנת הפרטיות – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	כן	לא	לא משתמש באינטרנט	לא יודע מסרב לענות	סה"כ N
% מהמדגם	22	70	5	3	529
מין					
גברים	29	64	4	3	260
נשים	15	75	6	4	269
גיל					
18-24	23	72	1	3	116
25-39	30	62	5	3	162
40-54	19	75	4	2	142
55+	13	72	10	5	109
השכלה					
יסודי או תיכון ללא בגרות	11	74	11	3	97
תיכון עם בגרות	26	65	5	4	117
על תיכוני או אקדמאי	25	70	3	2	297
סרב לענות	17	67	6	11	18
אזור מגורים					
ירושלים	17	72	11		65
מרכז	30	61	4	5	149
צפון	19	72	4	5	171
דרום	23	72	4	1	93
שרון	14	80	4	2	51
משלח יד					
עצמאי	22	70	3	5	73
שכיר	24	71	4	1	291
ללא מקצוע	19	68	8	5	165

Q27. האם לדעתך העברת מידע על ידך באמצעות האינטרנט היא בטוחה יחסית?

שימוש באינטרנט והגנה על מידע אישי – בדיקה נעזרת בקרב גולשי האינטרנט
נתונים סוציו דמוגרפיים

	כן	לא	מסרב לענות לא יודע	סה"כ N
% מהמדגם	60	35	5	503
מין				
גברים	66	31	4	250
נשים	55	38	7	253
גיל				
18-24	63	36	1	115
25-39	65	31	4	154
40-54	62	34	4	136
55+	46	40	14	98
השכלה				
יסודי או תיכון ללא בגרות	37	53	9	86
תיכון עם בגרות	51	45	4	111
על תיכוני או אקדמאי	70	25	5	289
סרב לענות	59	35	6	17
אזור מגורים				
ירושלים	52	36	12	58
מרכז	66	31	3	143
צפון	55	38	6	164
דרום	67	30	2	89
שרון	53	39	8	49
משלח יד				
עצמאי	69	31		71
שכיר	64	33	4	280
ללא מקצוע	49	39	11	152

Q27. האם שמעת על כלים או טכנולוגיות המגבילים או מונעים, איסוף מידע מהמחשב שלך על ידי גורמים זרים לדוגמא: פיירוול או מסנן עוגיות (cookies blocker)?

ShiluvMillwardBrown

שימוש באינטרנט והגנה על מידע אישי – בדיקה נעזרת בקרב גולשי האינטרנט
נתונים סוציו דמוגרפיים

	כן	לא	מסרב לענות לא יודע	סה"כ N
% מהמדגם	61	38	1	302
מין				
גברים	71	28	1	164
נשים	49	51	1	138
גיל				
18-24	70	30		73
25-39	64	36		100
40-54	63	37		84
55+	36	60	4	45
השכלה				
יסודי או תיכון ללא בגרות	22	78		32
תיכון עם בגרות	65	33	2	57
על תיכוני או אקדמאי	65	34		203
סרב לענות	80	20		10
אזור מגורים				
ירושלים	53	47		30
מרכז	73	26	1	95
צפון	57	42	1	91
דרום	57	43		60
שרון	50	50		26
משלח יד				
עצמאי	63	35	2	49
שכיר	59	40	1	178
ללא מקצוע	64	36		75

Q28. האם יצא לך להשתמש בעבר בכלים אלו?

ShiluvMillwardBrown

סיבה עיקרית לחוסר שימוש בכלים המגבילים איסוף מידע – בקרב גולשים שלא השתמשו בכלים אלו בעבר - בדיקה נעזרת
נתונים סוציו דמוגרפיים

	אני לא יודע איך להתקין את התוכנות הללו על המחשב	לא יודע איך להשתמש בהן	איני משוכנע שהן עובדות	לא מוסרד משאלות פרטיות כשאני גולש	הרכיבים יקרים מדי או הפתרון הזה יקר מדי	אחר	לא יודע מסרב לענות	סה"כ
% מהמדגם	24	22	6	16	4	24	3	116
מין								
גברים	24	22	4	17	4	28		46
נשים	24	23	7	16	4	21	4	70
גיל								
18-24	27	5	9	9	5	45		22
25-39	14	19	8	31	6	19	3	36
40-54	35	26	3	13	3	16	3	31
55+	22	37	4	7	4	22	4	27
השכלה								
יסודי או תיכון ללא בגרות	28	24		4	4	32	8	25
תיכון עם בגרות	37	21	5	16		21		19
על תיכוני או אקדמאי	17	23	9	21	6	23	1	70
סרב לענות	100							2
אזור מגורים								
ירושלים	36	29	7	21		7		14
מרכז	16	28		16	4	32	4	25
צפון	29	16	8	13	3	29	3	38
דרום	31	23	4	15	8	19		26
שרון		23	15	23	8	23	8	13
משלח יד								
עצמאי	24	12	6	29	6	24		17
שכיר	25	24	7	15	4	22	3	72
ללא מקצוע	22	26	4	11	4	30	4	27

Q30 מבין הסיבות הבאות, מהי הסיבה העיקרית לכך שלא השתמשת בכלים או טכנולוגיות המגבילים את איסוף המידע מהמחשב שלך, למרות שידעת על קיומם:

ShiluvMillwardBrown

גלישה באינטרנט ושמירה על הפרטיות – בקרב גולשי האינטרנט
נתונים סוציו דמוגרפיים

	תמיד	בדרך כלל	לעיתים רחוקות	כלל לא	לא יודע מסרב לענות	סה"כ
% מהגולשים	8	19	21	44	7	503
מין						
גברים	10	17	22	45	6	250
נשים	7	22	20	43	8	253
גיל						
18-24	12	20	21	43	3	115
25-39	6	21	24	43	5	154
40-54	8	19	22	44	7	136
55+	7	15	15	47	15	98
השכלה						
יסודי או תיכון ללא בגרות	7	13	17	45	17	86
תיכון עם בגרות	9	19	16	49	7	111
על תיכוני או אקדמאי	9	21	25	43	3	289
סרב לענות	6	29	12	35	18	17
אזור מגורים						
ירושלים	3	17	26	43	10	58
מרכז	7	22	21	46	4	143
צפון	13	14	19	45	9	164
דרום	8	24	21	39	8	89
שרון	2	24	22	45	6	49
משלח יד						
עצמאי	13	13	31	39	4	71
שכיר	8	23	19	46	4	280
ללא מקצוע	7	16	21	42	14	152

Q31 האם כאשר אתה גולש באינטרנט אתה בודק מהי מדיניות שמירת הפרטיות של האתר/החברה אליה גלשת?

ShiluvMillwardBrown

מתן פרטים אישיים ושמירה על הפרטיות
נתונים סוציו דמוגרפיים

	תמיד	בדרך כלל	לעיתים רחוקות	כלל לא	לא יודע מסרב לענות	סה"כ
% מהמדגם	50	27	8	10	5	529
מין						
גברים	51	24	8	11	5	260
נשים	49	30	7	9	4	269
גיל						
18-24	44	30	11	12	3	116
25-39	44	35	7	10	4	162
40-54	55	25	7	9	4	142
55+	61	15	7	9	8	109
השכלה						
יסודי או תיכון ללא בגרות	53	18	8	12	9	97
תיכון עם בגרות	52	27	9	10	2	117
על תיכוני או אקדמאי	49	31	8	9	3	297
סרב לענות	44	17	6	17	17	18
אזור מגורים						
ירושלים	37	35	14	9	5	65
מרכז	50	26	9	10	5	149
צפון	53	26	5	12	5	171
דרום	51	27	8	12	3	93
שרון	61	24	8	4	4	51
משלח יד						
עצמאי	60	22	3	11	4	73
שכיר	50	28	9	10	3	291
ללא מקצוע	47	27	8	11	7	165

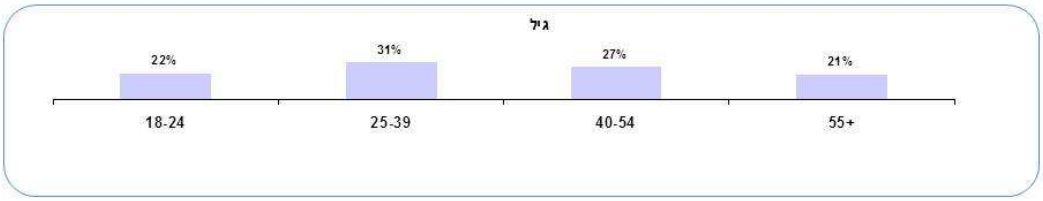
55

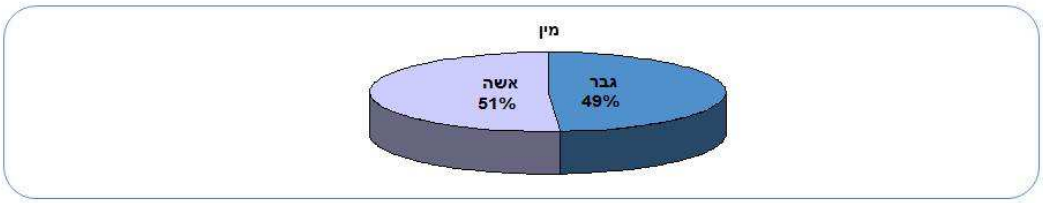
Q32 כאשר אתה מוסר פרטים לגוף כלשהו, האם אתה שואל לשם מה הם נדרשים?

ShiluvMillwardBrown



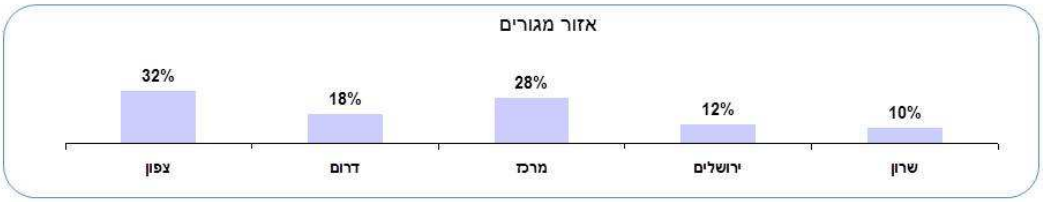
נתונים דמוגרפיים על המדגם

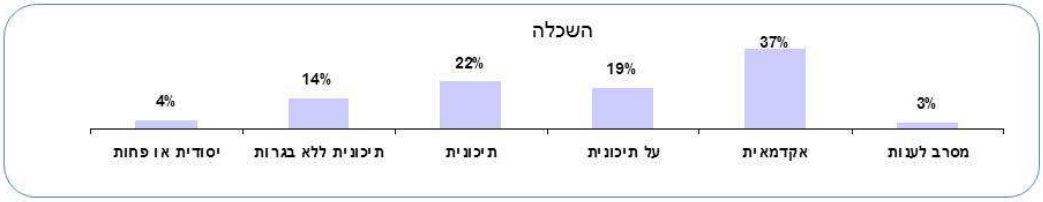

גיל
22%
31%
27%
21%
18-24
25-39
40-54
55+

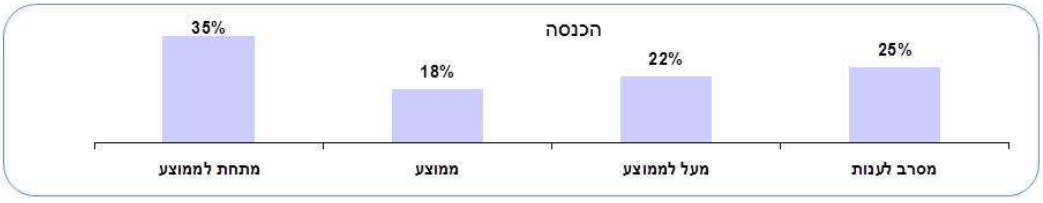

מין
אשה
51%
גבר
49%


מצב משפחתי
29%
60%
9%
3%
רווק
נשוי
גרוש, פרוד או אלמן
לא השיב

57


אזור מגורים
32%
18%
28%
12%
10%
צפון
דרום
מרכז
ירושלים
שרון


השכלה
4%
14%
22%
19%
37%
3%
יסודית או פחות
תיכונית ללא בגרות
תיכונית
על תיכונית
אקדמאית
מסרב לענות


הכנסה
35%
18%
22%
25%
מתחת לממוצע
ממוצע
מעל לממוצע
מסרב לענות

58



מטרות ושיטה

מטרות	בחינת רמת המודעות הקיימת במגזר העסקי לסוגיית ה"פרטיות" ובחינת הבנת המשמעות של חוק הגנת הפרטיות והשלכותיו במגזר העסקי
מי	203 נציגי חברות במגזר העסקי, אחראים או מעורבים בהחלטות לגבי נושאים הקשורים לניהול מידע בחברה או בארגון בו הם עובדים, במדגם ארצי, אקראי, ומייצג של אוכלוסיה זו.
מתי	במהלך חודש אוקטובר 2009
כיצד	סקר יעודי טלפוני באמצעות מערכת סקרים ממוחשבת CATI הראיונות נערכו בעברית.
ניתוח	הניתוח נערך בקרב כלל המדגם וכן על פי החיתוכים: ענף, גודל חברה, תפקיד בארגון, העברת מידע אישי באינטרנט והעברת מידע אישי למדינות אחרות.

2



- **ניהול מידע אישי נפוץ במרבית החברות והארגונים בישראל:**

  בכ-70% מהחברות מנהלים מידע אישי ממוחשב אודות אנשים. מתוכן, במרבית החברות (57%) מדובר במאגר של עד 1000 אנשים. ב-18% חברות נוספות נעות הרשומות עד עשרת אלפים איש. אחוזים בודדים לחברות בהן מאגרי מידע עד מאה אלף איש ומעלה. השונות בין הענפים השונים נמוכה.

- **יש מקום רב לשיפור ההיכרות של הגופים והחברות במשק עם חוק הגנת הפרטיות ומשמעויותיו:**
  - מעל מחצית מהחברות במשק הישראלי לא מכירות את הוראות חוק הגנת הפרטיות בתחום ההגנה על מידע אישי. גם בקרב 45% מהחברות שציינו שמכירים את הוראות חוק הגנת הפרטיות רק 17% ציינו "מכיר טוב".
  - התפיסה הרווחת בקרב מרבית האחראים על המידע האישי בחברות, שמכירים את החוק, היא שחוק הגנת הפרטיות בישראל מקנה לאזרחים הגנה ברמה בינונית (58%). רק 16% סבורים שהחוק מקנה הגנה ברמה גבוהה בעוד אחוז זהה של משיבים סבור שההגנה שמקנה החוק, נמוכה. יחד עם זאת, מרבית המשיבים (79%) סבורים כי מנקודת המבט של ניהול עסק מאפשר חוק הגנת הפרטיות לנהל עסק כמו שלהם. 14% סבורים כי החוק מקשה על ניהול עסק מעל הנדרש ואילו 7% ציינו לא יודע. בענפי המסחר והשירותים, בקרב ממונים על אבטחת מידע, מנהלי IT ובקרב חברות עם 21 עובדים ומעלה ההיכרות עם החוק טובה יותר.

4

- **החוק אינו מתמודד עם התופעה של העברת מידע אישי רב בין גורמים שונים:**
  - כמחצית מהמשיבים סבורים כי החוק הישראלי אינו מצליח להתמודד עם התופעה של העברת מידע אישי רב בין גורמים שונים (לדוגמא באמצעות האינטרנט) 24% נוספים השיבו "לא יודע". רק כ-2% מהמשיבים סבורים כי החוק מצליח להתמודד במידה טובה מאד. 25% נוספים ציינו כי החוק מצליח להתמודד עם התופעה במידה טובה. מעבירי מידע באינטרנט תופסים יותר מאחרים כי החוק מתמודד טוב יותר עם העברת מידע אישי.
- **יחד עם זאת יש נכונות בציבור העסקי לשיפור והבהרת משמעות החוק:**
  - כשני שליש מהנשאלים היו מעדיפים שיבהירו את משמעותן או ישפרו את קביעת הנורמות המחייבות בנושא אבטחת מידע. מעל מחצית מהנשאלים (56%) רוצים שיובהרו המגבלות של חוק הגנת הפרטיות על שימוש במידע אישי. 44% רוצים שתובהר חובת הרישום ותהליך רישום מאגרי מידע ו-42% סבורים שנדרשת הבהרה בנושא חקיקה ספציפית להוראות הנוגעות לעיבוד מידע אישי לפי סקטורים. כחמישית מהנשאלים מעדיפים שבמסגרת חוק הגנת הפרטיות יובהרו גם נושאים אחרים.

5

ShiluvMillwardBrown

- **יש לפעול להגברת המודעות ולשיפור הפעולות שננקטות להגנת הפרטיות בתוך החברות והארגונים:**
  - בשש מתוך עשר חברות נבחנים בשלב האפיון, הפיתוח והיישום של שירותי מידע שיקולים של הגנת המידע האישי המוחזק בחברה. ב-39% מהחברות בקביעות וב-22% מהחברות לעיתים. ב-19% מהחברות הנושא אינו נבחן. 20% ציינו לא יודע או סרבו לענות.
  - רק במחצית מהחברות והארגונים מודעים למוצרי חומרה או תוכנה המגבירים את הגנת הפרטיות במאגר המידע של החברה. בכ-18% מהחברות לא משתמשים, אבל מודעים לתחום ובכ-30% מהחברות לא משתמשים ומעולם לא שמעו על התחום. המודעות גבוהה יותר בחברות המונות מעל 20 עובדים.

