תאריך: 28 דצמבר, 2011
ב' טבת, תשע"ב
סימוכין: 015-99-2011-005798

הרשות למשפט, טכנולוגיה ומידע - דו"ח שנתי לשנת 2010

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

1. דבר ראש רמו"ט 6
2. עיקרי הדו"ח 10
3. סטטוס הקמת רמו"ט 13
א. כ"א 13
ב. הקמת מעבדה פורנזית 14
ג. הקמת יחידת חופש מידע במסגרת רמו"ט 14
4. מעורבות רמו"ט בחקיקה טכנולוגית 15
א. תזכיר הגנת הפרטיות (סמכויות אכיפה) 15
ב. תזכיר חוק הגנת הפרטיות (ניהול תקין של מידע אישי) 15
ג. מסלקה פנסיונית 16
ד. כרטיס חכם בתחבורה ציבורית 17
ה. נייר עמדה בנושא הגנה על קטינים 17
ו. תקנות אבטחת מידע 18
ז. הנחיות 19
ח. נייר עמדה בנושא השימוש במצלמות מעקב 19
ט. עיקולים מקוונים 20
י. נייר עמדה בנושא ביטול כלל הראיה הטובה ביותר 20
יא. מדריך פרטיות בעבודה 21
5. פעילות בינלאומית של רמו"ט 22
א. שבוע בינלאומי של "פרטיות במידע" בירושלים 22
1) כינוס ועדת ICCP של ה-OECD - 30 שנה להנחיות הארגון בנושא פרטיות והעברות מידע ... 22
2) הכנס הבינלאומי ה-32 של רשויות הגנת מידע – פרטיות:דורות 26
3) אירועים נוספים בשבוע הפרטיות במידע 32
א) כנס ה"קול הציבורי" – החופש והפרטיות של צרכנים דיגיטליים 32
ב) המחקר העכשווי בנושא פרטיות – היבטים גלובליים 32
ג) היבטי פרטיות ב"רשת חכמה" (smart Grid) 33
ד) פרטיות במכשירים ניידים 33
ה) הטמעת פרטיות בתוכניות ציות בישראל 33
4) נתונים אודות ההשתתפות בכנסים 34
ב. החלטת הנציבות האירופית על רמת הגנת הפרטיות בישראל 36
ג. פרוייקט ה-twinning עם הרשות הספרדית להגנת מידע אישי 37
ד. פרוייקט ה-accountablitiy 39

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. הצטרפות לרשת בינלאומית לאכיפת הגנת פרטיות - GPEN 39

6. דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2010 (מוגש למועצה להגנת הפרטיות מכח סעיף 10א לחוק הגנת הפרטיות) 41

א. מבוא 42

ב. נתונים 42

1) כמות התיקים שנוהלו לפי חתך מגזרי 43

2) הנושאים העיקריים שהטרידו את הציבור 43

ג. תיקי פיקוח נבחרים 44

1) מגזר ציבורי 44

א) עיריית רמת גן וחברת קידום 44

ב) משרד התחבורה – כספי מג'יק 45

ג) משרד התחבורה – חברת הפניקס 46

ד) מפלגת חד"ש 46

ה) הנהלת בתי המשפט 46

2) מגזר פרטי 47

א) חברת AIG 47

ב) חברת דיילקום 48

ג) בנק הפועלים 49

ד) המשביר לצרכן 49

ה) בנק לאומי 50

ו) ביטוח ישיר 51

ז) שופרסל 53

ח) חבר אוסקר החזרי מס – הכשלת פיקוח 53

ט) סלקום 54

י) מגדל 55

יא) חברת רותם חינוך בע"מ מפעילת "אור-אל חוויה לבר מצוה" 56

יב) Jobsplace.co.il 56

יג) חברת הראל 57

יד) טנא קט 57

טו) חברת טלאול - סלקום 58

טז) מכללת הייטק 59

יז) ארגון המורים 59

יח) פנקס הבוחרים – מתמודד לראשות עיריית רחובות 59

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

יט) תלונה מהולנד 60
ד. תיקי מבדק 60
1) מגזר ציבורי 60
ו) כרטיס חכם בתחבורה הציבורית 60
ה. חקירות פליליות 63
1) קבלת סמכויות פליליות והכשרות 63
2) תיק מ.נ.ר 64
3) תיק חקירה פלילי 65
ו. הטלת קנסות מנהליים 66
ז. רישום מאגרי מידע 67
1) נתונים 67
2) נושאים עקרוניים שעלו מהליך הרישום 69
א) דויטשה בנק – מאגר ניטור פעילות עובדים 69
ב) מנהרות הכרמל 70
ג) דחיית בקשות לרישום מאגרי מידע 70
7. פירוט הפעלת סמכויות רשם שירותי נתוני אשראי ושירותי מידע על עוסקים, מכוח חוק שירות נתוני אשראי, התשס"ב-2002 ותקנות שירות נתוני אשראי, התשס"ד-2004. 71
א. בעלי רישיונות 72
1) חברת לב אמון יזמים בע"מ 72
2) בעלי רשיונות תקפים 72
ב. תיקוני חקיקה 72
ג. תשלום בעלי הרישיונות לבנקים 73
ד. פיקוח על בעלי רישיונות לשירותי נתוני אשראי 73
1) נתונים 74
2) פעולות אישור לבעלי רשיונות 74
ז) חברת לב אמון בע"מ 74
ח) חברת בי.די.איי קופאס בע"מ 75
3) תיקי פיקוח נבחרים 75
ט) מתן זכות עיון 75
י) אבטחת מידע 76
8. דין וחשבון של רשם גורמים מאשרים בדבר הפעלת סמכויותיו בשנת 2010 לפי תקנה 16ל לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב–2001 77

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. פעולות פיקוח על הגורם המאשר – חברת קומסיין 77
(1) נתונים 77
(2) עדכון מסמך הנהלים של קומסיין 78
(3) כשל פרסום רשימת תעודות בטלות (CRL) 79
(4) הארכת מועד אישור הגורם הרושם – ההוצאה לאור של לשכת עורכי הדין 82
(5) אישור מתחמי עבודה נוספים 82
(6) אישור מנגנון שחרור מנעילה של כרטיס חכם 83
(7) בקשה לאישור גורם רושם נוסף 83
ב. בקשות רישום חדשות 83
(1) עדכון הנחיות פנימיות לרישום 83
(2) בקשת רישום של חברת סקיורנט גורם מאשר בע"מ 84
ג. פרסום הנחיות רשם גורמים מאשרים 84
(1) הנחייה 1-2010 84
(2) הנחייה 2-2010 85
(3) הנחייה 4-2010 87
(4) הנחייה 5-2010 - זיהוי חלופי 87
ד. תיקוני חקיקה 88
(1) חוק חתימה אלקטרונית (תיקון מס' 2), התש"ע-2010 88
(2) עדכון תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 89
ה. פעילות במסגרת FESA 89
9. נספחים 91
ו. נספחים לפרק 5 – פעילות בינלאומית של רמו"ט 91
1) נספח א' – הגנת הפרטיות בישראל – סקר תפיסות בקרב כלל האוכלוסייה 91
2) נספח ב' – החלטת הנציבות האירופית על רמת הגנת המידע האישי בישראל 152
ז. נספחים לפרק 8 – דו"ח רשם גורמים מאשרים 157
1) נספח א' – הנחיית רשם גורמים מאשרים 1-2010 157
2) נספח ב' – הנחיית רשם גורמים מאשרים 2-2010 162
3) נספח ג' – הנחית רשם גורמים מאשרים 4/2010 168
4) נספח ד' – הנחיית רשם גורמים מאשרים מס' 5-2010 196
5) נספח ה' – סיכום מפגש תקופתי FESA 200

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. דבר ראש רמו"ט

דין וחשבון זה לשנת 2010 של הרשות למשפט, טכנולוגיה ומידע (רמו"ט) במשרד המשפטים, מביא בפני הקורא את מגוון פעולות רמו"ט בשנה זו.

על הקמת רמו"ט החליטה ממשלת ישראל בתחילת שנת 2006, ובהקמתה הוחל בשלהי אותה שנה, עת מינתה אותי ממשלת ישראל להקימה. בשנת 2010, כפי העולה מהדו"ח, אף שלא הושלמו כל התהליכים המתחייבים מהקמתה – הגיעה רמו"ט לבגרות תפקודית מרשימה. הישג זה נובע בעיקר מכוח האדם המעולה ברמו"ט, אשר כולל עובדים בעלי רמה מקצועית גבוהה ביותר המתמחים בהיבטים השונים של הממשק בין משפט וטכנולוגית מידע.

שנת 2010 הייתה שנה בעלת גוון בינלאומי משמעותי בפעילות רמו"ט. האתגרים של משפט וטכנולוגיה הם חוצי גבולות, והנושאים המעסיקים את רמו"ט, ובפרט הגנת הפרטיות במידע, נמצאים במרכז הדיון הציבורי ברחבי העולם. לרמו"ט נקרתה הזדמנות יוצאת דופן בשנה זו, לארח בישראל את השמנא והסלתא של קהילת הפרטיות בעולם, בשל הזכות שניתנה לנו לארגן בסוף חודש אוקטובר 2010 שני כנסים בינלאומיים בנושא הגנת הפרטיות במידע: הכנס הבינלאומי הראשון של ארגון ה-OECD בישראל, אשר ציין 30 שנה להנחיות הארגון בנושא של הגנת פרטיות והעברות מידע בינלאומיות והכנס הבינלאומי ה-32 של נציבי הגנת מידע אישי ופרטיות.

אין זה מקרה שרמו"ט זכתה בכבוד זה – מדובר בתוצאה של תהליך ארוך טווח אשר מיקם אותה בצמרת רשויות הגנת המידע ברחבי העולם, והכנסים בססו מעמד זה. לצד כנסים אלה, התקיימו במהלך השנה שני תהליכים בינלאומיים משמעותיים נוספים על ידי רמו"ט: סיום תהליך ההכרה של הנציבות האירופית בכך שרמת ההגנה על מידע אישי בישראל עומדת בדרישות הדירקטיבה האירופית להגנת מידע אישי וקיומה של תוכנית Twinning בין רמו"ט לרשות הספרדית להגנת מידע אישי (AEPD).

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

בשנה שעברה העמיד הדו"ח השנתי של רמו"ט במרכזו את תפיסת ה"עיצוב לפרטיות" (Privacy By Design) ככלי מרכזי להתמודדות עם אתגרי הפרטיות העולים מפיתוח שירותי מידע חדשים, פרטים וציבוריים כאחד. קידום נושא זה נובע מההכרה ברמו"ט כי במקרים רבים יש תועלת חברתית רבה בפיתוחם של שירותי מידע חדשים, וכי תפקיד רמו"ט כרגולטור של הגנת מידע אישי למזער את הסיכונים לפרטיות הנובעים מכך, אך לא למנוע אותם ככל שיש בהם תועלת ברורה.

בשנה זו אני מבקש, כתוצאה מהעיסוק בכנסים הבינלאומיים שרמו"ט ארחה ב-2010, לייחד את דברי בפתח דו"ח זה לנושאים המרכזיים העומדים במסגרת הדיון העולמי על פרטיות במידע בעידן המודרני, אשר מחייבים לטעמי את התייחסותם של קובעי המדיניות בנושא.

- **<u>שירותי חינם ופרטיות</u>** - המתח שבין שירותי המידע החדשים ובין פרטיות במידע על אודות יחידים קפץ מדרגה עם התפתחות המודל הכלכלי של שירותי החינם באינטרנט בתחילת שנות ה-2000. פעילות מנועי חיפוש (כגון Google ו-Bing), מערכות דואר אלקטרוני (כגון gmail ו-hotmail), רשתות חברתיות (כגון Facebook ו-Twitter), אתרי אחסון ושיתוף מידע ממומנים על ידי מכירת פרסום מוכוון מידע אישי (behavioral targeting) לגופים המעוניינים במשתמשי השירותים. במודל זה, מידע אישי הופך למטבע עובר לסוחר באמצעותו משלמים המשתמשים עבור השימוש בשירותי החינם. המטבע מומר על ידי ספקי שירותי החינם לרשומות מאופיינות ועשירות במידע על אודות משתמשי השירותים, ועל בסיסם נמכרים שירותי הפרסום האלקטרוני המאפשרים פניה מכוונת לקבוצות מוגדרות של יחידים. מודל עסקי זה טומן בחובו איבוד הולך וגובר של אנשים את הפרטיות במידע האישי שלהם. ברוב המקרים, המשתמשים אינם מסוגלים להבין את מורכבות התהליך, ולרדת לעומק אופן פעולת מודל שירותי החינם ומשמעות אגירת המידע המאופיין הזה על אודותם. הכוחות הכלכליים והחברתיים המניעים תופעות אלה הם אדירים, ואלה מחייבים גיבוש מודל הסדרה עדכני לשימוש במידע האישי, שכן ברוב המקרים לא ניתנת הסכמה מודעת, כנדרש בחוק הגנת הפרטיות, לאיסוף המידע האישי על אודותם והשימושים הנעשים בו.

- **<u>הזכות להישכח (the right to oblivion)</u>** – הדיון בקהילת הפרטיות על הזכות להישכח (The right to Oblivion), זכותו של אדם שמידע על אותו יימחק, החל במחצית העשור הקודם. על פי חוק מור המפורסם, יכולת החישוב של מעבדים מכפילה עצמה כל 18 חודשים ויכולת אחסון המידע הדיגיטלי מכפילה עצמה מידי שנה, כמו גם קצב העברת המידע בתקשורת מחשבים. צירוף שלושה פרמטרים אלה מסביר את התופעה שה"רשת

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

אינה שוכחת", וכל פריט מידע שהועלה לאתר אינטרנט כלשהו יהיה בר השגה בעתיד. פיתוחם של מנועי איתור מידע מתקדמים, דוגמת google ו-bing, מאפשר היום למפתח ולאתר כל פריט מידע שהועלה לרשת על אודות אדם. יכולת איתור מידע טקסטואלי זו הולכת ומתרחבת גם לחיפוש ויזואלי וקולי. פריטי מידע שאדם פרסם על אודות עצמו, או שפורסמו על ידי אחרים (כגון תמונות שהועלו ותויגו על ידי אחרים ברשתות חברתיות כגון facebook), עשויים להישאר זמינים, ברי איתור ואחזור, לעד. על רקע תופעה זו מתקיים דיון ער בשאלת הזכות שיש לתת לאנשים ל"הישכח", קרי למחוק את פרטיהם מהאחסון הגלובלי ברשת, או למנוע מראש את קיומו. גם בישראל נושא זה עולה על הפרק, ורמו"ט כבר קיבלה מספר לא מבוטל של תלונות אזרחים על פסקי דין המכילים מידע אישי רגיש, וניתן לאחזור ברשת. ההתמודדות הרגולטורית עם נושא זה אינה פשוטה, שכן מידע רב מונגש, לכאורה, באופן לגיטימי ועל כן הסתרתו מתנגשת עם זכות הציבור לדעת וחופש הביטוי. בנוסף, בשל טבעו של המידע הדיגיטלי ואופן פעולתה של רשת האינטרנט, קשה מאוד למחוק מידע זה לאחר שהונגש, שכן עותקים של המידע נמצאים במקומות רבים. רמו"ט צופה כי הדיון בנושא, כמו גם נחיצותם של עדכוני חקיקה ורגולציה, יעסיקו את הציבור, המחוקק ואותה בשנים הקרובות.