6

- **מהארגונים והגופים שנדגמו, עולה כי העברת מידע אישי לגורם שלישי אינה תופעה שכיחה, אולם יש לחדד את נושא אמצעי הזהירות בהם יש לנקוט בעת ביצוע העברת המידע:**
  - רק 16% מהחברות ציינו כי הן מעבירות מידע אישי על אנשים לגורמים אחרים באמצעות האינטרנט. ואילו רק 7% מהחברות ציינו כי הן מעבירות מידע אישי על אנשים לחו"ל. מתוך חברות אלו, רק כמחצית נוקטות באמצעים למניעת שימוש שונה מהמטרה לשמה נמסר המידע. האמצעים למניעת שימוש שונה במידע: נוהליים (85%), טכנולוגיים (80%) ומשפטיים (60%).
  - ב-72% מהחברות המעבירות מידע אישי נוהגים ליידע את האדם עליו מועבר המידע. ב-39% מתוכן, מקבלים את הסכמת האדם מראש. כרבע מהחברות המעבירות מידע אינן נוהגות ליידע את האדם עליו הועבר המידע ו-3% ציינו לא יודע. האמצעים העיקריים המשמשים להעברת המידע: דואר אלקטרוני (69%), טלפון (61%) ובאמצעות רשת האינטרנט (56%), פקס (47%), שליחים (47%) רשת סגורה ומוצפנת ודואר רגיל (33% כל אחד).

- **יש לתקשר את החשיבות של קביעת מדיניות שמירת הפרטיות בארגונים השונים ומידת היותה של המדיניות נגישה כלפי הבאים במגע עם הארגון:**
  - לכשליש מהחברות במשק אין מדיניות לשמירה על הפרטיות. בקרוב לשליש מהחברות מדיניות שמירת הפרטיות אינה מפורסמת ברבים. רק ב-9% מהחברות והארגונים במשק הישראלי מפורסמת מדיניות שמירת הפרטיות בדף הראשי באתר האינטרנט של החברה. אצל 6% חברות נוספות יש קישור כלשהו למדיניות במקום כלשהו באתר החברה. 11% מהמשיבים ציינו אחר -15% ציינו לא יודע.
  - ל-4% מהחברות במשק הישראלי הופנו בקשות לעיין או לקבל מידע על בסיס סעיף 13 לחוק הגנת הפרטיות. ל- 68% מהחברות לא הופנו בקשות ואילו 28% נוספים ציינו לא יודע או סרבו לענות.
  - ב-94% מהארגונים והחברות טענו כי לא התקבלו תלונות מאנשים עליהם שמור בחברה מידע, 5% השיבו לא יודע ו-1% ציינו כי קיבלו פניות.

- **יש מקום לפעילות תקשורתית שתסביר את תפקיד יחידת רשם מאגרי המידע ותעודד פנייה אליה: מרבית הארגונים במשק הישראלי לא היו בקשר עם יחידת רשם מאגרי המידע, ייתכן שהסיבה לכך היא חוסר היכרות עם החוק המחייב רישום מאגרי מידע:**
  - ל-77% מהחברות לא היה קשר עם רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע. רק 9% ציינו כי היו בקשר עם הרשם. 13% ציינו לא יודע או סרבו לענות. הסיבה העיקרית לקשר עם יחידת הרשם הייתה בנוגע לרישום מאגרי מידע. בקרב הפונים ליחידת הרשם כ-58% מרוצים מתוכם 5% מרוצים מאד. 10% ציינו כי אינם מרוצים, מחציתם כלל לא מרוצים.
  - רק ל-15% מהחברות רשומים מאגרי המידע של החברה אצל רשם מאגרי המידע. 50% ציינו כי מאגרי המידע של החברה אינם רשומים בעוד 35% נוספים ציינו לא יודע או סרבו לענות.

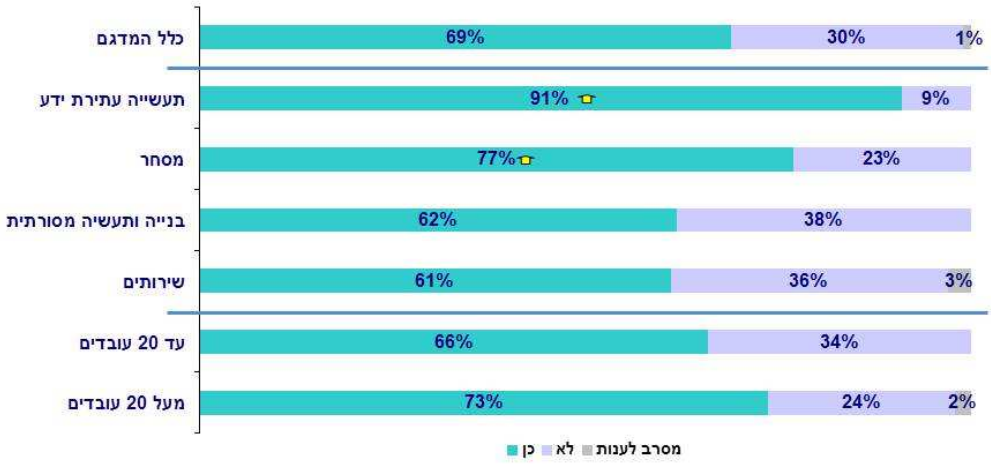


ניהול מידע אישי ומאגרי מידע בישראל

9

ניהול מידע אישי ממוחשב בחברות וארגונים – בדיקה נעזרת

כלל המדגם



- ניהול מידע אישי נפוץ במרבית החברות והארגונים בישראל. כאשר בענפי התעשייה עתירת הידע והמסחר הוא נפוץ יותר מאשר בענפי הבניה והתעשייה המסורתית והשירותים.
- ניהול המידע נפוץ יותר בחברות בהן מספר העובדים רב יותר.

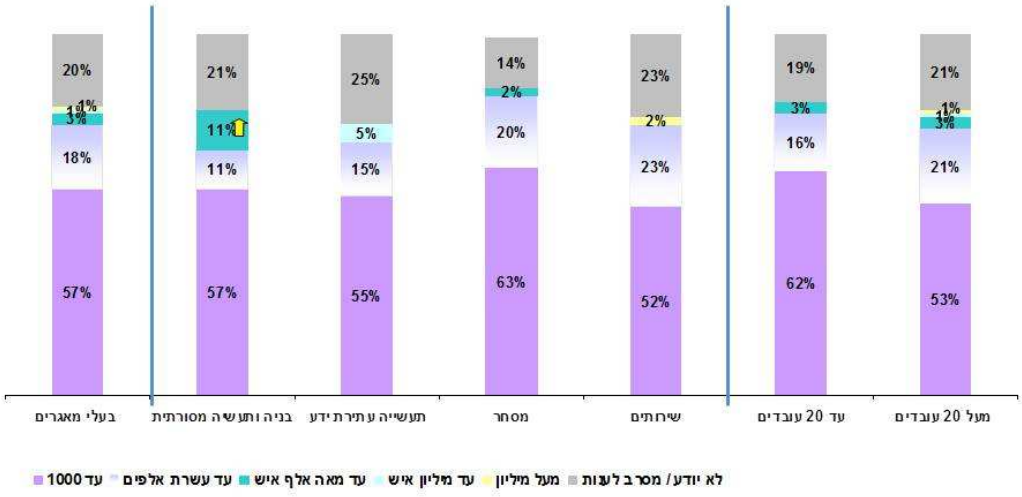
Q6. האם החברה מנהלת או ברשותה מידע אישי אודות אנשים באופן ממוחשב?

10 הבדל מובהק

ShiluvMillwardBrown

גודל מאגרי המידע בחברות ובארגונים - בדיקה נעזרת

בקרב חברות בעלות מאגרי מידע N=141



- במרבית החברות (57%) מכיל המאגר עד 1000 רשומות. בחברות בהן מעל 20 עובדים מאגרי המידע מכילים יותר רשומות.

Q7. על כמה אנשים יש מידע במאגרי המידע של החברה?

⇧ הבדל מובהק

ShiluvMillwardBrown

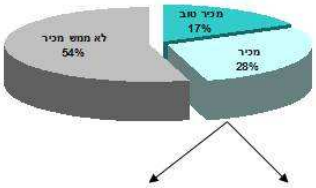


חוק הגנת הפרטיות – מודעות ותפיסות במגזר העסקי

ShiluvMillwardBrown

החברה או הארגון וחוק הגנת הפרטיות - נעזר

מודעות להוראות חוק הגנת הפרטיות
כלל המדגם



מנקודת המבט של ניהול עסק, האם לדעתך חוק הגנת הפרטיות בישראל
N=92



רמת ההגנה שמקנה חוק הגנת הפרטיות בישראל בקרב המכירים את החוק
N=92



- מעל מחצית מהחברות במשק הישראלי לא מכירות את חוק הגנת הפרטיות בתחום ההגנה על מידע אישי.
- בקרב המכירים את החוק, התפיסה היא שהחוק מקנה הגנה בינונית. כמו כן, מרבית מכירי החוק, מחזיקים בתפיסה לפיה מאפשר החוק ניהול עסק.

Q8. עד כמה אתה מכיר את הוראות חוק הגנת הפרטיות בתחום ההגנה על מידע אישי (מאגרי מידע) בישראל?
Q9. האם למיטב ידיעתך, חוק הגנת הפרטיות בישראל, מקנה לאזרחים הגנה ברמה: גבוהה בינונית או נמוכה?
Q10. מנקודת המבט של ניהול עסק, האם לדעתך חוק הגנת הפרטיות בישראל: מאפשר לנהל עסק כמו שלך או מקשה על ניהול עסק כמו שלך מעל הנדרש?

ShiluvMillwardBrown

הכרת חוק הגנת הפרטיות – בדיקה נעזרת

ניתוח לפי סגמנט

	מכיר טוב	מכיר	לא ממש מכיר	לא יודע / מסרב לענות	סה"כ
% מהמדגם	17	28	54		203
ענף					
בניה ותעשיה מסורתית	7	27	67		45
תעשיה עתירת ידע	5	36	59		22
מסחר	22	25	53		64
שירותים	24	29	46	1	72
גודל חברה					
עד 20 עובדים	12	26	62		105
מעל 20 עובדים	22	31	46	1	98
תפקיד בארגון					
ממונה אבטחת מידע	31	27	42		26
מנהל IT	27	23	50		22
מנהל שיווק	22	17	61		18
מנהל כח אדם / משאבי אנוש	8	13	75	4	24
מנכ"ל	14	31	55		84
מנהל כספים	10	45	45		29
מעביר מידע אישי באינטרנט					
כן	22	25	50	3	32
לא	16	29	55		166
לא יודע / מסרב לענות	20	20	60		5
מעביר מידע אישי לחו"ל					
כן	14	29	57		14
לא	17	28	54		184
לא יודע / מסרב לענות	20	20	40	20	5

מרואיינים מענפי המסחר והשירותים כמו גם ממונים על אבטחת מידע בחברות ומנהלי IT מכירים טוב יותר את חוק הגנת הפרטיות.

הבדל מובהק

Q8. [Q1a] עד כמה אתה מכיר את הוראות חוק הגנת הפרטיות בתחום ההגנה על מידע אישי (מאגרי מידע) בישראל?

ShiluvMillwardBrown

ההגנה שמקנה חוק הגנת הפרטיות בישראל – בדיקה נעזרת

ניתוח לפי סגמנט

	גבוהה	בינונית	נמוכה	לא יודע / מסרב לענות	סה"כ
% בקרב מכירי החוק	16	58	16	10	92
ענף					
בניה ותעשיה מסורתית	13	53	27	7	15
תעשיה עתירת ידע	11	44	11	33	9
מסחר	20	57	17	7	30
שירותים	16	63	13	8	38
גודל חברה					
עד 20 עובדים	18	60	13	10	40
מעל 20 עובדים	15	56	19	10	52
תפקיד בארגון					
ממונה אבטחת מידע	7	73	13	7	15
מנהל IT		64	18	18	11
מנהל שיווק	14	57	29		7
מנהל כח אדם / משאבי אנוש	20	60	20		5
מנכ"ל	24	47	16	13	38
מנהל כספים	19	63	13	6	16
מעביר מידע אישי באינטרנט					
כן	7	80	7	7	15
לא	19	53	19	9	75
לא יודע / מסרב לענות		50		50	2
מעביר מידע אישי לחו"ל					
כן		83	17		6
לא	18	56	17	10	84
לא יודע / מסרב לענות		50		50	2

Q9. האם למיטב ידיעתך, חוק הגנת הפרטיות בישראל מקנה לאזרחים הגנה ברמה:

ממונים על אבטחת מידע בחברות ומעבירי מידע אישי באינטרנט תפיסת החוק כמקנה הגנה לאזרחים גבוהה יותר.

הבדל מובהק

ShiluvMillwardBrown

תפיסת התמודדות החוק הישראלי בנושא העברת מידע אישי - נעזר

כלל המדגם



- כמחצית מהמשיבים סבורים כי החוק בישראל אינו מצליח להתמודד עם התופעה של העברת מידע אישי רב בין גורמים שונים.

Q11. באיזו מידה לדעתך החוק הישראלי מצליח להתמודד עם התופעה של העברת מידע אישי רב בין גורמים שונים (לדוגמה באמצעות האינטרנט)?

ShiluvMillwardBrown

תפיסת התמודדות החוק להגנת הפרטיות עם העברת מידע אישי – בדיקה נעזרת

ניתוח לפי סגמנט

	במידה טובה מאד	במידה טובה	במידה לא כל כך טובה	במידה כלל לא טובה	לא יודע / מסרב לענות	סה"כ
% מהמדגם	2	25	28	21	24	203
ענף						
בניה ותעשיה מסורתית	4	22	20	27	27	45
תעשיה עתירת ידע		23	27	9	41	22
מסחר	3	27	27	20	23	64
שירותים		26	35	22	17	72
גודל חברה						
עד 20 עובדים	2	26	23	25	25	105
מעל 20 עובדים	2	24	34	17	22	98
תפקיד בארגון						
ממונה אבטחת מידע		19	23	27	31	26
מנהל IT		36	23	9	32	22
מנהל שיווק	6	33	17	33	11	18
מנהל כח אדם / משאבי אנוש	4	29	29	17	21	24
מנכ"ל	1	23	31	24	21	84
מנהל כספים	3	21	34	14	28	29
מעביר מידע אישי באינטרנט						
כן	3	38	34	16	9	32
לא	2	23	27	22	26	166
לא יודע / מסרב לענות		20	20	20	40	5
מעביר מידע אישי לחו"ל						
כן		29	29	14	29	14
לא	2	25	28	22	23	184
לא יודע / מסרב לענות		20	40		40	5

מעבירי מידע אישי באינטרנט תופסים יותר מאחרים כי החוק מתמודד טוב יותר עם העברת מידע אישי. בענף השירותים ובחברות בהן מספר עובדים גבוה מ- 20 נתפסת ההתמודדות "במידה לא כל כך טובה".

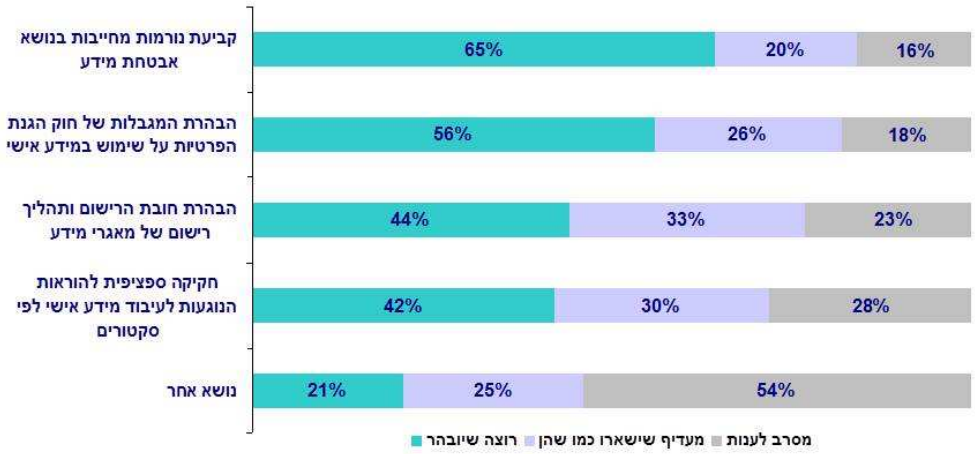
הבדל מובהק

Q11. [Q4] באיזו מידה לדעתך החוק הישראלי מצליח להתמודד עם התופעה של העברת מידע אישי רב בין גורמים שונים (לדוגמה באמצעות האינטרנט)?