- **<u>פרטיות קטינים</u>** – תכליתה המרכזית של הזכות לפרטיות היא הגנה על האוטונומיה והעצמאות של אדם, וברור הוא שילדים זקוקים להגנה זו באופן המובהק ביותר לשם גיבוש אישיותם. אבל ילדים אלה היום הם גם המשתמשים (users) הנלהבים והבקיאים בטכנולוגיות מידע חדשניות, כגון רשתות חברתיות, אשר אוספות מידע רב על אודותם ושומרות אותן לעד. אפשרות ההשפעה של אמצעי פרסום חדשניים, מוכווני מידע אישי, על קטינים, כמו גם חוסר מודעות בקרבם לתוצאות של פרסום מידע על אודותם ועל חבריהם, מחייבת תשומת לב רבה מצד בעלי העניין האמורים להגן על קטינים: הורים, מחנכים, רגולטורים, מחוקקים והקטינים עצמם. על רקע תופעה זו, רמו"ט גיבשה במהלך שנת 2010 מסמך מקיף על נושא זה, אשר צריך לשמש כתשתית לדיון ציבורי רחב בנושא, בו יהיו שותפים כל אותם בעלי העניין.

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

- **<u>עדכון המשטר הרגולטורי של פרטיות במידע</u>** – התופעות המתוארות לעיל, המתוארות ביתר פירוט בפרק העוסק בכנס הבינלאומי בירושלים, הניעו ברחבי העולם תהליכים מקבילים לעדכון הרגולציה בנושא הגנת הפרטיות במידע. במקביל לארגון ה-OECD, הבוחן את עדכונן של ההנחיה בנושא פרטיות במידע שגובשה בשנת 1980, בוחנת הנציבות האירופית את עדכונה של דירקטיבה 95/46/EC המסדירה את משטר הגנת המידע האישי במדינות אירופה. בארה"ב פורסמו מספר ניירות עמדה על ידי רשות הסחר הפדרלי (FTC) ורשות התקשורת והמידע (NTIA) אשר מקדמות תשתית הסדרה של פרטיות במידע אישי בארה"ב. גם בארגון לשיתוף פעולה כלכלי באסיה-פסיפיק (APEC) מקודמים הסדרים בנושא פרטיות במידע במדינות החברות בו, וכמו כן ניתן לראות פעילות משמעותית בדרום אמריקה, שם התקבלו בשנים האחרונות מספר חוקים חדשניים להגנת מידע אישי. מדינת ישראל השכילה בעבר להיות מחלוצות הסדרת הגנת הפרטיות, לרבות זו העוסקת במידע ממוחשב, ואסור לה להישאר מאחור. חוק הגנת הפרטיות הישראלי גובש בסוף שנות ה-70, ועבר שינוי יסודי אחד לעניין מידע ממוחשב בשנת 1996. על ישראל לישר קו עם המגמות העולמיות, ולעדכן את משטר הגנת הפרטיות במידע שלה באופן שיאפשר התמודדות אמיתית עם אתגרי הטכנולוגיה של המאה ה-21.

אני מאחל לכם קריאה מהנה של דו"ח זה.

יורם הכהן
ראש הרשות למשפט, טכנולוגיה ומידע

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. עיקרי הדו"ח

בשנת 2010, אף שלא הושלמו כל התהליכים המתחייבים מהקמתה, הגיעה רמו"ט לבגרות תפקודית מרשימה. הישג זה נובע בעיקר מכוח האדם המעולה ברמו"ט, אשר כולל עובדים בעלי רמה מקצועית גבוהה ביותר המתמחים בהיבטים השונים של הממשק בין משפט וטכנולוגית מידע.

שנת 2010 הייתה שנה בעלת גוון בינלאומי משמעותי בפעילות רמו"ט. אירחנו שני כנסים בינלאומיים מרכזיים בירושלים במסגרת אירועי "שבוע הפרטיות". בראשיתו התקיים הכנס הראשון של ארגון ה-OECD בישראל אשר ציין 30 שנה להנחיה ה-OECD בנושא הגנת הפרטיות והעברות מידע בינלאומיות, אותו פתח ראש הממשלה בנימין נתניהו בנאום שהציג את חזונו באשר להגנת הפרטיות ואבטחת המידע של אזרחי ישראל. באחריתו - הכנס הבינלאומי ה-32 של נציבי הגנת מידע אישי ופרטיות. במהלך השבוע התקיימו על ידי גופים בינלאומיים שונים, בחסות רמו"ט, עוד מספר אירועים הקשורים בהגנת הפרטיות במידע. בכנסים השתתפו כ-600 איש, 440 מהם מחו"ל ממגזרים שונים: מגזר פרטי, אקדמיה, ארגוני זכויות אדם, ממשל ורשויות הגנת מידע אישי.

במקביל, הסתיים בהצלחה תהליך הכרת הנציבות האירופית בכך שרמת הגנת המידע האישי בישראל מספקת (adequate) לצורך העברת מידע אישי מאירופה לישראל, תוך הכרזה על רמו"ט כמקיימת את דרישות הדירקטיבה האירופית להגנת מידע אישי (95/45/EC) כרשות הגנת מידע אישי עצמאית וראויה לדרישות הדירקטיבה. בנוסף, ניהלה רמו"ט במהלך השנה תכנית twinning עם רשות הגנת המידע האישי של ספרד (AEPD) במימון הנציבות האירופית לחיזוק יכולותיה של רמות בתחום הגנת המידע האישי. במהלך השנה השתתפה רמו"ט ביסוד הרשת הבינלאומית לאכיפת הגנת פרטיות (GPEN – Global Privacy Enforcement Network) ובפרוייקט לקידום האחריותיות (Accountability) בהגנת מידע אישי.

במהלך השנה עסקה רמו"ט רבות בניסיון לקדם את החקיקה הקשורה בפעולתה כרגולטור של הגנת מידע אישי, ובמהלכה פורסמה לתגובות הציבור טיוטת תזכיר חוק לשינוי סמכויות האכיפה של רמו"ט להגנת מידע אישי. במקביל, הייתה רמו"ט מעורבת במספר מהלכי חקיקה במסגרתם נדרשה הסדרה נכונה ומידתית של עיבוד מידע אישי, כגון יוזמת המסלקה הפנסיונית של אגף שוק

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

ההון במשרד האוצר, והכנסת כרטיס חכם אחיד למערכות הסעה המוניות על ידי משרד התחבורה.