ShiluvMillwardBrown

הבנת והבהרת חוק הגנת הפרטיות – בדיקה נעזרת

כלל המדגם



- מרבית הנשאלים היו רוצים לקבל הבהרות לאספקטים השונים של חוק הגנת הפרטיות ובעיקר לקביעת נורמות מחייבות בנושא אבטחת מידע.

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן?

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	הבהרת המגבלות של חוק הגנת הפרטיות על שימוש במידע אישי			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	56	26	18	203
ענף				
בניה ותעשיה מסורתית	67	20	13	45
תעשיה עתירת ידע	55	9	36	22
מסחר	50	31	19	64
שירותים	56	31	14	72
גודל חברה				
עד 20 עובדים	55	27	18	105
מעל 20 עובדים	57	26	17	98
תפקיד בארגון				
ממונה אבטחת מידע	65	12	23	26
מנהל IT	27	41	32	22
מנהל שיווק	44	28	28	18
מנהל כח אדם / משאבי אנוש	75	17	8	24
מנכ"ל	57	27	15	84
מנהל כספים	59	31	10	29
מעביר מידע אישי באינטרנט				
כן	59	25	16	32
לא	56	27	17	166
לא יודע / מסרב לענות	40	20	40	5
מעביר מידע אישי לחו"ל				
כן	50	21	29	14
לא	57	27	16	184
לא יודע / מסרב לענות	60		40	5

בענף הבנייה והתעשייה המסורתית היו רוצים שיובהר החוק. בעוד שבענפי המסחר והשירותים ובקרב בעלי התפקידים: מנהל IT, מנכ"ל ומנהל כספים מעדיפים המרואיינים לשמור על הסטטוס קוו.

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן: הבהרת המגבלות של חוק הגנת הפרטיות על שימוש במידע אישי

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	הבהרת חובת הרישום ותהליך רישום מאגרי מידע			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	44	33	23	203
ענף				
בניה ותעשיה מסורתית	40	33	27	45
תעשיה עתירת ידע	41	27	32	22
מסחר	44	36	20	64
שירותים	49	31	21	72
גודל חברה				
עד 20 עובדים	44	31	25	105
מעל 20 עובדים	45	34	21	98
תפקיד בארגון				
ממונה אבטחת מידע	46	27	27	26
מנהל IT	36	36	27	22
מנהל שיווק	33	39	28	18
מנהל כח אדם / משאבי אנוש	46	29	25	24
מנכ"ל	51	27	21	84
מנהל כספים	34	48	17	29
מעביר מידע אישי באינטרנט				
כן	47	38	16	32
לא	45	31	24	166
לא יודע / מסרב לענות	60		40	5
מעביר מידע אישי לחו"ל				
כן	36	43	21	14
לא	46	32	23	184
לא יודע / מסרב לענות	20	40		5

בקרב מנהלי כספים, ייצוג גבוה למעדיפים שחובת הרישום ותהליך רישום מאגרי מידע יישארו כמו שהן.

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן: הבהרת חובת הרישום ותהליך רישום מאגרי מידע

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	קביעת נורמות מחייבות בנושא אבטחת מידע			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	65	20	16	203
ענף				
בניה ותעשיה מסורתית	58	27	16	45
תעשיה עתירת ידע	73	9	18	22
מסחר	66	19	16	64
שירותים	65	19	15	72
גודל חברה				
עד 20 עובדים	61	24	15	105
מעל 20 עובדים	68	15	16	98
תפקיד בארגון				
ממונה אבטחת מידע	65	8	27	26
מנהל IT	68	18	14	22
מנהל שיווק	72	11	17	18
מנהל כח אדם / משאבי אנוש	58	25	17	24
מנכ"ל	62	24	14	84
מנהל כספים	69	21	10	29
מעביר מידע אישי באינטרנט				
כן	59	22	19	32
לא	66	19	14	166
לא יודע / מסרב לענות	40	20	40	5
מעביר מידע אישי לחו"ל				
כן	64	7	29	14
לא	65	21	14	184
לא יודע / מסרב לענות	60		40	5

בענף בניה ותעשייה מסורתית ובקרב בעלי התפקידים: מנהל כח אדם או משאבי אנוש ומנכ"ל העדפה להשארת הנורמות כמו שהן.

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן: קביעת נורמות מחייבות בנושא אבטחת מידע

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	חקיקה ספציפית להוראות הנוגעות לעיבוד מידע אישי לפי סקטורים			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	42	30	28	203
ענף				
בניה ותעשיה מסורתית	47	20	33	45
תעשיה עתירת ידע	18	45	36	22
מסחר	41	34	25	64
שירותים	47	28	25	72
גודל חברה				
עד 20 עובדים	38	30	31	105
מעל 20 עובדים	46	30	24	98
תפקיד בארגון				
ממונה אבטחת מידע	54	12	35	26
מנהל IT	36	32	32	22
מנהל שיווק	44	33	22	18
מנהל כח אדם / משאבי אנוש	50	13	38	24
מנכ"ל	39	37	24	84
מנהל כספים	34	38	28	29
מעביר מידע אישי באינטרנט				
כן	41	34	25	32
לא	42	30	28	166
לא יודע / מסרב לענות	40		60	5
מעביר מידע אישי לחו"ל				
כן	50	14	36	14
לא	41	32	27	184
לא יודע / מסרב לענות	60		40	5

בקרב ענפי המסחר והשירותים היו רוצים שיובהרו הוראות הנוגעות לעיבוד מידע אישי לפי סקטורים. בענף תעשיה עתירת ידע ובקרב בעלי התפקידים: מנהל IT, מנהל שיווק, מנכ"ל ומנהל כספים מעדיפים את השארת המצב כפי שהוא.

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן: חקיקה ספציפית להוראות הנוגעות לעיבוד מידע אישי לפי סקטורים

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	נושא אחר			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	21	25	54	203
ענף				
בניה ותעשיה מסורתית	31	13	56	45
תעשיה עתירת ידע	14	9	77	22
מסחר	16	34	50	64
שירותים	21	29	50	72
גודל חברה				
עד 20 עובדים	23	24	53	105
מעל 20 עובדים	18	27	55	98
תפקיד בארגון				
ממונה אבטחת מידע	23	12	65	26
מנהל IT	23	23	55	22
מנהל שיווק	17	39	44	18
מנהל כח אדם / משאבי אנוש	21	21	58	24
מנכ"ל	21	30	49	84
מנהל כספים	17	21	62	29
מעביר מידע אישי באינטרנט				
כן	25	25	50	32
לא	20	25	54	166
לא יודע / מסרב לענות		20	80	5
מעביר מידע אישי לחו"ל				
כן	14	7	79	14
לא	21	27	52	184
לא יודע / מסרב לענות	40	21	60	5

בענף בניה ותעשיה מסורתית רוצים שיובהרו נושאים אחרים בעוד שבקרב ענפי המסחר והשירותים ובקרב בעלי התפקידים: מנהל שיווק ומנכ"ל העדפה להשארת החוק כמו שהוא.

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או שיבהירו את משמעותן או שיישארו כמות שהן: נושא אחר

ShiluvMillwardBrown

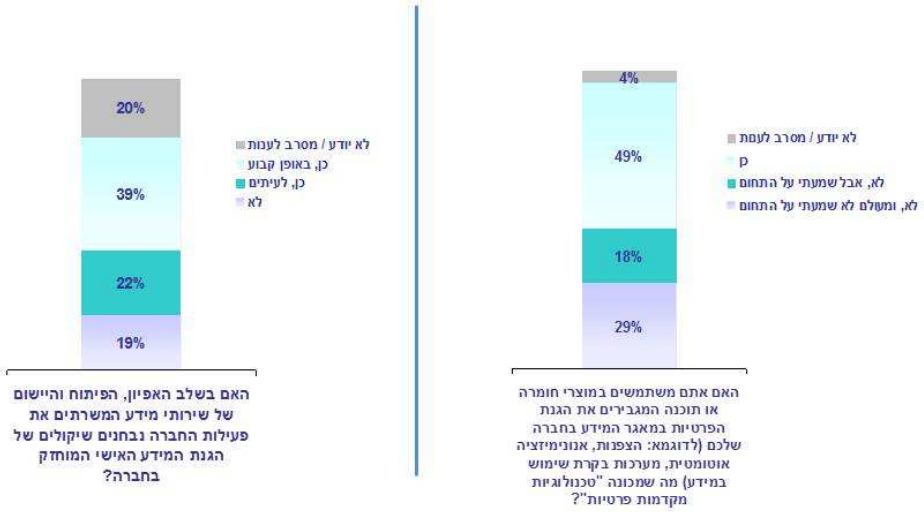


הגנה על מידע אישי בתוך הארגון

ShiluvMillwardBrown

הגנה על מידע אישי בתוך הארגון - נעזר

כלל המדגם



- **בשש מתוך עשר חברות נבחנים בשלב האפיון, הפיתוח והיישום של שירותי המידע שיקולים של הגנת המידע האישי המוחזק בחברה. בארבע מתוך עשר חברות בקביעות ובשתיים מתוך עשר חברות לעיתים. יחד עם זאת, בקרוב למחצית מהחברות והארגונים לא מודעים למוצרי חומרה או תוכנה המגבירים את הגנת הפרטיות במאגר המידע של החברה.**

Q13. האם בשלב האפיון, הפיתוח והיישום של שירותי מידע המשרתים את פעילות החברה נבחנים שיקולים של הגנת המידע האישי המוחזק בחברה?
Q14. [Q5] האם אתם משתמשים במוצרי חומרה או תוכנה המגבירים את הגנת הפרטיות במאגר המידע בחברה שלכם (לדוגמא: הצפנות, אנונימיזציה אוטומטית, מערכות בקרת שימוש במידע) מה שמכונה "טכנולוגיות מקדמות פרטיות"?

ShiluvMillwardBrown

שיקולי הגנה על מידע אישי בתוך הארגון בשלב אפיון פיתוח ויישום – בדיקה נעזרת

ניתוח לפי סגמנט

	סה"כ	לא יודע / מסרב לענות	לא	כן, לעיתים	כן, באופן קבוע
% כלל המדגם	203	20	19	22	39
ענף					
בניה ותעשיה מסורתית	45	22	27	22	29
תעשיה עתירת ידע	22	23	9	27	41
מסחר	64	23	19	25	33
שירותים	72	14	18	18	50
גודל חברה					
עד 20 עובדים	105	22	24	25	30
מעל 20 עובדים	98	17	14	19	49
תפקיד בארגון					
ממונה אבטחת מידע	26	19	15	12	54
מנהל IT	22	18	18	18	45
מנהל שיווק	18	6	11	28	56
מנהל כח אדם / משאבי אנוש	24	29	21	21	29
מנכ"ל	84	19	20	27	33
מנהל כספים	29	24	24	17	34
מעביר מידע אישי באינטרנט					
כן	32	9	16	38	38
לא	166	20	19	20	40
לא יודע / מסרב לענות	5	60	40		
מעביר מידע אישי לחו"ל					
כן	14	7	29	14	50
לא	184	20	18	23	38
לא יודע / מסרב לענות	5	40	20		40

בענף השירותים, בחברות מעל 20 עובדים ובקרב בעלי התפקידים: ממונה אבטחת מידע ומנהל שיווק בוחנים יותר, באופן קבוע, שיקולים של הגנת מידע בשלב האפיון, הפיתוח והיישום.

Q13. האם בשלב האפיון, הפיתוח והיישום של שירותי מידע המשרתים את פעילות החברה נבחנים שיקולים של הגנת המידע האישי המוחזק בחברה?

ShiluvMillwardBrown

שימוש בחומרות ותוכנות להגברת הגנת הפרטיות – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא, אבל שמעתי על התחום	לא, ומעולם לא שמעתי על התחום	לא יודע / מסרב לענות	סה"כ
% כלל המדגם	49	18	29	4	203
ענף					
בניה ותעשיה מסורתית	42	16	36	7	45
תעשיה עתירת ידע	59	27	5	9	22
מסחר	44	27	28	2	64
שירותים	56	8	32	4	72
גודל חברה					
עד 20 עובדים	44	16	35	5	105
מעל 20 עובדים	55	19	21	4	98
תפקיד בארגון					
ממונה אבטחת מידע	62	8	27	4	26
מנהל IT	50	23	18	9	22
מנהל שיווק	39	22	28	11	18
מנהל כח אדם / משאבי אנוש	33	21	38	8	24
מנכ"ל	51	17	30	2	84
מנהל כספים	52	21	28		29
מעביר מידע אישי באינטרנט					
כן	56	16	25	3	32
לא	48	19	28	5	166
לא יודע / מסרב לענות	40		60		5
מעביר מידע אישי לחו"ל					
כן	43	21	29	7	14
לא	50	18	28	4	184
לא יודע / מסרב לענות	40		40	20	5

בענפי התעשיה עתירת הידע והשירותים שמעו מי שאינם משתמשים באמצעים יותר על התחום.

בענפים: בניה ותעשיה מסורתית ושירותים, ובקרב חברות המונות עד 20 עובדים ייצוג בולט לקבוצה שאינה משתמשת ולא שמעה מעולם על התחום.

Q14. [5Q] האם אתם משתמשים במוצרי חומרה או תוכנה המגבירים את הגנת הפרטיות במאגר המידע בחברה שלכם (לדוגמא, הצפנות, אנונימיזציה אוטומטית, מערכות בקרת שימוש במידע) מה שמכונה "טכנולוגיות מקדמות פרטיות"?

ShiluvMillwardBrown

העברת מידע אישי לגורם שלישי - נעזר

כלל המדגם



- מרבית החברות במשק ציינו כי אינן נוהגות להעביר מידע אישי לגורם אחר.

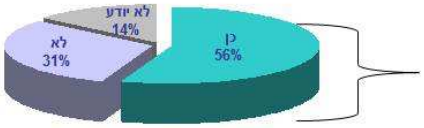
Q15. [Q6] האם החברה שלכם מעבירה מידע אישי על אנשים לגורם אחר באמצעות האינטרנט או בדרכים אחרות?
Q16. [Q8] האם החברה שלך מעבירה בדרך כלל מידע אישי על אנשים לחו"ל?

ShiluvMillwardBrown

העברת מידע אישי לגורם שלישי ואמצעי זהירות שנוקט הארגון - נעזר

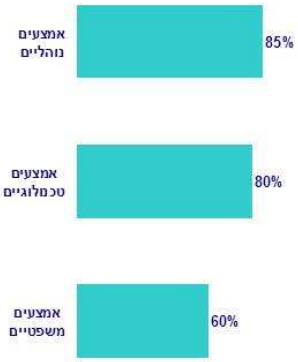
שימוש באמצעים למניעת שימוש שונה במידע אישי מהמטרה לשמה נמסר

בקרב מעבירי מידע אישי N=36*



באיזה אמצעים החברה נוקטת

בקרב מעבירי מידע אישי שנוקטים באמצעים N=20*



- מעט יותר ממחצית מהחברות המעבירות מידע אישי, נוקטות באמצעים כדי למנוע שימוש במידע אישי השונה מהמטרה לשמה הוא נמסר על ידם.

Q17. [Q7] האם החברה נוקטת באמצעים כדי למנוע שימוש במידע אישי השונה מהמטרה לשמה הוא נמסר על ידם?

Q18-Q20.באיזה אמצעים החברה נוקטת?

ShiluvMillwardBrown

העברת מידע אישי לגורם שלישי וחוק הגנת הפרטיות - נעזר

בקרב מעבירי מידע לגורם שלישי N=36*

האם האדם עליו מועבר המידע מיודע על כך:



סוג המידע המועבר:



אמצעי העברת המידע:



- ב-72% מהחברות המעבירות מידע אישי נוהגים ליידע את האדם עליו מועבר המידע.

Q21. כאשר אתם מעבירים מידע על אדם לגורם שלישי, האם האדם עליו מועבר המידע מיודע על כך?

Q22. [Q9] לגבי כל אחד מסוגי המידע הבאים, אמור האם החברה בה אתה עובד מעבירה לגורמים אחרים בארץ ובחו"ל מידע מסוג זה:

Q28-35. [Q10] כאשר אתם מעבירים לגורם אחר מידע אישי על אנשים איך המידע מועבר? האם אתם משתמשים באחד הכלים שאקריא לכם?

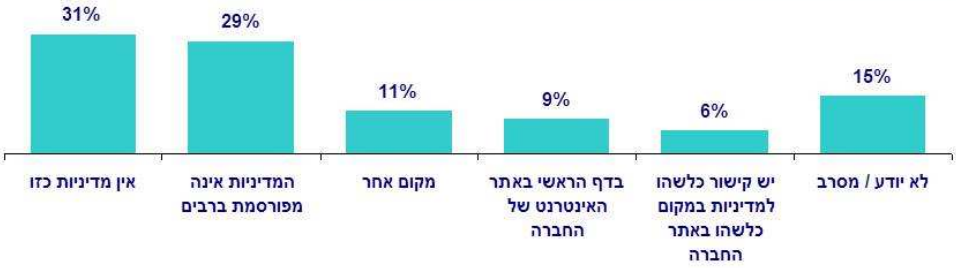
ShiluvMillwardBrown

פרסום מדיניות שמירת הפרטיות של הארגון - נעזר

כלל המדגם

סה"כ חברות שמפרסמות את מדיניות שמירת הפרטיות: 26%

סה"כ חברות בהן יש מדיניות שמירת פרטיות: 55%



- במרבית החברות במשק אין שקיפות בנושא מדיניות שמירת הפרטיות: בכשליש מהחברות כלל אין מדיניות לשמירה על הפרטיות ובקרוב לשליש נוסף המדיניות אינה מפורסמת ברבים.
- לכרבע מהחברות במשק הישראלי יש מדיניות שמירה על הפרטיות: רק בחברה אחת מתוך עשר ניתן לראות מדיניות שמירה על הפרטיות בדף הראשי באתר האינטרנט של החברה. ב-6% חברות נוספות יש קישור למדיניות במקום כלשהו באתר החברה ול- 11% חברות נוספות ניתן לראות מדיניות במקום אחר.

Q36. האם יש לחברה בה אתה עובד מדיניות שמירה על הפרטיות ואם כן היכן היא מפורסמת?

ShiluvMillwardBrown

מדיניות הגנת הפרטיות ושקיפות לגביה בארגון – בדיקה נעזרת

ניתוח לפי סגמנט

	בדף הראשי באתר האינטרנט של החברה	יש קישור כלשהו למדיניות במקום כלשהו באתר החברה	במקום אחר	המדיניות אינה מפורסמת ברבים	אין מדיניות כזו
% כלל המדגם	9	6	11	29	31
ענף					
בניה ותעשיה מסורתית	7	2	16	20	42
תעשיה עתירת ידע	5	5	14	27	32
מסחר	3	11	8	36	33
שירותים	17	4	10	29	21
גודל חברה					
עד 20 עובדים	10	5	8	32	32
מעל 20 עובדים	8	7	14	26	29
תפקיד בארגון					
ממונה אבטחת מידע	15	4	19	27	23
מנהל IT	9	5	14	45	9
מנהל שיווק	6			33	44
מנהל כח אדם / משאבי אנוש	13	4	17	25	13
מנכ"ל	10	10	11	29	29
מנהל כספים		3	3	21	66
מעביר מידע אישי באינטרנט					
כן	9	13	19	38	9
לא	8	5	9	28	35
לא יודע / מסרב לענות	20		20		20
מעביר מידע אישי לחו"ל					
כן	21		29	21	21
לא	8	7	9	30	32
לא יודע / מסרב לענות	20		20		

בקרב חברות בענף השירותים ובחברות המעבירות מידע אישי לחו"ל ייצוג בולט למפרסמים את מדיניות שמירת הפרטיות בדף הראשי באתר האינטרנט בחברה.

בקרב ענף בניה ותעשיה מסורתית ייצוג בולט לחברות בהן אין מדיניות כזאת.

Q36. האם יש לחברה בה אתה עובד מדיניות שמירה על הפרטיות ואם כן, היכן היא מפורסמת?



חוק הגנת הפרטיות וקשר עם רשם מאגרי המידע

33

פניות לחברה או לארגון בנושא הגנת הפרטיות וקשר עם הרשם - נעזר
כלל המדגם



- מרבית הארגונים במשק הישראלי לא קיבלו פניות או תלונות מאנשים בנושא הגנת הפרטיות. היו בקשר עם יחידת רשם מאגרי המידע.

Q37. [Q14] האם הופנו לחברה בקשות לעיין או לקבל מידע על בסיס סעיף 13 לחוק הגנת הפרטיות?
Q38. [Q15] האם החברה שלכם קיבלה תלונות מאנשים שעליהם יש לכם מידע בחברה לגבי השימוש שהחברה עושה במידע עליהם?
Q39. [Q12a] האם יש או היה לחברה קשר עם רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע במשרד המשפטים?

34

ShiluvMillwardBrown

קשר עם רשם מאגרי המידע– בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	9	77	13	203
ענף				
בניה ותעשיה מסורתית	4	82	13	45
תעשיה עתירת ידע	9	73	18	22
מסחר	13	80	8	64
שירותים	10	74	17	72
גודל חברה				
עד 20 עובדים	6	88	7	105
מעל 20 עובדים	13	66	20	98
תפקיד בארגון				
ממונה אבטחת מידע	19	58	23	26
מנהל IT	9	68	23	22
מנהל שיווק	6	83	11	18
מנהל כח אדם / משאבי אנוש	4	67	29	24
מנכ"ל	11	85	5	84
מנהל כספים	3	86	10	29
מעביר מידע באינטרנט				
כן	16	69	16	32
לא	8	80	11	166
לא יודע / מסרב לענות		40	60	5
מעביר מידע אישי לחו"ל				
כן		71	29	14
לא	10	80	10	184
לא יודע / מסרב לענות			100	5

בקרב חברות המונות מעל 20 עובדים ובקרב ממונים על אבטחת מידע בארגון, ייצוג גבוה ליוצרי קשר עם הרשם.

Q39. [Q12a] האם יש או היה לחברה קשר עם רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע במשרד המשפטים?

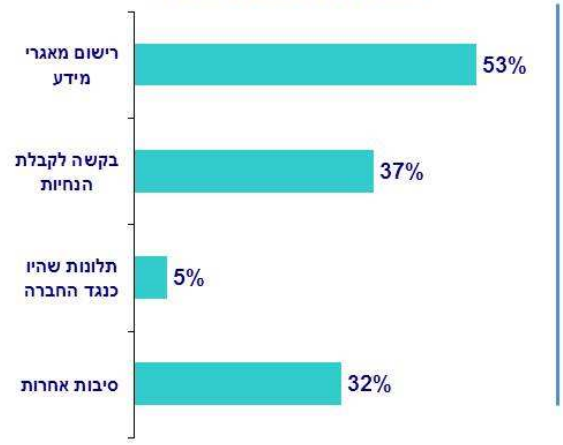
35

ShiluvMillwardBrown

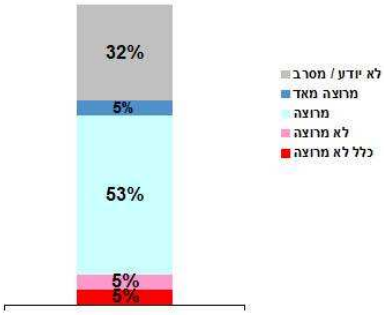
נושאים ליצירת קשר עם יחידת רשם מאגרי המידע ושביעות רצון – נעזר

בקרב יוצרי הקשר עם יחידת הרשם N=19*

נושאים ליצירת קשר עם הרשם:



שביעות רצון מהקשר עם הרשם:



- הסיבה העיקרית ליצירת קשר עם הרשם: רישום מאגרי מידע.
- כ-58% מהפונים ליחידת הרשם מרוצים, מתוכם 5% מרוצים מאד.

Q12b]Q40-43] האם הקשר שיצרה החברה עם הרשם היה בנוגע ל

Q44. מהי מידת שביעות הרצון מהשירות שניתן לכם על ידי יחידת הרשם של מאגרי המידע?

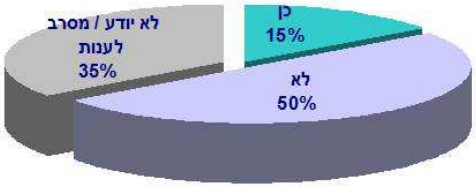
* תא סטטיסטי קטן

36

ShiluvMillwardBrown

רישום מאגרי מידע – נעזר

כלל המדגם



- מרבית מאגרי המידע הקיימים בחברות במשק הישראלי עדיין אינם רשומים אצל רשם מאגרי המידע.

Q45. האם מאגרי המידע של החברה רשומים אצל רשם מאגרי המידע?

ShiluvMillwardBrown

רישום מאגרי המידע– בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	15	50	35	203
ענף				
בניה ותעשיה מסורתית	13	60	27	45
תעשיה עתירת ידע	14	55	32	22
מסחר	14	48	38	64
שירותים	17	43	40	72
גודל חברה				
עד 20 עובדים	14	52	33	105
מעל 20 עובדים	15	47	38	98
תפקיד בארגון				
ממונה אבטחת מידע	23	35	42	26
מנהל IT	14	55	32	22
מנהל שיווק	11	50	39	18
מנהל כח אדם / משאבי אנוש	8	29	63	24
מנכ"ל	15	54	31	84
מנהל כספים	14	66	21	29
מעביר מידע באינטרנט				
כן	22	50	28	32
לא	13	50	37	166
לא יודע / מסרב לענות	20	40	40	5
מעביר מידע אישי לחו"ל				
כן	21	43	36	14
לא	14	51	35	184
לא יודע / מסרב לענות	20	20	60	5

בענף בניה ותעשייה מסורתית ובקרב בעלי התפקידים: מנהל IT, מנכ"ל ומנהל כספים בולט נושא אי רישום מאגרי המידע בחברה אצל רשם מאגרי המידע.

Q45. האם מאגרי המידע של החברה רשומים אצל רשם מאגרי המידע?

ShiluvMillwardBrown



נספח

39

ShiluvMillwardBrown

סיווג החברות והארגונים – בדיקה נעזרת

ניתוח לפי סגמנט

	חברה עצמאית	חברה בתוך אשכול חברות ישראלי	חברה בינלאומית שהנהלתה בישראל	חברה בינלאומית שהנהלתה אינה בישראל	לא יודע / מסרב לענות	סה"כ
% מהמדגם	80	8	7	4		203
ענף						
בניה ותעשיה מסורתית	96	2	2			45
תעשיה עתירת ידע	64	5	14	14	5	22
מסחר	78	11	9	2		64
שירותים	78	10	6	7		72
גודל חברה						
עד 20 עובדים	90	4	5	1		105
מעל 20 עובדים	69	12	9	8	1	98
תפקיד בארגון						
ממונה אבטחת מידע	73	19		4	4	26
מנהל IT	73	5	5	18		22
מנהל שיווק	89		6	6		18
מנהל כח אדם / משאבי אנוש	88		8	4		24
מנכ"ל	80	10	8	2		84
מנהל כספים	83	7	10			29
מעביר מידע אישי באינטרנט						
כן	78	9	6	6		32
לא	81	8	7	4		166
לא יודע / מסרב לענות	80				20	5
מעביר מידע אישי לחו"ל						
כן	71			29		14
לא	82	9	7	3		184
לא יודע / מסרב לענות	60		20		20	5

40

Q4. האם החברה שלכם היא:

ShiluvMillwardBrown

סיווג החברות והארגונים – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	12	82	6	203
ענף				
בניה ותעשיה מסורתית	2	93	4	45
תעשיה עתירת ידע	9	82	9	22
מסחר	17	78	5	64
שירותים	14	79	7	72
גודל חברה				
עד 20 עובדים	4	93	3	105
מעל 20 עובדים	20	70	9	98
תפקיד בארגון				
ממונה אבטחת מידע	23	69	8	26
מנהל IT	9	86	5	22
מנהל שיווק	11	83	6	18
מנהל כח אדם / משאבי אנוש	4	79	17	24
מנכ"ל	10	86	5	84
מנהל כספים	17	83		29
מעביר מידע אישי באינטרנט				
כן	9	84	6	32
לא	12	83	5	166
לא יודע / מסרב לענות	20	60	20	5
מעביר מידע אישי לחו"ל				
כן	14	86		14
לא	11	83	6	184
לא יודע / מסרב לענות	40	40	20	5

41

Q5. האם החברה ציבורית (נסחרת בבורסה)?

ShiluvMillwardBrown

סיווג החברות והארגונים – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	69	30	1	203
ענף				
בניה ותעשיה מסורתית	62	38		45
תעשיה עתירת ידע	91	9		22
מסחר	77	23		64
שירותים	61	36	3	72
גודל חברה				
עד 20 עובדים	66	34		105
מעל 20 עובדים	73	24	2	98
תפקיד בארגון				
ממונה אבטחת מידע	65	35		26
מנהל IT	86	14		22
מנהל שיווק	89	11		18
מנהל כח אדם / משאבי אנוש	63	33	4	24
מנכ"ל	68	31	1	84
מנהל כספים	59	41		29
מעביר מידע אישי באינטרנט				
כן	84	9	6	32
לא	66	34		166
לא יודע / מסרב לענות	80	20		5
מעביר מידע אישי לחו"ל				
כן	71	29		14
לא	69	30	1	184
לא יודע / מסרב לענות	80		20	5

42

Q6. האם החברה מנהלת או ברשותה מידע אישי אודות אנשים באופן ממוחשב (לדוגמה עובדים , לקוחות)?

ShiluvMillwardBrown

גודל מאגר המידע – בדיקה נעזרת

בקרב חברות בעלות מאגרי מידע ניתוח לפי סגמנט

	עד אלף	עד עשרת אלפים	עד מאה אלף איש	עד מיליון איש	מעל מיליון	לא יודע / מסרב לענות	סה"כ
% מחברות בעלות מאגרי מידע	57	18	3	1	1	20	141
ענף							
בניה ותעשיה מסורתית	57	11	11			21	28
תעשיה עתירת ידע	55	15		5		25	20
מסחר	63	20	2			14	49
שירותים	52	23			2	23	44
גודל חברה							
עד 20 עובדים	62	16	3			19	69
מעל 20 עובדים	53	21	3	1	1	21	72
תפקיד בארגון							
ממונה אבטחת מידע	47	18				35	17
מנהל IT	58	16				26	19
מנהל שיווק	44	25				31	16
מנהל כח אדם / משאבי אנוש	53	7	13			27	15
מנכ"ל	65	21	2	2	2	9	57
מנהל כספים	59	18	6			18	17
מעביר מידע אישי באינטרנט							
כן	70	19	4			7	27
לא	55	19	3	1	1	22	110
לא יודע / מסרב לענות	50					50	4
מעביר מידע אישי לחו"ל							
כן	60	30				10	10
לא	58	18	3	1	1	19	127
לא יודע / מסרב לענות	25					75	4

Q7. על כמה אנשים יש מידע במאגרי המידע של החברה?

ShiluvMillwardBrown

היכרות עם חוק הגנת הפרטיות – בדיקה נעזרת

ניתוח לפי סגמנט

	מכיר טוב	מכיר	לא ממש מכיר	לא יודע / מסרב לענות	סה"כ
% מהמדגם	17	28	54		203
ענף					
בניה ותעשיה מסורתית	7	27	67		45
תעשיה עתירת ידע	5	36	59		22
מסחר	22	25	53		64
שירותים	24	29	46	1	72
גודל חברה					
עד 20 עובדים	12	26	62		105
מעל 20 עובדים	22	31	46	1	98
תפקיד בארגון					
ממונה אבטחת מידע	31	27	42		26
מנהל IT	27	23	50		22
מנהל שיווק	22	17	61		18
מנהל כח אדם / משאבי אנוש	8	13	75	4	24
מנכ"ל	14	31	55		84
מנהל כספים	10	45	45		29
מעביר מידע אישי באינטרנט					
כן	22	25	50	3	32
לא	16	29	55		166
לא יודע / מסרב לענות	20	20	60		5
מעביר מידע אישי לחו"ל					
כן	14	29	57		14
לא	17	28	54		184
לא יודע / מסרב לענות	20	20	40	20	5

Q8. [Q1a] עד כמה אתה מכיר את הוראות חוק הגנת הפרטיות בתחום ההגנה על מידע אישי (מאגרי מידע) בישראל?