בפעילות הרגולטורית של רשם מאגרי מידע, הפועל במסגרת רמו"ט, הוטלו בשנה זו קנסות מינהליים ב-12 תיקי פיקוח על הפרות חוק הגנת הפרטיות. במקום בו ממצאי הפיקוח לא סיפקו רמת וודאות מספקת למשפט פלילי, אך אותרה הפרה מנהלית של החוק, נקבעה כי התקיימו הפרות של הוראות החוק על ידי הגורם המפוקח. במקרה ראשון בעקבות קביעה כזו, הוגשה תביעה ייצוגית כנגד אחד הגופים שנקבעה לגביו הפרה (חברת סלקום בע"מ).

עיקר תלונות הציבור בנושא הגנת פרטיות במידע היה בשל הפרת עקרון צמידות המטרה (שימוש במידע שלא למטרה למענה נמסר) וכן בשל דיוור ישיר בלתי חוקי. מידגם מתיקי הפיקוח המגוונים אשר נסקרים בדו"ח, מעלה את המקרים הבאים:

- עיריית רמת גן נתנה שירותי דיוור ישיר על אודות תלמידי העיר לחברת קידום מבלי הסמכה חוקית;
- חברת דיילקום נתנה שירותי טיוב מידע על בסיס מידע שהגיע מפנקס הבוחרים;
- חברת ביטוח ישיר השתמשה במידע על אודות דרישות עיקולים שהופנו אליה מההוצאה לפועל, לצורך גיבוש הצעת ביטוח לפונה שאינו לקוח החברה, בניגוד למטרת מאגר ההוצאה לפועל והוראות החוק;
- חברת סלקום ביצע תהליך העשרת מידע הלקוחות שלה במידע על אודות בני משפחה של לקוחותיה המועמדים לשירות צבאי, לצורך הצעת התקשרות ב"חבילת חיילים".

במהלך השנה התקיים על ידי רמו"ט מבדק של מימוש הכרטיס החכם בתחבורה הציבורית, אשר על בסיסו גובשו תהליכי חקיקה והנחיה למפעילים.

זרוע החקירות הפליליות של רמו"ט, מחלקת האכיפה והחקירות, קיבלה בחודש יוני 2010 הסמכה לבצע חקירות פליליות לגבי עבירות של חוק הגנת הפרטיות וחוק שירות נתוני אשראי. על בסיס סמכויות אלה החלה המחלקה בחקירה פלילית ראשונה, אשר בשנת 2010 עדיין הייתה בשלב הסמוי.

כרגולטור של תחום נתוני אשראי, ביטל רשם שירותי נתוני אשראי ומידע על עוסקים רשיון שלב א' שניתן לחברת לב-אמון יזמים בע"מ לפעול כשירות נתוני אשראי, בשל אי עמידה בחובות אבטחת המידע הנדרשות מבעל רשיון. החברה הפסיקה גם את פעילותה כשירות מידע על עוסקים.

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

בתחום החתימה האלקטרונית, עודכן מסמך הנהלים (תקנון השירות) של הגורם המאשר חברת קומסיין בע"מ, והוסדרו מחדש התחייבויותיו והצהרותיו כלפי לקוחותיו. במהלך השנה התגלה כשל בתהליך פרסום רשימת התעודות הבטלות (CRL) של הגורם המאשר, ותחקיר האירוע העלה תמונה מטרידה באשר להתנהלות חברת קומסיין וקיום חובותיה על פי החוק והנחיות רשם גורמים מאשרים.

במהלך השנה, הוגשה בקשה לרישום של גורם מאשר חדש, על ידי חברת סקיורנט גורם מאשר בע"מ, והיא נמצאת עדיין בתהליכי בחינה.

רשם גורמים מאשרים פרסם מספר הנחיות בעלות חשיבות במהלך השנה: הנחיה עניין הסיסמה הנדרשת לצורך הפעלת התעודה האלקטרונית לחתימה אלקטרונית מאושרת, הנחיה לעניין חובות מהותיות למערכות הטכנולוגיות המשמשות את הגורם המאשר בפעולתו, הנחיה לעניין האלגוריתמים ואורך מפתחות ההצפנה הראויים לשמש בתהליכי הנפקתן של תעודות אלקטרוניות לחתימה אלקטרונית מאושרת, והנחיה לעניין מסמכי זיהוי חלופיים בתהליכי הנפקת תעודות כאמור.

במהלך השנה התקבל תיקון מס' 2 לחוק חתימה אלקטרונית, התשס"א-2001, אשר התיר את כניסת הממשלה לפעולה כגורם מאשר לצורך פרוייקט תעודת הזהות החכמה, והוסף פרק אכיפה חלופית לחוק אשר מאפשר לרשם גורמים מאשרים להטיל עיצום כספי על גורם מאשר שאינו מקיים את הנחיותיו.

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. סטטוס הקמת רמו"ט

ג. כ"א

במהלך שנת 2010 נמשכה בניית תשתית כוח האדם ברמו"ט, אך גם בשנה זו לא הושלמה יצירת תקני כוח האדם ואיושם ליעד של 24 עובדי מדינה מלאים כפי שאושר על ידי נציבות שירות המדינה ומשרד המשפטים בשלבים הראשוניים של הקמת רמו"ט.

בסוף שנת 2010 עמדה מצבת כוח האדם של רמו"ט על 23 איש, מהם שלושה קבלנים וארבעה מתמחים באופן הבא:

מחלקה	מצבת כ"א						הערות
	קיימת				מתוכננת		
	סה"כ עובדים		עובדי מדינה קבועים		קבלנים ועובדים זמניים		עובדי מדינה קבועים
	2009	2010	2009	2010	2009	2010	
לשכת ראש רמו"ט	2	3	2	3	-	-	3	
מחלקת רישום ופיקוח	6	7	4	5	2	2	7	
מחלקת אכיפה וחקירה	4	6	3	5	1	1	7	
מחלקה משפטית	6	7	3	3	4	3	7	מהם ארבעה מתמחים
	18	23	12	16	7	6	24	

בשנת 2010 הייתה אמורה רמו"ט להשלים את בניית התקנים ואיושם, אך בשל מגבלות תקציבי כ"א של משרד המשפטים התהליך לא הושלם.

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

ב. הקמת מעבדה פורנזית

בתחילת 2010 הוחל בהליכי הרכש למערך מחשוב הנדרש שם הקמת המעבדה, ותהליך זה היה קרוב בסוף שנת 2010 לסיומו.

במהלך שנת 2010 בוצעו מספר פעילויות מבצעיות של חקירות פורנזיות של מאגרי מידע ומחשבים, והחל להבנות ידע ייחודי בסוגיות ספציפיות אלה של חקירת מחשבים.

ג. הקמת יחידת חופש מידע במסגרת רמו"ט

במהלך שנת 2010 נבחנה על ידי רמו"ט, על פי בקשת מנכ"ל משרד המשפטים, האפשרות כי תוסף לרמו"ט פעילות בנושא יישום הוראות חוק חופש המידע, התשנ"ח-1998.

לצורך בחינת שאלה זו התקיימה, במסגרת תוכנית ה-twinning עם הרשות הספרדית להגנת מידע אישית, פעילות בינלאומית מיוחדת אשר עסקה בשאלה זו, וזאת מאחר וברחבי העולם יש דוגמאות רבות להכללת פעילות הרגולציה בנושא חופש מידע ביחד עם הרגולציה של הגנת מידע אישי ופרטיות. הסיבות לכך הן רבות, ובעיקר בשל היכולת של רגולטור אחד לאזן את שני העקרונות אשר לעיתים מתנגשים, וכן ההתמחות בנושא של מידע, אשר גם בגופי ממשל מיוצר יותר ויותר בפורמט אלקטרוני.