ShiluvMillwardBrown

ההגנה שמקנה חוק הגנת הפרטיות בישראל – בדיקה נעזרת

ניתוח לפי סגמנט

	גבוהה	בינונית	נמוכה	לא יודע / מסרב לענות	סה"כ
% בקרב מכירי החוק	16	58	16	10	92
ענף					
בניה ותעשיה מסורתית	13	53	27	7	15
תעשיה עתירת ידע	11	44	11	33	9
מסחר	20	57	17	7	30
שירותים	16	63	13	8	38
גודל חברה					
עד 20 עובדים	18	60	13	10	40
מעל 20 עובדים	15	56	19	10	52
תפקיד בארגון					
ממונה אבטחת מידע	7	73	13	7	15
מנהל IT		64	18	18	11
מנהל שיווק	14	57	29		7
מנהל כח אדם / משאבי אנוש	20	60	20		5
מנכ"ל	24	47	16	13	38
מנהל כספים	19	63	13	6	16
מעביר מידע אישי באינטרנט					
כן	7	80	7	7	15
לא	19	53	19	9	75
לא יודע / מסרב לענות		50		50	2
מעביר מידע אישי לחו"ל					
כן		83	17		6
לא	18	56	17	10	84
לא יודע / מסרב לענות		50		50	2

Q9. האם למיטב ידיעתך, חוק הגנת הפרטיות בישראל מקנה לאזרחים הגנה ברמה:

ShiluvMillwardBrown

תפיסת חוק הגנת הפרטיות מנקודת מבט של ניהול עסק – בדיקה נעזרת

ניתוח לפי סגמנט

	מאפשר לנהל עסק כמו שלך	מקשה על ניהול עסק כמו שלך מעל הנדרש	לא יודע / מסרב לענות	סה"כ
% בקרב מכירי החוק	79	14	7	92
ענף				
בניה ותעשיה מסורתית	87	7	7	15
תעשיה עתירת ידע	100			9
מסחר	73	20	7	30
שירותים	76	16	8	38
גודל חברה				
עד 20 עובדים	80	13	8	40
מעל 20 עובדים	79	15	6	52
תפקיד בארגון				
ממונה אבטחת מידע	73	13	13	15
מנהל IT	73	9	18	11
מנהל שיווק	100			7
מנהל כח אדם / משאבי אנוש	60	40		5
מנכ"ל	82	16	3	38
מנהל כספים	81	13	6	16
מעביר מידע אישי באינטרנט				
כן	80	7	13	15
לא	80	16	4	75
לא יודע / מסרב לענות	50		50	2
מעביר מידע אישי לחו"ל				
כן	67	17	17	6
לא	81	14	5	84
לא יודע / מסרב לענות	50		50	2

Q10. מנקודת המבט של ניהול עסק, האם לדעתך חוק הגנת הפרטיות בישראל

ShiluvMillwardBrown

התמודדות החוק להגנת הפרטיות עם העברת מידע בין גורמים שונים – בדיקה נעזרת

ניתוח לפי סגמנט

	במידה טובה מאד	במידה טובה	במידה לא כל כך טובה	במידה כלל לא טובה	לא יודע / מסרב לענות	סה"כ
% מהמדגם	2	25	28	21	24	203
ענף						
בניה ותעשיה מסורתית	4	22	20	27	27	45
תעשיה עתירת ידע		23	27	9	41	22
מסחר	3	27	27	20	23	64
שירותים		26	35	22	17	72
גודל חברה						
עד 20 עובדים	2	26	23	25	25	105
מעל 20 עובדים	2	24	34	17	22	98
תפקיד בארגון						
ממונה אבטחת מידע		19	23	27	31	26
מנהל IT		36	23	9	32	22
מנהל שיווק	6	33	17	33	11	18
מנהל כח אדם / משאבי אנוש	4	29	29	17	21	24
מנכ"ל	1	23	31	24	21	84
מנהל כספים	3	21	34	14	28	29
מעביר מידע אישי באינטרנט						
כן	3	38	34	16	9	32
לא	2	23	27	22	26	166
לא יודע / מסרב לענות		20	20		40	5
מעביר מידע אישי לחו"ל						
כן		29	29	14	29	14
לא	2	25	28	22	23	184
לא יודע / מסרב לענות		20	40		40	5

Q11. [Q4] באיזו מידה לדעתך החוק הישראלי מצליח להתמודד עם התופעה של העברת מידע אישי רב בין גורמים שונים (לדוגמה באמצעות האינטרנט)?

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	הבהרת המגבלות של חוק הגנת הפרטיות על שימוש במידע אישי			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	56	26	18	203
ענף				
בניה ותעשיה מסורתית	67	20	13	45
תעשיה עתירת ידע	55	9	36	22
מסחר	50	31	19	64
שירותים	56	31	14	72
גודל חברה				
עד 20 עובדים	55	27	18	105
מעל 20 עובדים	57	26	17	98
תפקיד בארגון				
ממונה אבטחת מידע	65	12	23	26
מנהל IT	27	41	32	22
מנהל שיווק	44	28	28	18
מנהל כח אדם / משאבי אנוש	75	17	8	24
מנכ"ל	57	27	15	84
מנהל כספים	59	31	10	29
מעביר מידע אישי באינטרנט				
כן	59	25	16	32
לא	56	27	17	166
לא יודע / מסרב לענות	40	20	40	5
מעביר מידע אישי לחו"ל				
כן	50	21	29	14
לא	57	27	16	184
לא יודע / מסרב לענות	60		40	5

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי: אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שישארו כמות שהן: הבהרת המגבלות של חוק הגנת הפרטיות על שימוש במידע אישי

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	הבהרת חובת הרישום ותהליך רישום של מאגרי מידע			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	44	33	23	203
ענף				
בניה ותעשיה מסורתית	40	33	27	45
תעשיה עתירת ידע	41	27	32	22
מסחר	44	36	20	64
שירותים	49	31	21	72
גודל חברה				
עד 20 עובדים	44	31	25	105
מעל 20 עובדים	45	34	21	98
תפקיד בארגון				
ממונה אבטחת מידע	46	27	27	26
מנהל IT	36	36	27	22
מנהל שיווק	33	39	28	18
מנהל כח אדם / משאבי אנוש	46	29	25	24
מנכ"ל	51	27	21	84
מנהל כספים	34	48	17	29
מעביר מידע אישי באינטרנט				
כן	47	38	16	32
לא	45	31	24	166
לא יודע / מסרב לענות		60	40	5
מעביר מידע אישי לחו"ל				
כן	36	43	21	14
לא	46	32	23	184
לא יודע / מסרב לענות	20	40		5

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יובהרו את משמעותן או שיישארו כמות שהן: הבהרת חובת הרישום ותהליך רישום מאגרי מידע

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	קביעת נורמות מחייבות בנושא אבטחת מידע			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	65	20	16	203
ענף				
בניה ותעשיה מסורתית	58	27	16	45
תעשיה עתירת ידע	73	9	18	22
מסחר	66	19	16	64
שירותים	65	19	15	72
גודל חברה				
עד 20 עובדים	61	24	15	105
מעל 20 עובדים	68	15	16	98
תפקיד בארגון				
ממונה אבטחת מידע	65	8	27	26
מנהל IT	68	18	14	22
מנהל שיווק	72	11	17	18
מנהל כח אדם / משאבי אנוש	58	25	17	24
מנכ"ל	62	24	14	84
מנהל כספים	69	21	10	29
מעביר מידע אישי באינטרנט				
כן	59	22	19	32
לא	66	19	14	166
לא יודע / מסרב לענות	40	20	40	5
מעביר מידע אישי לחו"ל				
כן	64	7	29	14
לא	65	21	14	184
לא יודע / מסרב לענות	60		40	5

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יובהרו את משמעותן או שיישארו כמות שהן: קביעת נורמות מחייבות בנושא אבטחת מידע

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	חקיקה ספציפית להוראות הנוגעות לעיבוד מידע אישי לפי סקטורים			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	42	30	28	203
ענף				
בניה ותעשיה מסורתית	47	20	33	45
תעשיה עתירת ידע	18	45	36	22
מסחר	41	34	25	64
שירותים	47	28	25	72
גודל חברה				
עד 20 עובדים	38	30	31	105
מעל 20 עובדים	46	30	24	98
תפקיד בארגון				
ממונה אבטחת מידע	54	12	35	26
מנהל IT	36	32	32	22
מנהל שיווק	44	33	22	18
מנהל כח אדם / משאבי אנוש	50	13	38	24
מנכ"ל	39	37	24	84
מנהל כספים	34	38	28	29
מעביר מידע אישי באינטרנט				
כן	41	34	25	32
לא	42	30	28	166
לא יודע / מסרב לענות	40		60	5
מעביר מידע אישי לחו"ל				
כן	50	14	36	14
לא	41	32	27	184
לא יודע / מסרב לענות	60		40	5

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן: חקיקה ספציפית להוראות הנוגעות לעיבוד מידע אישי לפי סקטורים

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	נושא אחר			
	רוצה שיובהר	מעדיף שיישארו כמו שהן	לא יודע / מסרב לענות	סה"כ
% מהמדגם	21	25	54	203
ענף				
בניה ותעשיה מסורתית	31	13	56	45
תעשיה עתירת ידע	14	9	77	22
מסחר	16	34	50	64
שירותים	21	29	50	72
גודל חברה				
עד 20 עובדים	23	24	53	105
מעל 20 עובדים	18	27	55	98
תפקיד בארגון				
ממונה אבטחת מידע	23	12	65	26
מנהל IT	23	23	55	22
מנהל שיווק	17	39	44	18
מנהל כח אדם / משאבי אנוש	21	21	58	24
מנכ"ל	21	30	49	84
מנהל כספים	17	21	62	29
מעביר מידע אישי באינטרנט				
כן	25	25	50	32
לא	20	25	54	166
לא יודע / מסרב לענות		20	80	5
מעביר מידע אישי לחו"ל				
כן	14	7	79	14
לא	21	27	52	184
לא יודע / מסרב לענות	40		60	5

Q12. אקריא לך רשימה של פעולות לגבי כל אחת אמור לי אם היית מעדיף שבמסגרת חוק הגנת הפרטיות היית מעדיף שישפרו או יבהירו את משמעותן או שיישארו כמות שהן: נושא אחר

ShiluvMillwardBrown

הגנה על מידע אישי בתוך הארגון – בדיקה נעזרת

ניתוח לפי סגמנט

	כן, באופן קבוע	כן, לעיתים	לא	לא יודע / מסרב לענות	סה"כ
% כלל המדגם	39	22	19	20	203
ענף					
בניה ותעשיה מסורתית	29	22	27	22	45
תעשיה עתירת ידע	41	27	9	23	22
מסחר	33	25	19	23	64
שירותים	50	18	18	14	72
גודל חברה					
עד 20 עובדים	30	25	24	22	105
מעל 20 עובדים	49	19	14	17	98
תפקיד בארגון					
ממונה אבטחת מידע	54	12	15	19	26
מנהל IT	45	18	18	18	22
מנהל שיווק	56	28	11	6	18
מנהל כח אדם / משאבי אנוש	29	21	21	29	24
מנכ"ל	33	27	20	19	84
מנהל כספים	34	17	24	24	29
מעביר מידע אישי באינטרנט					
כן	38	38	16	9	32
לא	40	20	19	20	166
לא יודע / מסרב לענות			40	60	5
מעביר מידע אישי לחו"ל					
כן	50	14	29	7	14
לא	38	23	18	20	184
לא יודע / מסרב לענות	40		20	40	5

Q13. האם בשלב האפיון, הפיתוח והיישום של שירותי מידע המשרתים את פעילות החברה נבחנים שיקולים של הגנת המידע האישי המוחזק בחברה?

ShiluvMillwardBrown

שימוש בחומרות ותוכנות להגברת הגנת הפרטיות – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא, אבל שמעתי על התחום	לא, ומעולם לא שמעתי על התחום	לא יודע / מסרב לענות	סה"כ
% כלל המדגם	49	18	29	4	203
ענף					
בניה ותעשיה מסורתית	42	16	36	7	45
תעשיה עתירת ידע	59	27	5	9	22
מסחר	44	27	28	2	64
שירותים	56	8	32	4	72
גודל חברה					
עד 20 עובדים	44	16	35	5	105
מעל 20 עובדים	55	19	21	4	98
תפקיד בארגון					
ממונה אבטחת מידע	62	8	27	4	26
מנהל IT	50	23	18	9	22
מנהל שיווק	39	22	28	11	18
מנהל כח אדם / משאבי אנוש	33	21	38	8	24
מנכ"ל	51	17	30	2	84
מנהל כספים	52	21	28		29
מעביר מידע אישי באינטרנט					
כן	56	16	25	3	32
לא	48	19	28	5	166
לא יודע / מסרב לענות	40		60		5
מעביר מידע אישי לחו"ל					
כן	43	21	29	7	14
לא	50	18	28	4	184
לא יודע / מסרב לענות	40		40	20	5

Q14. [SQ] האם אתם משתמשים במוצרי חומרה או תוכנה המגבירים את הגנת הפרטיות במאגר המידע בחברה שלכם (לדוגמא, הצפנות, אנונימיזציה אוטומטית, מערכות בקרת שימוש במידע) מה שמכונה "טכנולוגיות מקדמות פרטיות"?

ShiluvMillwardBrown

העברת מידע אישי באמצעות האינטרנט – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	16	82	2	203
ענף				
בניה ותעשיה מסורתית	13	87		45
תעשיה עתירת ידע	9	86	5	22
מסחר	13	83	5	64
שירותים	22	76	1	72
גודל חברה				
עד 20 עובדים	16	81	3	105
מעל 20 עובדים	15	83	2	98
תפקיד בארגון				
ממונה אבטחת מידע	23	69	8	26
מנהל IT	23	77		22
מנהל שיווק	11	83	6	18
מנהל כח אדם / משאבי אנוש	17	83		24
מנכ"ל	14	85	1	84
מנהל כספים	10	86	3	29
מעביר מידע אישי לחו"ל				
כן	71	29		14
לא	11	88	1	184
לא יודע / מסרב לענות	20	20	60	5

Q15. [Q6] האם החברה שלכם מעבירה מידע אישי על אנשים לגורם אחר באמצעות האינטרנט או בדרכים אחרות?

55

ShiluvMillwardBrown

העברת מידע אישי על אנשים לחו"ל – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	7	91	2	203
ענף				
בניה ותעשיה מסורתית	4	96		45
תעשיה עתירת ידע	9	86	5	22
מסחר	5	94	2	64
שירותים	10	86	4	72
גודל חברה				
עד 20 עובדים	8	91	1	105
מעל 20 עובדים	6	90	4	98
תפקיד בארגון				
ממונה אבטחת מידע	8	85	8	26
מנהל IT	9	91		22
מנהל שיווק	17	78	6	18
מנהל כח אדם / משאבי אנוש	4	92	4	24
מנכ"ל	5	95		84
מנהל כספים	7	90	3	29
מעביר מידע באינטרנט				
כן	31	66	3	32
לא	2	97	1	166
לא יודע / מסרב לענות		40	60	5

Q16. [Q7] האם החברה שלך מעבירה בדרך כלל מידע אישי על אנשים לחו"ל?

56

ShiluvMillwardBrown

הגנה על מידע אישי בהעברת מידע – בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% בקרב חברות שמעבירות מידע באינטרנט או מעבירות מידע לחו"ל	56	31	14	36
ענף				
בניה ותעשיה מסורתית	67	33		6
תעשיה עתירת ידע	100			3
מסחר	50	30	20	10
שירותים	47	35	18	17
גודל חברה				
עד 20 עובדים	67	17	17	18
מעל 20 עובדים	44	44	11	18
תפקיד בארגון				
ממונה אבטחת מידע	33	50	17	6
מנהל IT	29	43	29	7
מנהל שיווק	100			3
מנהל כח אדם / משאבי אנוש	25	50	25	4
מנכ"ל	77	23		13
מנהל כספים	67		33	3
מעביר מידע אישי באינטרנט				
כן	53	31	16	32
לא	75	25		4
לא יודע / מסרב לענות				
מעביר מידע אישי לחו"ל				
כן	79	14	7	14
לא	43	43	14	21
לא יודע / מסרב לענות			100	1

Q17. [Q7] האם החברה נוקטת באמצעים כדי למנוע שימוש במידע אישי השונה מהמטרה לשמה הוא נמסר על ידם?

ShiluvMillwardBrown

אמצעי הגנה על מידע אישי שמועבר לגורם שלישי – בדיקה נעזרת

בקרב מעבירי מידע ניתוח לפי סגמנט

	אמצעים משפטיים	אמצעים טכנולוגיים	אמצעים נוהליים	סה"כ
% בקרב נוקטים באמצעי הגנה	60	80	85	20
ענף				
בניה ותעשיה מסורתית	75	50	75	4
תעשיה עתירת ידע		100	100	3
מסחר	80	80	80	5
שירותים	63	88	88	8
גודל חברה				
עד 20 עובדים	58	75	75	12
מעל 20 עובדים	63	88	100	8
תפקיד בארגון				
ממונה אבטחת מידע	50	50	100	2
מנהל IT	50	100	50	2
מנהל שיווק		100	100	3
מנהל כח אדם / משאבי אנוש		100	100	1
מנכ"ל	80	80	80	10
מנהל כספים	100	50	100	2
מעביר מידע אישי באינטרנט				
כן	59	76	82	17
לא	67	100	100	3
לא יודע / מסרב לענות				
מעביר מידע אישי לחו"ל				
כן	55	82	100	11
לא	67	78	67	9
לא יודע / מסרב לענות				

Q18-20. באילו אמצעים החברה נוקטת?

ShiluvMillwardBrown

הגנה על הפרטיות בהעברת מידע לצד שלישי – בדיקה נעזרת

ניתוח לפי סגמנט

	כן, ומקבלים את הסכמתו מראש	כן	לא	לא יודע / מסרב לענות	סה"כ
% בקרב מעבירי מידע	39	33	25	3	36
ענף					
בניה ותעשיה מסורתית	17	17	67		6
תעשיה עתירת ידע		67		33	3
מסחר	50	20	30		10
שירותים	47	41	12		17
גודל חברה					
עד 20 עובדים	28	39	28	6	18
מעל 20 עובדים	50	28	22		18
תפקיד בארגון					
ממונה אבטחת מידע	50	33	17		6
מנהל IT	57	29	14		7
מנהל שיווק	33	33		33	3
מנהל כח אדם / משאבי אנוש	50	25	25		4
מנכ"ל	31	31	38		13
מנהל כספים		67	33		3
מעביר מידע אישי באינטרנט					
כן	41	28	28	3	32
לא	25	75			4
לא יודע / מסרב לענות					
מעביר מידע אישי לחו"ל					
כן	21	43	29	7	14
לא	48	29	24		21
לא יודע / מסרב לענות	100				1

Q21. כאשר אתם מעבירים מידע על אדם לגורם שלישי, האם האדם עליו מועבר המידע מיודע על כך?