בפעילות השתתפו נציגים מרשויות הגנת מידע וחופש מידע מרחבי אירופה (בריטניה, ספרד, פורטוגל, שוודיה ואירלנד) וכן גורמים ממשרד המשפטים (מחלקת ייעוץ וחקיקה), אקדמיה ומגזר אזרחי. על בסיס יום עיון זה גובשה עמדת רמו"ט בנושא, וזו הוגשה למנכ"ל משרד המשפטים.

העמדה תמכה בהכנסת פעילות הרגולציה של חופש מידע לרמו"ט, אך הצביעה על הכלים והמשאבים הנדרשים לרמו"ט, בשלב זה של הקמתה, לצורך פעולה אפקטיבית כרגולטור בנושא חופש מידע ומניעת הפגיעה באפקטיביות של רמו"ט כרגולטור של הגנת מידע אישי.

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. מעורבות רמו"ט בחקיקה טכנולוגית

א. תזכיר הגנת הפרטיות (סמכויות אכיפה)

במרץ 2010 הופץ תזכיר חוק הגנת הפרטיות (סמכויות אכיפה) אשר נועד לקבוע כלי פיקוח ואכיפה מוגברים לרשם מאגרי מידע[1]. במסגרת התזכיר הוצעו כלים חדשנים לאכיפה וכן הוגדרו בצורה מפורטת עבירות והפרות הקשורות בהגנת הפרטיות במידע, כמו גם מנגנון של הטלת עיצומים כספיים שנועדו לאפשר אכיפה יעילה.

בעקבות התזכיר קיימה רמו"ט, יחד עם מחלקת ייעוץ וחקיקה, דיונים עם גורמים שונים שהעירו הערות לתזכיר. בעקבות דיונים אלה צומצמו הוראות מסוימות בתזכיר, וזאת על מנת לקדמו בהקדם האפשרי לקראת חקיקה. התזכיר אמור להפוך להצעת חוק ממשלתית במהלך שנת 2011.

ב. תזכיר חוק הגנת הפרטיות (ניהול תקין של מידע אישי)

במהלך שנת 2010 התקיימו עם מחלקת ייעוץ וחקיקה (חקיקה) במשרד המשפטים דיונים להמשך קידומו של החלק השני של תיקון משטר הרגולציה בנושא הגנת מידע אישי.

במסגרת פרק זה מציעה רמו"ט להמיר את המשטר הקיים של רישום מאגרי מידע בחובה חדשה של ניהול תקין של מידע אישי (ומסמכים המעידים על כך), ולצמצם באופן משמעותי את חובת רישום מאגרי המידע, תוך השארת החובה לכך על גופים העוסקים בסחר במידע בלבד ולחוקרים פרטיים.

[1] לנוסח התזכיר ודיווח מפורט, ראו דו"ח הרשות למשפט, טכנולוגיה ומידע לשנת 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

ג. מסלקה פנסיונית

במסגרת חוק ההסדרים במשק המדינה לשנת 2010-2011, נכלל פרק שמטרתו הסמכה של הממונה על שוק ההון והחיסכון להסדיר הקמה של מערכת מידע שמטרתה העברת מידע על חסכונות פנסיונים לצורך שכלול שוק הייעוץ הפנסיוני (להלן – **המסלקה הפנסיונית**).

ביוזמת המסלקה הפנסיונית פוטנציאל גבוה לפגיעה בפרטיות של כלל אזרחי ישראל, שכן היא מאפשרת יצירת תמונת מידע עדכנית ומקיפה של כלל הנכסים הפיננסיים של תושבי ישראל לצורך שכלול שוק הייעוץ הפנסיוני האובייקטיבי, שהיא מטרה ראויה ביותר.

רמו"ט זיהתה בשלבים הראשונים של התהליך כי יוזמה זו היא כר נרחב לפעילות "עיצוב לפרטיות" (privacy by design), ועל כן ליוותה את התהליך משלבי ייזומו הראשוניים.

בעת גיבוש הצעת המחליטים לממשלה ובשלב ניסוח תזכיר החוק, יחד עם מחלקת ייעוץ וחקיקה (חקיקה) התווספו ביוזמת רמו"ט עקרונות שמטרתם מיזעור סיכוני הפרטיות במערכת זו, לרבות מזעור המידע שנאסף ונשמר במערכת, וזאת **מבלי לפגוע בתכליות העיקריות של החוק**.

במסגרת הצעת החוק נקבעה התייעצות בין שר האוצר לשר המשפטים בנושאים הקשורים בחקיקת משנה העוסקת במידע ביחס למסלקה, והתייעצות בין הממונה לרשם מאגרי מידע בנושאים הקשורים לרישוי ופרטיות.

במהלך הדיונים בוועדת העבודה של הכנסת נכללו הוראות נוספות שמטרתן קביעת מגבלות על שמירת מידע, ושמירה של נתונים המתעדים את ביצוע הפעילות במסלקה בלבד.

בנוסף במהלך הדיונים בוועדת העבודה של הכנסת נקבעו הוראות מפורשות לעניין זכות העיון של הלקוח במידע הפנסיוני אודותיו באמצעות המערכת.

רמו"ט השתתפה בכל הדיונים שהתקיימו בהצעת החוק עד לאישורה בכנסת, והיא תהא שותפה במהלך 2011 להתקנת חקיקת המשנה הרלבנטית לנושאי הפרטיות במסלקה, ולבחינת בקשות הרישוי.

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

ו. כרטיס חכם בתחבורה ציבורית

במסגרת טיוטת הצעת חוק ההסדרים לשנים 2011-2012 נכלל פרק שמטרתו הסדרת השימוש וההטמעה של כרטיס חכם בתחבורה ציבורית.

במהלך שנת 2010 בוצע על ידי מחלקת רישום ופיקוח ברמו"ט מבדק (audit) על אופן ההטמעה של הכרטיס החכם אצל מספר מייצג של מפעילי תחבורה ציבורית. במסגרת הממצאים עלו סימני שאלה ביחס למקור החוקי לאיסוף ועיבוד מידע אישי במסגרת הפרוייקט.

בד בבד עם הליך הפיקוח קידם משרד התחבורה במסגרת חוק ההסדרים תיקון לפקודת התעבורה על מנת להסדיר נושא זה. רמו"ט, יחד עם מחלקת ייעוץ וחקיקה (חקיקה), הייתה מעורבת בהכנת הצעת החוק, באופן שנקבעו בה הוראות לעניין מיזעור הסיכון לפרטיות בעת הפעלת המערכת, וכן הוראות המחייבות את ביצוע ההסדרה בתיאום בין שר התחבורה לשר המשפטים או המפקח הארצי על התחבורה לבין רשם מאגרי מידע, לפי העניין.

בעקבות קידום הצעת החוק וממצאי הפיקוח, מקיימת רמו"ט קשרי עבודה עם משרד התחבורה על מנת לבצע תהליך של סקר השפעה על הפרטיות (PIA - Privacy Impact Assessment) על המערכת, ובהתאם לכך לעצב את איסוף, עיבוד ושמירת המידע האישי באופן הפוגע פחות בפרטיות. תוצרי העבודה ישולבו בהצעת החוק ובתקנות שיוכנו שצפויות להיות מטופלות במהלך 2011.

ז. נייר עמדה בנושא הגנה על קטינים

בדצמבר 2010, לאחר מחקר משווה ופעילויות גם גורמים מחו"ל במסגרת פרוייקט ה – twinning, פרסמה רמו"ט נייר עמדה ובו טיוטת כללי אתיקה והתנהגות לבעלי מאגרים האוספים מידע על קטינים.

הצורך בהסדרה בתחום זה עולה ממחקרים שנעשו בישראל בשנים האחרונות. מבדיקה שביצעה רמו"ט עולה פער בין הדין החל על ההגנה על פרטיותם של קטינים ועל איסוף ושימוש במידע על אודותם, לבין המצב בפועל. בהתאם לכך הציעה רמו"ט כללי אתיקה והתנהגות ספיציפיים לבעלי מאגרים האוספים מידע על קטינים. הכללים המוצעים ע"י רמו"ט נועדו לחייב את מי שאוסף מידע מקטינים לנהוג באחריות, ולקבל הסכמה הורית לשימוש במידע,

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

תוך מתן הסבר בשפה ברורה, מה הם השימושים במידע, על מנת לאפשר גם להורים להפעיל שיקול דעת.

העקרונות בנייר העמדה מבוססים על המאפיינים המיוחדים של מידע אודות קטינים, על יכולתם וכושרם לקבל החלטות ביחס לגילוי ופרסום מידע על אודותם, ועל מעמדם ותפקידם של הוריהם ביחס להחלטות אלה.

בהתאם לכך מוצע כי עקרונות ההסדרה יכללו:

א. חובה כללית על עיצוב לפרטיות (Privacy by Design), באופן שנועד להגן על פרטיות קטינים ולמזער את הסיכונים לפגיעה בהם.

ב. איסור על פעולות ניצול לרעה של חולשותיו של קטין ואיסוף מידע שאינו הוגן.

ג. איסור על איסוף מידע אודות ילד מתחת לגיל 14 ללא הסכמה הורית, ואיסור איסוף מידע רגיש מתחת לגיל 18. האיסור יחול בצורה מלאה על מי שפונה לקטינים, ויטיל חובת זהירות גם על מי שפונה לקהל כללי (כלומר לא לקטינים בלבד) לוודא כי הוא אינו עובר על הוראה זו.

ד. בעת קבלת הסכמה, יידרש חיוב במסירת מידע תמציתי וברור להורים וקטינים אודות השימושים המבוקשים במידע על מנת לאפשר "הסכמה מדעת" לשימוש במידע על אודותם.

ה. חיוב ספקים האוספים מידע אודות קטינים בעריכת מסמך "מדיניות פרטיות" וכן עריכת תמצית בהירה של מסמך זה.

ו. איסור פרסום מידע המאפשר לזהות ילד מתחת לגיל 14.

ז. עידוד בקרה עצמית באמצעות עמידה בהוראות התקנות על ידי גורם בלתי תלוי.

להשלמה יצוין כי עמדת רמו"ט היא כי המשפט אינו הכלי היחידי להגנה על קטינים; לצד ההסדרה המוצעת, יש לקדם ולחזק את העלאת המודעות והחינוך לפרטיות של קטינים, הוריהם, אנשי חינוך ורווחה וגורמים אחרים בעלי השפעה, ורמו"ט פועלת גם במישור זה.

ו. תקנות אבטחת מידע

בפברואר 2010 הפיצה רמו"ט נייר עמדה ובו הצעה לתיקון תקנות הגנת הפרטיות (אבטחת מידע). הנייר כולל הסדר מודולרי המטיל חובות בתחום אבטחת המידע.

נייר העמדה הוצג לראשונה במסגרת כנס שנערך במסגרת תוכנית ה- twinning, ולאחר מכן במסגרת כנסי אבטחת מידע שונים. תגובות קהילת אבטחת המידע ככלל היו אוהדות לכוונה זו, בשל הצורך בהנחייה מעודכנת בנושא דינאמי 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

בעקבות ההערות שהתקבלו תעביר רמו"ט לאישור מחלקת ייעוץ וחקיקה ולאחר מכן לשר המשפטים בתחילת שנת 2011 גרסה מעודכנת של התקנות המוצעות.

ו. הנחיות

במהלך שנת 2010 רמו"ט הפיצה טיוטת הנחייה בנושא מיקור חוץ (outsourcing) של מאגרי מידע. הוראות אלה נועדו לסייע לבעלי מאגרים במילוי חובותיהם על פי חוק הגנת הפרטיות בעת ביצוע מיקור חוץ. המסמך נועד גם להצביע למחזיקים במידע על מארג הדרישות המצופה מהם כנותני שירותים במידע רגיש.

לטיוטת ההנחיה התקבלו מספר לא רב של הערות הוא צפוי לצאת כהנחייה סופית במהלך שנת 2011.

ז. נייר עמדה בנושא השימוש במצלמות מעקב

בנובמבר 2010 פרסמה רמו"ט חוות דעת בנושא השימוש במצלמות מעקב במרחב הציבורי.

הצורך בנייר העמדה נובע מכך שבמהלך העשורים האחרונים צובר תאוצה השימוש במערכות טלוויזיה במעגל סגור לצרכים שונים, כגון מניעת עבירות והכוונת תנועה. בישראל זכו מצלמות המעקב לתשומת לב ציבורית לאחרונה בין השאר לאור השימוש בהן בתכנית "עיר ללא אלימות" המופעלת בכ-80 רשויות מקומיות ברחבי הארץ, ולנוכח יוזמות פרטיות להפעלתן במקומות רגישים כדוגמת בתי ספר.

למצלמות המעקב השפעה מהותית על המרחב הציבורי והשימוש בהן כרוך בפגיעה בפרטיות התושבים המצולמים. למרות זאת עד היום לא גובשה מדיניות מקיפה בנושא ולא נבדקו כל ההיבטים המשפטיים של הפעלת המצלמות.

חוות הדעת שהוכנה בנושא במחלקה המשפטית ברשות למשפט, טכנולוגיה ומידע, מבהירה את תחולתם של דיני הפרטיות והגנת המידע על השימוש במצלמות המעקב, ומציגה את עקרונות השימוש במצלמות לאור דיני הפרטיות.

השימוש במצלמות המעקב כרוך בפגיעה בזכות לפרטיות, ועל אוסף הצילומים המוקלט חלות במקרים מסויימים הוראות חוק הגנת הפרטיות, התשמ"א-1981 הנוגעות ל - "מאגר מידע", אשר הפרתן עלולה להגיע כדי עבירה פלילית. כך למשל יש להגדיר מראש מהי תכלית הצבת המצלמה ולהשתמש בצילומים רק למטרה שנקבעה מראש. הפרטיות היא גם זכות חוקתית

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

מוגנת, ולכן קבלת ההחלטה על עצם הצבת המצלמה חייבת לעמוד במבחן המידתיות, אם היא מותקנת בידי רשות ציבורית או בנסיבות רלבנטיות אחרות.