ShiluvMillwardBrown

סוגי המידע המועברים לגורמים אחרים בארץ ובחו"ל – בדיקה נעזרת

ניתוח לפי סגמנט

	מידע הנדרש לניהול משאבי אנוש	מידע על צרכנים או לקוחות למטרות שיווק	מידע שאספתם לצרכיו של הגורם אליו העבר המידע	מידע הנדרש לצורך אספקת שירותי החברה לאדם	מידע אחר	סה"כ
% בקרב מעבירי מידע	39	50	39	61	25	36
ענף						
בניה ותעשיה מסורתית	50	83	67	83	33	6
תעשיה עתירת ידע	67	67	67	100		3
מסחר	20	60	20	40	20	10
שירותים	41	29	35	59	29	17
גודל חברה						
עד 20 עובדים	33	61	39	61	28	18
מעל 20 עובדים	44	39	39	61	22	18
תפקיד בארגון						
ממונה אבטחת מידע	17			50	17	6
מנהל IT	14	29	29	43	14	7
מנהל שיווק	33	67	100	100		3
מנהל כח אדם / משאבי אנוש	100	50	25	50		4
מנכ"ל	46	69	46	62	46	13
מנהל כספים	33	100	67	100	33	3
מעביר מידע אישי באינטרנט						
כן	41	50	34	63	28	32
לא	25	50	75	50		4
לא יודע / מסרב לענות						
מעביר מידע אישי לחו"ל						
כן	36	57	57	57	14	14
לא	38	48	29	62	33	21
לא יודע / מסרב לענות	100	100			100	1

Q22-27. [Q9] לגבי כל אחד מסוגי המידע הבאים, אמור האם החברה בה אתה עובד מעבירה לגורמים אחרים בארץ ובחו"ל מידע מסוג זה?

ShiluvMillwardBrown

התמודדות החוק להגנת הפרטיות עם העברת מידע בין גורמים שונים – בדיקה נעזרת

ניתוח לפי סגמנט

	באמצעות הטלפון	באמצעות פקס	בדואר רשום או שירות שליחים	בדואר רגיל	בדואר אלקטרוני	באמצעות רשת סגורה או מוצפנת	באמצעות רשת האינטרנט	באמצעים אחרים	סה"כ
% משיבי כן בקרב מעבירי מידע	61	47	47	33	69	33	56	17	36
ענף									
בניה ותעשיה מסורתית	100	67	33	33	67		33		6
תעשיה עתירת ידע	100	100	67	33	67	33	67		3
מסחר	70	50	40	50	60	30	40	10	10
שירותים	35	29	53	24	76	47	71	29	17
גודל חברה									
עד 20 עובדים	67	56	33	22	72	28	50	17	18
מעל 20 עובדים	56	39	61	44	67	39	61	17	18
תפקיד בארגון									
ממונה אבטחת מידע	33	17	17	33	67	50	50	33	6
מנהל IT	14	14	29	14	57	29	57		7
מנהל שיווק	67	67	67	33	100	33	33		3
מנהל כח אדם / משאבי אנוש	75	75	50	25	75		75		4
מנכ"ל	92	54	62	54	62	38	54	23	13
מנהל כספים	67	100	67		100	33	67	33	3
מעביר מידע אישי באינטרנט									
כן	63	47	47	31	66	28	50	19	32
לא	50	50	50	50	100	75	100		4
לא יודע / מסרב לענות									
מעביר מידע אישי לחו"ל									
כן	57	57	43	36	86	36	50	14	14
לא	67	43	52	33	62	33	62	19	21
לא יודע / מסרב לענות									1

Q28-35. [Q10] לגבי כל אחד מסוגי המידע הבאים, אמור האם החברה בה אתה עובד מעבירה לגורמים אחרים בארץ ובחו"ל מידע מסוג זה?

ShiluvMillwardBrown

מדיניות הגנת הפרטיות ושקיפות לגביה בארגון – בדיקה נעזרת

ניתוח לפי סגמנט

	בדף הראשי באתר האינטרנט של החברה	יש קישור כלשהו למדיניות במקום כלשהו באתר החברה	במקום אחר	המדיניות אינה מפורסמת ברבים	אין מדיניות כזו	לא יודע / מסרב לענות	סה"כ
% כלל המדגם	9	6	11	29	31	15	203
ענף							
בניה ותעשיה מסורתית	7	2	16	20	42	13	45
תעשיה עתירת ידע	5	5	14	27	32	18	22
מסחר	3	11	8	36	33	9	64
שירותים	17	4	10	29	21	19	72
גודל חברה							
עד 20 עובדים	10	5	8	32	32	13	105
מעל 20 עובדים	8	7	14	26	29	16	98
תפקיד בארגון							
ממונה אבטחת מידע	15	4	19	27	23	12	26
מנהל IT	9	5	14	45	9	18	22
מנהל שיווק	6			33	44	17	18
מנהל כח אדם / משאבי אנוש	13	4	17	25	13	29	24
מנכ"ל	10	10	11	29	29	13	84
מנהל כספים		3	3	21	66	7	29
מעביר מידע אישי באינטרנט							
כן	9	13	19	38	9	13	32
לא	8	5	9	28	35	14	166
לא יודע / מסרב לענות	20		20		20	40	5
מעביר מידע אישי לחו"ל							
כן	21		29	21	21	7	14
לא	8	7	9	30	32	14	184
לא יודע / מסרב לענות	60			20		20	5

Q36. האם יש לחברה בה אתה עובד מדיניות שמירה על הפרטיות ואם כן, היכן היא מפורסמת?

ShiluvMillwardBrown

תפיסת בהירות החוק להגנת הפרטיות– בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	4	68	28	203
ענף				
בניה ותעשיה מסורתית	2	73	24	45
תעשיה עתירת ידע		55	45	22
מסחר	5	67	28	64
שירותים	7	69	24	72
גודל חברה				
עד 20 עובדים	6	70	24	105
מעל 20 עובדים	3	65	32	98
תפקיד בארגון				
ממונה אבטחת מידע		73	27	26
מנהל IT	5	68	27	22
מנהל שיווק	6	56	39	18
מנהל כח אדם / משאבי אנוש	4	58	38	24
מנכ"ל	5	74	21	84
מנהל כספים	7	62	31	29
מעביר מידע באינטרנט				
כן	3	47	50	32
לא	5	72	23	166
לא יודע / מסרב לענות		60	40	5
מעביר מידע אישי לחו"ל				
כן		36	64	14
לא	5	71	24	184
לא יודע / מסרב לענות		40	60	5

Q37. [Q14] האם הופנו לחברה בקשות לעיין או לקבל מידע על בסיס סעיף 13 לחוק הגנת הפרטיות?

ShiluvMillwardBrown

תלונות על פגיעה בפרטיות בעקבות החוק– בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	1	94	5	203
ענף				
בניה ותעשיה מסורתית	2	96	2	45
תעשיה עתירת ידע		82	18	22
מסחר	2	98		64
שירותים	1	92	7	72
גודל חברה				
עד 20 עובדים	3	94	3	105
מעל 20 עובדים		93	7	98
תפקיד בארגון				
ממונה אבטחת מידע		85	15	26
מנהל IT		100		22
מנהל שיווק		94	6	18
מנהל כח אדם / משאבי אנוש	4	92	4	24
מנכ"ל	2	95	2	84
מנהל כספים		93	7	29
מעביר מידע באינטרנט				
כן		91	9	32
לא	2	95	3	166
לא יודע / מסרב לענות		60	40	5
מעביר מידע אישי לחו"ל				
כן		86	14	14
לא	2	95	3	184
לא יודע / מסרב לענות		60	40	5

Q38. [Q15] האם החברה שלכם קיבלה תלונות מאנשים שעליהם יש לכם מידע בחברה לגבי השימוש שהחברה עושה במידע עליהם?

ShiluvMillwardBrown

קשר עם רשם מאגרי המידע– בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	9	77	13	203
ענף				
בניה ותעשיה מסורתית	4	82	13	45
תעשיה עתירת ידע	9	73	18	22
מסחר	13	80	8	64
שירותים	10	74	17	72
גודל חברה				
עד 20 עובדים	6	88	7	105
מעל 20 עובדים	13	66	20	98
תפקיד בארגון				
ממונה אבטחת מידע	19	58	23	26
מנהל IT	9	68	23	22
מנהל שיווק	6	83	11	18
מנהל כח אדם / משאבי אנוש	4	67	29	24
מנכ"ל	11	85	5	84
מנהל כספים	3	86	10	29
מעביר מידע באינטרנט				
כן	16	69	16	32
לא	8	80	11	166
לא יודע / מסרב לענות		40	60	5
מעביר מידע אישי לחו"ל				
כן		71	29	14
לא	10	80	10	184
לא יודע / מסרב לענות			100	5

Q39. [Q12a] האם יש או היה לחברה קשר עם רשם מאגרי המידע ברשות למשפט, טכנולוגיה ומידע במשרד המשפטים?

ShiluvMillwardBrown

סיבות ליצירת קשר עם הרשם – בדיקה נעזרת

בקרב יוצרי הקשר עם הרשם ניתוח לפי סגמנט

	רישום מאגרי מידע	בקשה לקבלת הנחיות	תלונות שהיו כנגד החברה שלך	סיבות אחרות	סה"כ
% בקרב יוצרי הקשר משיבי כן	53	37	5	32	19
ענף					
בניה ותעשיה מסורתית	50	50			2
תעשיה עתירת ידע				50	2
מסחר	50	38		38	8
שירותים	71	43	14	29	7
גודל חברה					
עד 20 עובדים	17	33		17	6
מעל 20 עובדים	69	38	8	38	13
תפקיד בארגון					
ממונה אבטחת מידע	80	40		20	5
מנהל IT				50	2
מנהל שיווק	100				1
מנהל כח אדם / משאבי אנוש					1
מנכ"ל	44	56	11	33	9
מנהל כספים	100			100	1
מעביר מידע אישי באינטרנט					
כן	60	40	20	60	5
לא	50	36		21	14
לא יודע / מסרב לענות					
מעביר מידע אישי לחו"ל					
כן					
לא	53	37	5	32	19
לא יודע / מסרב לענות					

Q40-43. [Q12b] האם הקשר שיצרה החברה עם הרשם היה בנוגע ל:

ShiluvMillwardBrown

שביעות רצון מהשירות ביחידת הרשם – בדיקה נעזרת

בקרב יוצרי הקשר עם הרשם ניתוח לפי סגמנט

	מרוצה מאד	מרוצה	לא כל כך מרוצה	לא מרוצה בכלל	לא יודע / מסרב לענות	סה"כ
% בקרב יוצרי הקשר	5	53	5	5	32	19
ענף						
בניה ותעשיה מסורתית		50			50	2
תעשיה עתירת ידע		50			50	2
מסחר		63	13	13	13	8
שירותים	14	43			43	7
גודל חברה						
עד 20 עובדים		67			33	6
מעל 20 עובדים	8	46	8	8	31	13
תפקיד בארגון						
ממונה אבטחת מידע		20		20	60	5
מנהל IT		50			50	2
מנהל שיווק		100				1
מנהל כח אדם / משאבי אנוש		100				1
מנכ"ל	11	56		11	22	9
מנהל כספים		100				1
מעביר מידע אישי באינטרנט						
כן	20	40			40	5
לא		57	7	7	29	14
לא יודע / מסרב לענות						
מעביר מידע אישי לחו"ל						
כן						
לא	5	53	5	5	32	19
לא יודע / מסרב לענות						

Q44. מהי מידת שביעות הרצון מהשירות שניתן לכם על ידי יחידת הרשם של מאגרי המידע?

ShiluvMillwardBrown

רישום מאגרי המידע– בדיקה נעזרת

ניתוח לפי סגמנט

	כן	לא	לא יודע / מסרב לענות	סה"כ
% מהמדגם	15	50	35	203
ענף				
בניה ותעשיה מסורתית	13	60	27	45
תעשיה עתירת ידע	14	55	32	22
מסחר	14	48	38	64
שירותים	17	43	40	72
גודל חברה				
עד 20 עובדים	14	52	33	105
מעל 20 עובדים	15	47	38	98
תפקיד בארגון				
ממונה אבטחת מידע	23	35	42	26
מנהל IT	14	55	32	22
מנהל שיווק	11	50	39	18
מנהל כח אדם / משאבי אנוש	8	29	63	24
מנכ"ל	15	54	31	84
מנהל כספים	14	66	21	29
מעביר מידע באינטרנט				
כן	22	50	28	32
לא	13	50	37	166
לא יודע / מסרב לענות	20	40	40	5
מעביר מידע אישי לחו"ל				
כן	21	43	36	14
לא	14	51	35	184
לא יודע / מסרב לענות	20	20	60	5

Q45. האם מאגרי המידע של החברה רשומים אצל רשם מאגרי המידע?

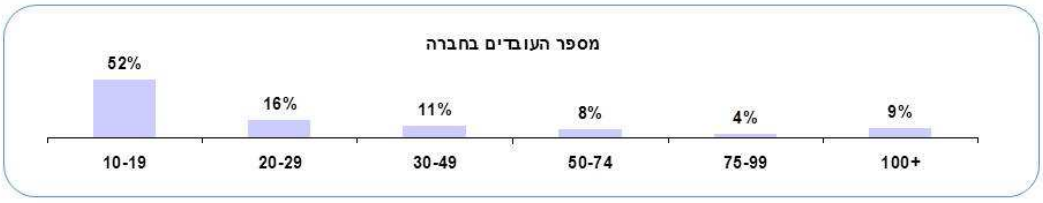
ShiluvMillwardBrown

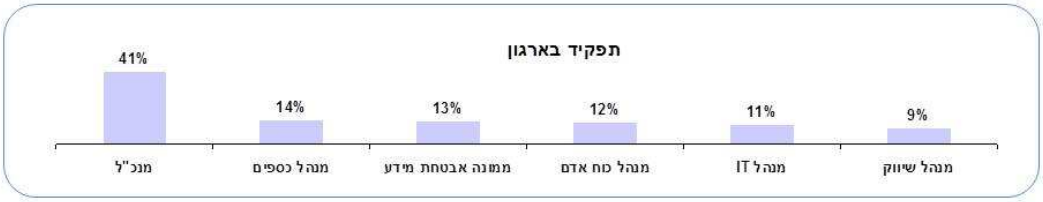


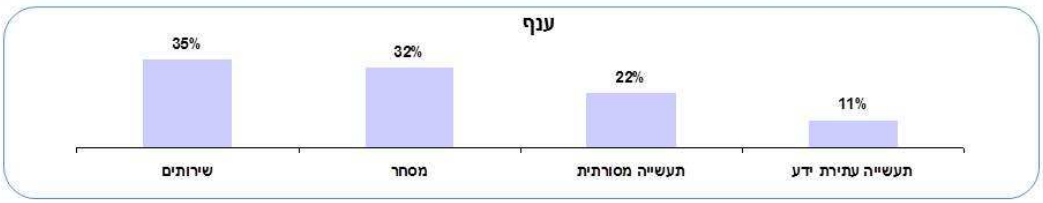
נתוני רקע על המדגם

69

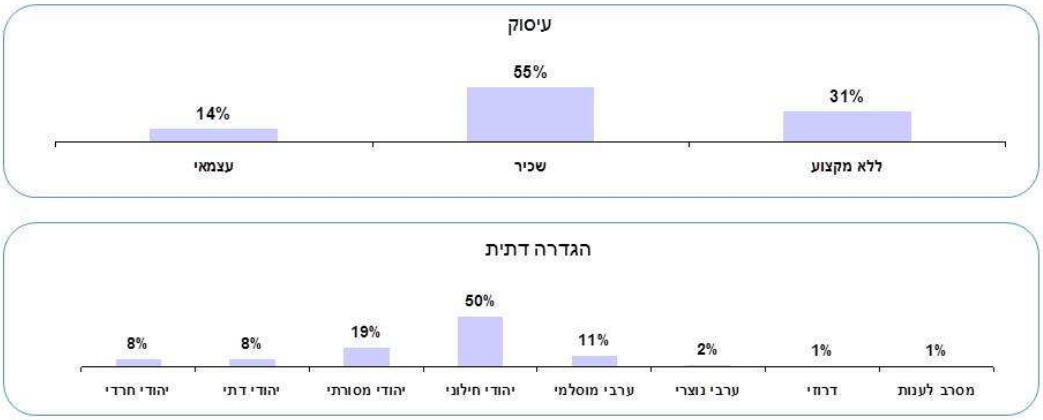
ShiluvMillwardBrown







70


עיסוק
14%
55%
31%
עצמאי
שכיר
ללא מקצוע
הגדרה דתית
8%
8%
19%
50%
11%
2%
1%
1%
יהודי חרדי
יהודי דתי
יהודי מסורתי
יהודי חילוני
ערבי מוסלמי
ערבי נוצרי
דרוזי
מסרב לענות

59

טו. נספח ה' - החלטת Working Party 29 לגבי עמידת ישראל בהוראות הדירקטיבה האירופית להגנת מידע אישי

ARTICLE 29 DATA PROTECTION WORKING PARTY

02316/09/EN
WP 165

Opinion 6/2009 on the level of protection of personal data in Israel

Adopted on 1 December 2009

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

The Working Party on the protection of individuals with regard to the processing of personal data

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "the Directive") and in particular Article 29 and Article 30 (1) (b) thereof,

Having regard to the Rules of Procedure of the Working Party, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. BACKGROUND

On 12 July 2007, the Israeli Mission to the European Union requested the Commission to launch the procedure to declare Israel as a country that ensures an adequate level of protection for the purposes provided for in Articles 25 and 26 of the Directive.