בהתאם לחוות הדעת, הגנת הפרטיות צריכה לשמש שיקול מרכזי גם בתכנון מערכת המצלמות ובאופן השימוש השוטף בהן, וזאת בהתאם לתפיסת "תכנון לפרטיות" (Privacy By Design) ולעקרון המידתיות - למשל ביחס למיקום התקנת המצלמות ולזוויות הצילום שלהן. לפי הוראות החוק, יש ליידע את הציבור על הצבת מצלמות המעקב לפחות באמצעות שילוט קריא וברור בסמוך למקום התקנתן; את הקלטות הצילומים אין לשמור לזמן ארוך יותר מן הנחוץ במישרין לצורך הגשמת מטרת התקנת המצלמה, וכל עוד הן נשמרות מקנה החוק למצולמים זכות לעיין בהקלטות הנוגעות להם; החוק גם מחייב לוודא את אבטחת המידע הנקלט ונאגר במערכת המצלמות, והסקירה מצביעה על האחראים לקיום החובה ועל האמצעים המינימאליים שיש לנקוט לצורך השגת רמה נאותה שלה.

ט. עיקולים מקוונים

במסגרת חוק ההסדרים נכלל פרק המתקן את פקודת המסים (גבייה) וקובע הסדרים להטלת עיקולים באמצעים ממוחשבים, תוך שימוש בחתימה אלקטרונית כהגדרתה בחוק חתימה אלקטרונית, התשס"א-2001.

רמו"ט היתה שותפה לניסוח החקיקה, וכן לדיונים בועדת החוקה, חוק ומשפט של הכנסת בהיבטי ההסדרה המשפטיים של נושא זה, עד לאישור החוק.

י. נייר עמדה בנושא ביטול כלל הראיה הטובה ביותר

בהצעת חוק לתיקון פקודת הראיות (מספר 15) (העתק ומקור), התשס"ו-2006, ביקש משרד המשפטים לבטל את "כלל הראיה הטובה ביותר". בדיון בהצעת החוק בועדת החוקה, חוק ומשפט של הכנסת בשנת 2006 נשמעו הערות ביחס לצורך בפירוט רב יותר בהסדרה של נושא זה, במיוחד ביחס למערכות ארכיבאות אלקטרונית.

בעקבות בחינת היבטים אלה, גובשו על ידי הרשות למשפט טכנולוגיה ומידע, על דעת מחלקת ייעוץ וחקיקה (פלילי) במשרד המשפטים, הצעות קונקרטיות להסדרה של נושא זה, בדרך של מודל משולב הכולל הוראות מפורטות יותר מהצעת החוק בחקיקה, והוראות משלימות בתקנות.

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

במאי 2010 הפיצה רמו"ט נייר עמדה בנושא ביטול כלל הראיה הטובה ביותר וארכיבאות אלקטרונית. לנייר העמדה הגיעו מספר תגובות והן מעובדות על ידי רמו"ט, על דעת מחלקת ייעוץ וחקיקה. מטרתו של נייר העמדה לקבל את תגובות גורמי המקצוע העוסקים בנושא זה בתחום המשפטי, הארגוני ובתחום מערכות המידע, לקראת הפצת תזכיר הצעת חוק.

יא. מדריך פרטיות בעבודה

במהלך שנת 2010, כתוצאה מתוכנית ה-twinning עם הרשות הספרדית להגנת מידע אישי, הוחל בכתיבה של מדריך לפרטיות במקום העבודה, אשר אמור לשמש מעסיקים בסקטור הציבורי והפרטי לשם הבנת החובות החלות כלפי עובדיהם באיסוף, שמירה וניהול המידע האישי שלהם.

עיקר העבודה של כתיבת מדריך זה הסתיימה לקראת סוף השנה, אך הפצתו נדחתה בשל אי-בהירות לגבי המצב המשפטי העדכני בעקבות הגשת ערעור על פסק הדין של בית הדין הארצי לעבודה בע"ע 90/88 טלי איסקוב ענבר נ' הממונה על חוק עבודת נשים ואח'.

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. פעילות בינלאומית של רמו"ט

ג. שבוע בינלאומי של "פרטיות במידע" בירושלים

בתאריכים 25-29 באוקטובר 2010 אירחה רמו"ט בירושלים שני כנסים בינלאומיים מרכזיים בנושא פרטיות במידע:

א. כינוס של ועדת ICCP של ארגון ה-OECD לציון 30 שנה להנחיות הארגון בנושא פרטיות והעברות מידע ("כנס ה-OECD").

ב. הכנס הבינלאומי ה-32 של רשויות הגנת מידע אישי ופרטיות ("הכנס הבינלאומי")

אירועי שבוע זה נקראו "שבוע הפרטיות במידע" (privacy week), ובמסגרתו נערכו אירועים נוספים הקשורים להגנת הפרטיות במידע, כמפורט בהרחבה להלן.

1) כינוס ועדת ICCP של ה-OECD - 30 שנה להנחיות הארגון בנושא פרטיות והעברות מידע



שבוע הפרטיות החל בכינוס חגיגי של ועדת ה-ICCP (Information, Communication and Computers Policy) של ארגון ה-OECD, ועדה אשר רמו"ט ביחד עם משרד התקשורת משמשים כנציגי מדינת ישראל בדיוניה.

ראש רמו"ט משמש גם נציג ישראל בקבוצת העבודה WPISP (Working Party on Information Security and Privacy), אשר ציינה בשנת 2010 מלאת 30 שנה להנחיית ה-OECD בנושא של הגנת הפרטיות והעברות מידע בין-לאומיות[2]. הנחיית

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

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-OECD בנושא זה הינו המסמך הבינלאומי הראשון אשר עסק בסוגית הפרטיות במידע, ונחשב לאחת מאבני היסוד של הפרטיות במידע. בתהליך הצטרפות ישראל לארגון ה-OECD, נבחנה עמידת ישראל בהוראותיו, כמו גם בהנחיות מאוחרות יותר בנושאים אלה.

ביוזמת רמו"ט, קיבלה הנהלת ICCP את ההצעה כי הכינוס השני בין שלושת האירועים שתוכננו לציון 30 שנה להנחיה ייערך בירושלים, בצמוד לכנס הבינלאומי. הכנס הראשון של ה-OECD בנושא עסק בבחינת השפעת ההנחיה על גיבוש המדיניות בנושא הגנת פרטיות במידע ויישומה לאחר 30 שנה. הכנס בירושלים עסק בתפקיד המתפתח של היחיד בהגנת הפרטיות, בעולם שבו אנשים אינם רק נושאי מידע (data subjects) אלא גם יוצרי מידע (data publishers) בפלטפורמת Web 2.0. בסוף שנת 2010 נערך הכנס השלישי אשר עסק בהיבטים הכלכליים של מידע אישי.

את כנס ה-OECD פתח בערבו של ה-25 באוקטובר סגן מזכ"ל ה-OECD השגריר ריצ'רד באוצ'ר, אשר בירך את באי הכנס והודה למדינת ישראל על אירוח הכנס.