In order to examine Israel's adequacy, the Commission requested the Centre de Recherches Informatique et Droit (hereinafter "CRID") from Namur University to produce an extensive report which analysed the extent to which the Israeli regulatory system fulfilled the requirements for the application of the personal data protection regulations set out in the Working Document "Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection Directive", adopted by the Working Party set up under Article 29 of the Directive on 24 July 1998 (document WP12).

The aforementioned report, together with the preliminary response to the same from the Israeli authorities, was discussed by the Safe Harbour Subgroup during a meeting held on 18 March 2009.

At that meeting, the Subgroup submitted to the Working Party for an opinion a proposal that its President should send a letter to the Israeli authorities which, while positively assessing the existing data protection scheme in Israel, would emphasize those issues that required further clarification.

On 2 September 2009, the Israeli authorities sent, through the Israeli Law, Information and Technology Authority (hereinafter "ILITA"), an extensive report to the Working Party, in which they responded to the issues raised in the said letter.

This report has been analysed by the members of the Subgroup, and was also the subject of a meeting to hear the aforementioned authorities, which was held on 16 September 2009. During that meeting, the members of the Subgroup requested the Israeli authorities, represented by the Head of ILITA and the Head of its Legal Department, to clarify those issues that, following the earlier discussion of the report sent to the Subgroup, still needed further clarification.

The Subgroup informed the Working Party, during its meeting held on 12 and 13 October 2009, of the conclusions reached at the meeting of 16 September, and proposed the adoption of the present Opinion, under the terms contained herein. The proposal was approved by the Working Party at the aforementioned meeting.

2. LAW ON DATA PROTECTION IN ISRAEL

The Israeli legal system is characterized by two key elements which distinguish it from other legal systems and, in particular, from those of the Member States: firstly, Israel does not have a written Constitution; secondly, although its system may be considered as fundamentally linked to those systems that are based on Common Law, it also includes certain characteristics which point to the influence of Continental Law.

The absence of a written Constitution is complemented by the existence of the so called "Basic laws" which have been given constitutional status by the Supreme Court of Israel. At the same time, certain basic principles and fundamental human rights, such as equality, freedom of speech or freedom of religion, also have constitutional status.

Within this framework, the right to privacy is included under section 7 of the Basic Law: Human Dignity and Liberty, which establishes the following:

> *(a) All persons have the right to privacy and to intimacy.*
> *(b) There shall be no entry into the private premises of a person who has not consented thereto.*
> *(c) No search shall be conducted on the private premises of a person, nor in the body or personal effects.*
> *(d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.*

At the same time, the right to privacy and to the protection of personal data is regulated by the Privacy Protection Act (hereinafter the "PPA"), passed in 1981 and subject to amendments on nine subsequent occasions. The most relevant amendment was passed in 2007 and it established new requirements for the processing of personal data, and regulated the organization, powers and functions of the supervising authority in matters of personal data protection in greater detail and with greater precision than the existing legislation up to that date, creating an Authority within the Ministry of Justice - namely the Israeli Law, Information and Technology Authority (ILITA) - which includes the previous Database Registrar.

In addition, due attention has to be paid to a report drafted in January 2007 by a Committee of Experts appointed by the Ministry of Justice, known as the "Schoffman Report", which made a set of recommendations for amending the data protection legislation which are currently being considered for the purposes of adopting a new data protection framework.

Lastly, the data protection legislation is complemented, with respect to the written law, by several decisions adopted by the Israeli Government, specifically with regard to the implementation of the PPA (for example, on international data transfers) as well as to the organization and functioning of ILITA (for example, with respect to the duration and causes for the termination of the mandate of the head of ILITA).

Furthermore, as indicated previously, the Israeli legal system shares, to a great extent, the principles that are characteristic of the Common Law systems. This is why written regulatory provisions must, in any event, be supplemented by the judgments adopted in accordance with them, which have the value of precedent and directly form part of the Israeli sources of law. The report requested by the Committee and issued by the Israeli authorities, as well as the statements made by the latter during the hearing held by the Subgroup on 16 September 2009, have provided the Working Party with a large number of judicial resolutions which have to be taken into consideration in the assessment to be conducted by the Working Party.

Lastly, in this preliminary assessment, it must be pointed out that Israel has ratified the International Covenant on Civil and Political Rights of 1966, although in Israeli law, ratification of an International Agreement does not mean that it is directly incorporated into domestic law.

3. ASSESSMENT OF THE DATA PROTECTION LAW OF ISRAEL AS PROVIDING ADEQUATE PROTECTION OF PERSONAL DATA

The Working Party points out that its assessment on the adequacy of the Law on data protection in Israel focuses on the Privacy Protection Act (PPA).

This Act's provisions, as well as the case law made by the courts with regard to the protection of personal data, have been compared with the main provisions of the Directive, taking into account opinion WP12 of the Working Party. This opinion lists a number of principles which constitute *a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate.*

3.1 Scope of the regulating rules on data protection within the Israeli law.

As on certain previous ocassions, the Working Party believes that it is necessary, before proceeding to the specific assessment of the fulfilment of the principles settled in the document WP12, to examine the scope of application of the regulation on data protection within Israeli law.

a) Concept of personal data or "information".

In particular, the Working Party believes that it is necessary to take into account the concept of the term "personal information" referred to in the PPA and its link to the concept of "personal data" provided in the Directive. Likewise, it will be necessary to determine whether Israeli law establishes the appropriate safeguards on data protection in relation to any processing or if the said regulation is only applicable to total or partial automated processing systems, taking into account the framework of protection established through the Directive.

In relation to the first issue, the Working Party confirms that the definition of "information" referred to in section 7 of the PPA is not similar to the definition set out in the Directive. Thus, the aforementioned rule states that *"information means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person"*. The definition refers solely to certain data categories and does not allow to know if information regarding a non-identified but identifiable person would be protected under the PPA.

Nonetheless, the Working Party takes into account the explanations given on this issue by the Israeli authorities and, in particular, the judicial precedents provided by them which imply an extension of the legal concept of information, making it similar to the concept of *"data of a personal nature"* within the meaning of the Directive.

In particular, this conclusion is reached in view of certain rulings, such as the one pronounced by Israel´s Supreme Court in the case of *Israel v. Bank Ha'Po'alim*, which states that *"the term information (...) should include data that can be derived from a database which is not indexed according to individual names"*.

The Working Party, in addition to the rest of the rulings provided, considers as especially relevant the case-law arising out of the judgment *Rani Mor v. Ynet* of the District Court of Haifa, referring to the IP address, where the conclusion reached can be assimilated to that held by the Working Party, by indicating that *"Identifying an online user by disclosing his or her IP address without consent may constitute a tort of infringement of privacy"*.

Therefore, with regard to the concept of personal data or "information" for the purpose of the application of the regulation on data protection, the Working Party believes that the case law has supplemented what was established by the PPA, making it possible from this perspective to consider the safeguards offered by this Law as constituting a protective framework, as regards the concept of personal data, similar to the one provided by the Directive.

b) Protected processing systems in Israeli law.

The Working Party has to refer at this point to the special structure of the PPA and, in particular, its first two Chapters: Chapter 1 refers to breaches of privacy in general, while Chapter 2 regulates the protection of privacy in databases.

With respect to the second chapter, Section 7 of the PPA defines a database as *"a collection of data, kept by a magnetic or optic means and intended for computer processing"*. In this way, the system of guarantees established in Chapter 2 will be applicable only to those cases in which there is an automated processing of information and not in those cases where there is no such automated processing.

The Working Party takes note of the explanations given by the Israeli authorities, to the effect that citizens would be protected against non-automated data processing (or manual processing) by the safeguards enshrined in Chapter 1 of the PPA, where certain principles are reflected, such as the limitation of the purpose, secrecy and consent.

Nonetheless, it is worth recalling that the protection which the Directive conferson these types of processing relates not only to the abovementioned principles, but to the totality of its system and, in particular, to the principles contained in document WP12. For this reason, in order to be able to consider that the level of data protection of a certain State with regard to non-automated processing systems is adequate, it would be necessary for the domestic law of the said State to recognize, at least in respect of these processing systems, the aforementioned principles.

For this reason, since Chapter 1 does not include the abovementioned principles in their entirety, it is not possible to consider the Israeli legislation as adequate with regard to non-automated or manual processing systems. In this connection, the Working Party would like to recall that the "Schoffman Report" reached the same conclusion, proposing a reform of the legal framework in force in Israel to extend the totality of the data protection safeguards to include manual processing systems.

Thus, the Working Party believes that the analysis of the adequacyof the system of data protection in Israel cannot refer to the non-automated processing of data, since the said framework does not establish the safeguards envisaged in document WP12.

To this end, the Working Party also wishes to make it clear that it believes it could continue its adequation analysis with regard to total or partially automated processing systems. Therefore, it should not be considered as excluding from the adequation examination, which will be carried out from this point, those international data transfers to Israel that are made through automated means or those that, even if they have not been carried out through the said means, refer to data that are subsequently going to be the subject of automated processing in the State of Israel.

Therefore, only those international data transfers whereby the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means will be excluded from this assessment, since it is only in such cases that the provisions of Chapter 1 of the PPA do not apply.

The Working Party is aware that the volume of transfers excluded from the adequation assessment will be residual, and will not significantly affect the application of the Decision that may ultimately be adopted; however, it believes it is essential to make the said exception in the light of the Directive´s provisions. At the same time, it recommends the adoption of provisions that envisage the application of Israeli legislation to manual databases as part of the legislative developments to be carried out in the future, and in particular in those related to the implementation of the "Schoffman Report", with the aim of being able to expand its assessment, where applicable, to include these processing systems.

3.2. Principles related to the content

Taking the above statements into consideration, we will now proceed to assess the level of data protection in Israel, in the light of the principles contained in document WP12, starting with the study of the principles with which the legislation of the State of Israel should comply.

a) Fundamental Principles

> **1) The purpose limitation principle:** data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive.

The Working Party believes that Israeli legislation respects this principle. Thus, in general terms, Article 2 (9) of the PPA states *that "using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given"* is a breach of privacy.

This general principle is even reinforced by Article 8 (b) of the Law, which provides that *"a person shall not use information in a database that requires registration under this section except for the purpose for which the database was established"*.

Furthermore, for those instances in which the database has been registered with the supervisory authority, Article 9 (b) (2) of the PPA says that the request must include *"the purposes for which the database was established and the purposes for which the information is intended"*.

Finally, the Working Party confirms that the Courts of Justice have interpreted these rules in similar terms to those envisaged by the Directive. In particular, it takes into consideration the prohibition of incompatible use of financial data referred to by Israel´s Supreme Court in the case *Database Registrar v. Ventura*.

> **2) The data quality and proportionality principle:** data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

With regard to the principle of quality in the strict sense, the Working Party believes that, even though it is not listed as an independent principle, the obligation of keeping the exact data and, if appropriate, keeping them up to date, is recognized by Israeli law through the regulation on the right to rectification referred to in Section 14 of the PPA.

Thus, Subsection (a) of the said Section states that *"A person who, on inspecting any information about himself finds that it is not correct, not complete, not clear or not up to date may request the owner of the database or, if such owner is a non-resident, the possessor thereof to amend or delete the information"*.

Subsections (b) and (c) refer to the decision of the owner of the database. Therefore, *"Where the owner of a database agrees to a request under subsection (a), he shall make the necessary changes in the information and shall notify them to every person who received the information from him within a period prescribed by regulations"*.

In case of refusal, the owner must communicate it to the data subject, adding Section 15 whereby *"a person requesting information may, in the form and manner prescribed by regulations, appeal to the Magistrate's Court against refusal by the owner of a database to enable inspection under section 13 or section 13A and against notice of refusal under section 14(c)"*.

With regard to the principle of proportionality derived from Article 6(1)(c) of the Directive, the Working Party confirms that this principle is not specifically recognized in the PPA. Nonetheless, the Working Party satisfactorily receives explanations and case law provided in relation to this issue by the Israeli authorities, which to a large extent enable the said deficiency to be offset.

Thus, the Working Party considers as satisfactory the clarifications given with respect to the constitutional scope of the proportionality principle when the processing is carried out in the public sector. In particular, it considers as especially relevant the law of precedent derived from the judgement by the Supreme Court pronounced in the case *Acri v. Minister of Interior,* provided by the Israeli authorities, where there is an express reference to the undertaking of the proportionality principle in the terms provided by the Directive.

In the same way, the Working Party welcomes with satisfaction the clarifications given by the Israeli authorities with regard to the legal requirement of proportionality in the processing, based on the principles of reasonableness of the measure and good faith. In this sense, it considers particularly interesting the precedent established by the case *Eisner v. Richmond,* which restricted the use of videocameras at the workplace and by others following a ruling by the National Labour Court in Tel Aviv. The Working Party also considers relevant the application of the proportionality principle in consumer protection and the court resolutions in which the competent courts, and in particular the Standard Contract Court in Jerusalem, have invalidated clauses that allowed the exchange of information within business groups, as in the case *Bank of Israel v. First International Bank of Israel*.

In light of this case-law, the Working Party believes that the proportionality principle is guaranteed in most of the instances in which it would be possible to apply a disproportionate processing to personal data and, in particular, that the proportionality principle is a constitutional principle that must be observed by any data processing carried out within the public sector or within the private sector when performing public tasks.

Nonetheless, the Working Party believes it would more satisfactory if Israeli legislation explicitly included this principle, with the aim of guaranteeing that the activities that lie within the private sector and tare different from those for which there are already court rulings based on the principles of reasonability and good faith, will be able to deal in the future with problems of intepretation that could hinder the adequate protection of the rights of the individuals involved. In this connection, the Working Party recalls that the inclusion of this principle within the PPA is contained in the conclusions of the "Schoffman Report".

In this way, without the aforementioned conclusion affecting the final assessment regarding the level of protection of the State of Israel, the Working Party believes that the future legislative developments and, in particular, those related to the implementation of the "Schoffman Report", should adopt the provisions that envisage the express application of the principle of proportionality in relation to the totality of personal data processing carried out by the public and private sectors.

> **3) The transparency principle:** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2)3 and 13 of the Directive.

The Working Party believes that the legislation of the State of Israel complies sufficiently with this principle.

Section 11 of the PPA provides that:

> *"A request to a person for information with a view to the keeping and use thereof in a database shall be accompanied by a notice indicating*
> *(1) whether that person is under a legal duty to deliver that information or whether its delivery depends on his volition and consent;*
> *(2) the purpose for which the information is requested;*
> *(3) to whom the information is to be delivered and the purposes of such delivery."*

Furthermore, in accordance with section 13A (1) of the PPA *"The owner of a database who keeps it at the place of another person (in this section - the possessor) shall refer the person making the request to the possessor, with his address, and order the possessor, in writing, to enable the person making the request the inspection"*. Likewise, according to subsection (2) *"Where the person making the request applies to the possessor first, the possessor shall inform him if he possesses information about him, and also the name and address of the owner of the database"*.

> **4) The security principle:** Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

The Working Party believes that the State of Israel guarantees this principle, taking specifically into account the provisions of sections 16, 17, 17A and 17B of the PPA.

Section 7 defines "information security" as the *"protection of the integrity of the information, or protection of the information from being exposed, used or copied, without lawful permission"* and Section 17 adds that *"A database owner, possessor or manager, are each responsible for the information security in the database"*.

Article 17B specifically establishes that certain owners of a database or its processors must appoint a security supervisor with the appropriate qualifications, who will be responsible for the security obligations.

In addition, Article 16 regulated the confidentiality obligation in the processing of information by establishing that *"No person shall disclose any information obtained by him by virtue of his functions as an employee, manager or possessor of a database save for the purpose of carrying out his work or implementing the Law or under a court order in connection with a legal proceeding; where the request is made before a proceeding has been instituted, it shall be heard in the Magistrate's Court"*. Failure to comply with this obligation may result in a prison sentence of up to five years.

Finally, Article 17A of the PPA refers to the processor, providing the following:

> *"(a) A person who possesses databases of different owners shall ensure that access to each database is provided only to persons who are expressly authorized to do so by written agreement between the person and the owner of the said database.*
> *(b) A person who possesses at least five databases that require registration under section 8 shall deliver annually to the Registrar a list of the databases in his*

possession, indicating the names of the owners of the databases, verified by affidavit that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the security supervisor, as referred to in section 17B."

5) **The rights of access, rectification and opposition:** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights must be in line with Article 13 of the Directive.

Section 13 (a) of the PPA establishes that *"every person is entitled to inspect, either himself or through a representative authorized by him in writing or his guardian, any information about him kept in a database"*, `providing Section 13 (b) that *"the owner of a database shall enable, at the request of a person referred to in subsection (a) (hereinafter "person making the request") inspection of the information, in the Hebrew, Arabic or English language"*.

With regard to the right of rectification, section 14 (a) of the PPA, already analysed above, establishes that *"A person who, on inspecting any information about himself finds that it is not correct, not complete, not clear or not up to date may request the owner of the database or, if such owner is a non-resident, the possessor thereof to amend or delete the information"*.

Failure to comply with the obligations imposed on the controllers by virtue of these sections constitutes a criminal offence under Article 31 and could also give rise to a civil liability vis-à-vis the data subject under section 31B. These sections will be studied in more detail later in the present opinion.

With regard to the right to object, section 17F of the PPA expressly establishes such right in relation to direct marketing activities, as will be seen further on.

Having said this, the Working Party confirms that the Israeli legislation does not establish this right through a general clause. Nonetheless, it takes into account that, according to the PPA, data can be collected only for a limited purpose (sections 8(b), 2(9)), of which the data subject has been informed (sec. 11). Hence, the Working Party considers that a data subject can oppose the processing of the data on the grounds that it exceeds the purposes for which the data was collected, or that he was not properly informed thereof. In such a case, the excessive processing is considered a violation of privacy under sec. 2(9) of the PPA, a criminal offence under sec. 31A(a)(1), and misrepresentation of the notice requirement, which is a criminal offence under sec. 31A(a)(3).

Section 15 of the PPA additionally establishes that *"a person requesting information may, in the form and manner prescribed by regulations, appeal to the Magistrate's Court against refusal by the owner of a database to enable inspection under section 13 or section 13A and against notice of refusal under section 14(c)"*.

Lastly, the Working Party believes that exemptions to the exercise of the right to access, and therefore to rectify, provided in section 13 (c·) of the PPA are consistent with those contained in Article 13 of the Directive for the Member States. In this sense, the Working Party positively values the case law derived from the law courts in relation to the exercise of the aforementioned rights and, in particular, the case law contained in the ruling pronounced by

the Supreme Court in the case of *Fischler v. Chief of Police,* in which the data subject was granted the right to know the information about himself contained in the police files.

Therefore, the Working Party believes that the legislation of the State of Israel sufficiently guarantees the rights of the data subjects to access their data, request the rectification or object to the processing thereof, according to the terms contained in document WP12.

> **6) Restrictions on onward transfers:** further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive (These exemptions are examined in Chapter Five).

For the purpose of assessing compliance with this principle, the Working Party takes into consideration the provisions of Privacy Protection (Transfer of Databases Abroad) Regulations adopted by the Government of Israel on 17 June 2001.

The regulations prohibit the transfer of data to third countries, unless those countries provide a level of data protection which is not less than that laid down in Israeli law, and specifically refers to several basic principles, such as lawful and legal collection and processing of data, purpose limitation, data quality (accuracy and keeping data up to date), respect for the right of access (and subsequently, according to Israeli legislation, rectification), and data security.

Regulation 2 (8) specifies several cases that could be considered as a legal presumption of adequacy, including Member States, those countries that are a Party to Convention 108 of the Council of Europe or those for which *"the Registrar of Databases announced that an agreement has been achieved with a privacy agency of the third country".*

Paragraphs (1) to (7) of Regulation 2 specify several exemptions to these general rules:

- *"if the data subject consented.*
- *if it is impossible to have the consent, and it is crucial to transfer the data to protect the person's health.*
- *if the data is transferred to a [foreign] corporation held by the owner of the [local] database, and he has guaranteed the data protection.*
- *if the receiver of the data has undertaken the obligation to provide data protection as if it were kept in Israel.*
- *if the data is available to the public under a statutory authorization.*
- *if the transfer is crucial to protect public order of safety.*
- *if the transfer of data is required by Israeli law."*

Regulation 3 states the accountability principle, which provides that the transferring party should arrange for the receipt of a guarantee from the receiver of the data that sufficient measures are undertaken to secure the data, and that such data are not further transferred.

The Working Party also believes that the rules that have been set out comply with the principle of restriction of further data transfers to third countries and that the guarantees provided by the Israeli legislation on this issue make it possible to guarantee adequate respect for the rights of citizens of the European Union whose data are being processed in Israel.

Nonetheless, the Working Party would like to recall the criteria for the interpretation of exemptions established by Article 26(1) of the Directive and contained in its "*Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*" (document WP114) and it urges the Israeli authorities to carry out any interpretation of the exemptions contained in rule 2, previously mentioned, in accordance with the criteria included in the said document and in the Directive itself.

b) Supplementary principles

Document WP12 refers to certain principles that must be applied to specific processing systems, in particular the following:

> **1) Sensitive data -** where 'sensitive' categories of data are involved (those listed in Article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

Section 7 of the PPA includes the concept of "sensitive data", defining it as:

> *"(1) data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person;*
> *(2) information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, is sensitive information.";*

The Working Party believes that, although the above list does not fully coincide with the one established under Article 8 of the Directive, it may be regarded as similar. In particular, the WP understands that information which refers to opinions and beliefs includes much of the data mentioned in the said Article. In addition, the Working Party urges the Israeli authorities to consider as sensitive, not least because it belongs to the "*intimate affairs*" category, such information which refers to the data listed in Article 8 of the Directive that could not be included under the other categories envisaged by the PPA and, in particular, the data related to ethnic origin or sexual preferences.

The Working Party also confirms that, in general, data may only be collected with the prior consent of the data subject, which - according to section 3 of the PPA - may be either express or implicit. This possibility does not fully meet the requirements of Article 8 of the Directive, which states that the consent must be explicit.

However, this possible gap is overcome by the abovementioned section 3, which requires that, in any event, the consent has to be informed. In this way, the Working Party believes the processing of such data may only be carried out as a consequence of an action from the data subject and not as a result of the direct giving of consent if the subject has been clearly informed of the terms explained when referring to the principle of transparency.

For this reason, even when the processing may derive from implicit consent of the data subject, the Working Party believes that a prior action from the controller is necessary, aimed at enabling the data subject to learn of all the consequences of the action involved in him giving this consent.

Therefore, even though there is no rule similar to the one envisaged in the Directive, the Working Party believes the Israeli legislation adequately meets this principle.

2) Direct marketing - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt out' from having his/her data used for such purposes at any stage.

The Working Party satisfactorily confirms that this principle is clearly regulated by the Israeli legislation, since the PPA contains a Part within its Chapter 2 specifically aimed at "direct mailing" defined as *"contacting a person personally, based on his belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a database"*.

The Israeli legislation contains specific obligations in the event of the processing of the said data. In particular, the controllers must register the file with the supervisory authority and keep an up-to-date register of the sources from which they obtained the data. Furthermore, there are specific information requirements that must be included in all deliveries addressed to the data subjects.

With regard to the principle itself, the Working Party believes that it is met by subsections (b) and (e) of section 17F of the PPA, which establish the following:

"(b) Every person is entitled to demand, in writing, of the owner of the database used for direct mailing that the information relating to him be deleted from the database.
(c) Every person is entitled to demand, in writing, of the owner of the database used for direct-mailing services or of the owner of the database containing the information based on which the contact was made, that the information relating to him not be delivered to a person, to a type of persons or to specific persons, for either a limited period of time or permanently.
(d) Where a person informed the owner of the database of his demand as specified in subsections (b) or (c), the owner of the database shall act in accordance with the demand and notify the person, in writing, that he acted accordingly.
(e) Where the owner of the database did not give notice as specified in subsection (d) within 30 days from the day of receipt of the demand, the person whom the information is about may apply to the Magistrate's Court in the manner prescribed by regulations, to order the owner of the database to act as specified."

3) Automated individual decision: where the purpose of the transfer is the taking of an automated decision within the meaning of Article 15 of the Directive, the individual should have the right to know the logic underlying this decision, and other measures should be taken to safeguard the individual's legitimate interest.

The Working Party confirms that Israeli legislation does not contain any express provision with regard to this principle. However, it satisfactorily receives comments contained in the report issued by the CRID and the clarifications carried out by the Israeli authorities in the sense that the Israeli law, in any event, enables the data subject to object to the adoption of these types of decisions.

In any event, without prejudice to considering this principle as met at this point in time, the Working Party urges the Israeli authorities to explicitly contemplate this principle in similar terms to Article 15 of the Directive in all future regulatory measures to be adopted regarding this matter.

3.3. Procedure/Application mechanisms

The opinion issued by the Working Party WP12 "Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive" indicates that, in order to provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the range of different judicial and non-judicial procedural mechanisms used in third countries.

In this respect, the objectives of a data protection system are essentially threefold:

- To deliver a good level of compliance with the rules.
- To provide support and help to individual data subjects in the exercise of their rights.
- To provide appropriate redress to the injured party where rules are not complied with.

a) To deliver a good level of compliance with the rules: a good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important part in ensuring respect for the rules, as can systems of direct verification by authorities, auditors, or independent data protection officials.

The Israeli Law, Information and Technology Authority (ILITA).

Pursuant to Section 7 of the PPA, a Database Registrar is created, whereby the *"Registrar means a person who has the qualifications to be appointed judge of a Magistrate's Court, and was appointed by the Government, by notice in Reshumot, to keep a "Register of Databases" (hereinafter referred to as "the Register") as prescribed in section 12"*.

This Registrar has been currently integrated, by virtue of a decision from the Government of Israel in 2006, in ILITA, which was created under the aforementioned decision so that the controller of the Database Register is, in turn, the Head of ILITA. Furthermore, ILITA also integrates the Certification Authorities Registrar and the Credit Data Services Registrar.

The enforcement capabilities of ILITA are regulated by section 10 of the PPA. In this sense, the Working Party, in accordance with the explanation given above, is aware that these capabilities, granted by Law to the Database Registrar, correspond to ILITA, in which this Registrar is integrated.

In particular, the PPA grants ILITA powers to register and inspect the processing, under the terms mentioned below.

The Working Party takes note of the recent modifications adopted by the Government of the State in relation to the appointment and dismissal of the Head of ILITA and believes that such modifications grant the latter, and therefore the said authority, an adequate degree of independence for the purposes that are established for supervisory authorities regulated by the Directive. In particular, it takes into account that those who integrate ILITA and its Head have the profile of civil servants, and are not subject to any type of mandate or political profile.

To that end, the Working Party takes into account that, in accordance with Government Decision 4660 (HC/195) dated 8 January 2006, the appointment of the Head of ILIRA, as a high ranking official, is subject to prior assessment by an independent committee, composed of five members, with representatives from the public authorities, the Academy and the supervised entities, who set the required conditions for the appointee and propose the appointment of the person chosen.

In addition, the Working Party acknowledges with satisfaction that, according to Government Decision No. 4470 dated 8 February 2009, the term of tenure for the Head of ILITA was set at six years. The functions of Head of ILITA may be terminated only in special circumstances by a special Civil Service Commission committee headed by a former judge. This mechanism is similar to that established in Israel, among others, for the Antitrust Commissioner, the Capital Markets and Insurance Regulator or the Accountant General in the Ministry of Finance. Moreover, any decision to terminate the Head of ILITA would be subject to judicial review in which reasonable grounds would have to be shown. Finally, the Head of ILITA is protected by Israeli labour law, including the provisions of the Basic Law: Freedom of Employment; principles of reasonableness, proportionality and procedural fairness.

With regard to ILITA's budgetary independence, the Working Party takes into account the explanations given by the Israeli authorities in relation to the applicable budget scheme, in general terms, for supervisory authorities in Israel, which is similar to ILITA´s and, at the same time, confirms that assignations given in the last few years make it possible to consider its status of independence as adequate.

Moreover, the Working Party takes into consideration the fact that, pursuant to section 36S (b) of the PPA, the funds resulting from the collection of fees for the registration of databases directly revert to ILITA as the supervisory authority for the development of the functions which have been attributed to it by Law.

The Working Party also takes into consideration the statements made by the Israeli authorities in which they express the independence with which these authorities have carried out their duties, including the performance of inspections to public bodies, such as the Office of the Attorney General, the Ministry of Internal Affairs, the Ministry of Transportation, the Ministry of Defence or even the Ministry of Justice, in which ILITA is integrated.

Finally, the Working Party believes that the competencies attributed to ILITA, which even include the prosecution of criminal offences against privacy, and the fact that ILITA has been designated to organize the 32nd International Conference on Privacy and Personal Data Protection, which is scheduled to be held in Jerusalem in October 2010, reinforce the efforts made by the State of Israel to guarantee the existence of a personal data protection authority and to adequately safeguard this right.

In the light of all of the above, the Working Party concludes at this point that the State of Israel has a supervisory authority for the protection of data that possesses the necessary independence and the adequate enforcement competencies, in similar terms to those provided by Article 28 of the Directive.

Enforcement and sanctioning measures

After investigating a complaint, ILITA decides whether it is justified. If so, ILITA has the power to issue compliance instructions to the database controller.

Section 31A of PPA provides a list of criminal offences in cases of infringment. It should be noted that, as aforementioned, ILITA has been granted the authority to investigate, according to its enforcement powers, those offences a previous phase or the criminal procedure sustained by the courts of justice.

In addition, ILITA has the power to impose administrative fines for the offences listed in sec. 31A and according to an annex to the *Regulations of Administrative Offenses (Administrative Fines – Privacy Protection), 2004*, which were issued by the Minister of Justice under the authority vested in him by the *Administrative Offenses Act of 1985*. The system of administrative fines allows the relevant executive to impose a fine, and allows the defendant to either pay the fine or require that a trial is held.

Together with the abovementioned sanctions, section 10 (f) of the PPA provides that *"Where the possessor or owner of a database infringes any provision of this Law or the regulations thereunder, or fails to comply with a request made to him by the Registrar, the Registrar may suspend the registration for a period that he shall determine or cancel the registration of the database in the Register, provided that prior to the suspension or cancellation the owner of the database was given the opportunity to be heard"*.

In the light of all this, the Working Party believes that the Israeli legislation has put in place the necessary elements to guarantee a good level of compliance with the rules on data protection.

> **b)** To provide **support and help to individual data subjects** in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. In order to do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

The Working Party believes that this principle is sufficiently guaranteed by the Israeli legislation. In particular, subsections (d) and (e1) of Section 10 establish the following:

> *"(d) The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, shall establish by order, a supervisory unit that will supervise the databases, their registration, and the information security therein; the unit shall be sized accordingly with the supervision needs.*
>
> *(e) The Registrar shall head the supervisory unit, and shall appoint inspectors to carry out the supervision pursuant to this Law; no person shall be appointed inspector unless he received the appropriate professional training in the field of computerization and information security and exercising powers under this Law, and the Israel Police did not object to his appointment for reasons of public safety.*
>
> *(e1) In carrying out his functions, an inspector may –*

(1) demand every relevant person to deliver to him information and documents relating to a database;

(2) enter a place as to which he has reasonable belief that a database is being operated, search the place and seize objects, if he is convinced that doing so is necessary to ensure implementation of this Law and to prevent violation of its provisions; the provisions of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 5869 – 1969 shall apply to an object that has been seized under this section; arrangements for entering a military installation or an installation of a security authority within its meaning in section 19(c) shall be determined by the Minister of Justice upon consultation with the minister in charge of the security authority, as the case may be; in this paragraph, "object" includes computer material and output as defined in the Computers Law, 5765 – 1995;

(3) notwithstanding the provisions of paragraph (2), an inspector shall not enter a place that is used solely as a residence, other than pursuant to an order given by a judge of the Magistrate's Court."

c) To provide **appropriate redress** to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

Together with the previously analysed sanctioning measures, both at an administrative and at a criminal level, section 31B of the PPA states that *"An act or omission in violation of the provisions of chapters two or four or in violation of regulations enacted under this Law shall be a wrong under the Civil Wrongs Ordinance"*.

Therefore, the Working Party believes that Israeli law sufficiently guarantees the right of the data subject to be compensated for any damage infringing upon his rights or property as a consequence of the illicit processing of his personal data.

4. RESULTS OF THE ASSESSMENT

In conclusion, taking all of the above into account, the Working Party believes that **Israel guarantees an adequate level of protection** according to provision 6 of Article 25 of Directive 95/46/EC of the European Parliament and of the Council, dated 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in relation to automated international data transfers or, where they are not automated, they are subject to further automated processing in Israeli territory.

At the same time, the Working Party encourages the Israeli authorities in future legislative developments, and in particular those related to the implementation of the "Schoffman Report", to adopt provisions that envisage:

- The application of Israeli legislation to manual databases, in order to extend the adequation assessment to those cases that have not been included in the conclusions of the opinion stated herein.

- The express application of the proportionality principle in relation to the totality of personal data processing carried out by the private sector.

- An interpretation of the exemptions in international data tranfers online envisaged in Article 26(1) of the Directive.

Finally, the Working Party states that, within the framework to be established by the Decision finally adopted by the Commission, it will closely follow the measures adopted within the framework of the issues discussed above.

Done at Brussels, on 1 December 2009

For the Working Party
The Chairman
Alex TÜRK