את ערב פתיחת הכנס חתם ראש הממשלה בנימין נתניהו נאום שסקר את המשק הישראלי והצטרפות ישראל לארגון ה-OECD, והציג את משנתו באשר לאתגרי הפרטיות במידע, והשלכתה על ישראל ומעמדה בעולם. נבקש להביא את הציטוט מדברי רוה"מ בסוגית הפרטיות ואבטחת המידע:

> *"...אני חושב שלישראל יש את היכולת להתחרות בשוק הגלובלי כיוון שאנו שמים דגש על יתרון המוח. אני חושב ששוק בעל זרימה חופשית של אינפורמציה ורעיונות, בו חברות ואנשים פרטיים יודעים להסתגל במהירות לעולם המשתנה תדיר, הוא אתגר שאנו יכולים לעמוד בו. **אני חושב שליתרונות שיש לנו בעידן המידע נלווה גם האתגר להבטיח סביבה שבה המידע מוגן, וזה דבר חשוב עבורנו ועבור כל מדינה חופשית בעולם, כיוון שאחד הדברים שאנו גאים בהם, כמו חברות חופשיות אחרות, הוא שיש לנו אינפורמציה חופשית.***
>
> ***אולם החופש הזה טומן בחובו גם סכנות רבות לפרטיות ולביטחון שלנו**. ישנן חברות ישראליות חדשות המתמודדות עם אתגר כפול זה. החברות הללו מצטיינות בפיתוח תוכנות המגנות על המידע, ואני יודע שככל שאתגר ההגנה על המידע במרחב הוירטואלי יהפוך יותר ויותר מורכב, כך חברות ישראליות ימשיכו לפתח טכנולוגיות פורצות דרך. **זו לא רק בעיה של אנשים פרטיים, אמנם, בראש ובראשונה זו בעיה של אנשים פרטיים- אם מישהו חודר למרחב שלך ברשת***

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

חברתית, ואני חושב שיש כאן כמה נציגים – האם Facebook כאן או Google? - כולם. זו לא רק בעיה שלך כצרכן או כאזרח, זו בעיה של המדינה וזו בעיה גם ברמה הבינלאומית. אם מישהו פורץ לתוך חשבון הבנק שלכם, זו בעיה שלכם, אבל זו גם בעיה של הכלכלה הלאומית וזו גם בעיה של מערכת הבנקאות הבינלאומית וזו בעיה של הקהילה הבינלאומית באופן כללי.

אנו נידרש לנקוט צעדים שיגנו על החברה שלנו, שיגנו על האזרחים שלנו, אבל גם על החברה שלנו. הגנה על האדם היא חלק מאותה הגנה לאומית ובינלאומית על החופש. אולם המדינות יידרשו גם לעשות מאמץ מיוחד כדי להגן על תעשיות מרכזיות, למשל הבנקאות, החשמל או השירותים הציבוריים. ***היכולת לאיים על הביטחון והפרטיות של האדם מאיימת גם על אינטרסים לאומיים ובינלאומיים חיוניים****, ואני מאמין שבמאה ה-21 הגנה על המרחב הוירטואלי הינה מרכיב קריטי בהגנה על ביטחונן של חברות חופשיות.*

לכן זהו אתגר אדיר. וזה אתגר שאני יודע שאתם מתמודדים איתו, עם אחד ההיבטים החשובים והיסודיים ביותר שלו, אולם זה יעסיק אותנו יותר ויותר ככל שהטכנולוגיה תתקדם והאתגרים ייערמו ויתרבו. האתגר הניצב בפנינו הוא לא רק טכנולוגי, לא במדינה הזו ולא ברחבי העולם. עלינו לאמץ סטנדרטים חדשים ותקנות חדשות, ואני בטוח שאנו מוכנים לכך. תהיה אולי תקופה של חוסר התמצאות. זה תמיד קורה עם כניסתן של טכנולוגיות חדשות לעולמנו, אבל באופן כללי, אנו מתקדמים לקראת עתיד טוב יותר.

העתיד הזה יחייב חינוך טוב יותר. אני רואה לנגד עיניי אוכלוסייה יותר אחידה שיש לה את האפשרות להעניק לכל ילד, לכל אזרח, את היכולת להיות חלק ממנה ולא להידחק לשוליים, ואין לי כל ספק שבתחומים הקריטיים הללו, וברבים אחרים, יש לנו הרבה מה ללמוד האחד מהשני.

זוהי הסיבה שאני מאמין שהמאמצים שעושה ה-OECD להתמודד עם הסוגיה הזו ועם סוגיות רבות אחרות בהן אנו דנים יחד יסייעו ביצירת סביבה שהיא חיונית לצמיחתנו המשותפת, אך גם לביטחוננו המשותף. זה אולי משהו שהוא עדיין לא לחלוטין מובן מאליו היום, אבל ***<u>היכולת להעניק לאנשים את הזכות לקדם את הרעיונות שלהם, לתעד את חלומותיהם, לתקשר האחד עם השני מבלי שתהיה להם תחושה של פלישה לפרטיות, תחושה שמישהו מחטט בחייהם האישיים,</u>***

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

<u>היא בעיניי אחד האתגרים האדירים של המאה ה-21 וזה משהו שיבטיח גם את המאה ה-22</u>. *(הדגשות של רמו"ט)*

דיוני כנס ה-OECD נפתחו בערבו של ה-25 באוקטובר במושב שעסק ב"פרטיות בעולם האינטרנט – מתעדים הכל ולא שוכחים דבר".

ביום הדיונים העיקרי, ה-26 באוקטובר התקיימו המושבים הבאים:

- יצירת מידע ושיתופו על ידי יחידים על אודות יחידים (Data Creation and Sharing by Individuals about Individuals)
- צבירת מידע אישי וניתוחו – יצירת פרופיל מידע אישי על אודות כל אדם (Aggregation and Analytics: Constructing an Individual Profile)
- מודעות, הבנה וקבלת החלטות על ידי יחידים לגבי מידע אישי (Awareness, Understanding, and Individual Decision-Making)
- עידוד יצירתיות בתהליכי הגנת מידע אישי (Fostering Innovations in Privacy Protection)
- משמעויות לקביעת מדיניות ציבורית להגנת פרטיות במידע אישי (Implications for Policy Making)

כנס ה-OECD הסתיים בדברי סיכום של הגב' ג'ניפר סטודארט, נציבת הגנת הפרטיות של קנדה.

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) הכנס הבינלאומי ה-32 של רשויות הגנת מידע – פרטיות:דורות



הכנס הבינלאומי הוא האירוע המרכזי של משטר הרגולציה של הגנת מידע אישי (privacy and data protection) בעולם. בכנס ה-31 שנערך במדריד, ספרד בחודש נובמבר 2009 התקבלה רמו"ט לכנס[3] וכן התקבלה הצעתה לארח את הכנס ה-32 בירושלים[4].

מטרת ארגון הכנס על ידי רמו"ט הייתה להשפיע באופן משמעותי על השיח הבינלאומי והלאומי בנושא פרטיות במידע, שכן הדיונים במסגרתו בוחנים את הנושאים המרכזיים המטרידים את העוסקים בתחום זה, כמו גם להביא את הנושאים המדוברים בכנס לידיעת הציבור הישראלי. מטרת משנית, אך לא נעדרת חשיבות, הייתה לחשוף את קהילת הפרטיות העולמית, קהילה העוסקת באופן יום-יומי בזכויות אדם, למדינת ישראל.

[3] הכנס הבינלאומי אינו, בשלב זה, ארגון בינלאומי אך יש לו כללים ברורים לזכות להשתתף במעמד של נציג. בשנים 2007-2009 רמו"ט השתתפה בו במעמד של משקיף, ולאחר שהוכיחה כי מתווה הפעולה של רמו"ט תואם את הדרישות המחמירות של הכנס באשר לעצמאות וסמכויות, התקבלה רמו"ט כחברה שוות זכויות בכנס ה-31 במדריד.

[4] ראו דו"ח רמו"ט לשנת 2009, בעמ' 16.

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

תוכנית הכנס שמה לה למטרה לבחון שלוש שאלות יסוד:

- האם כניסתן של טכנולוגיות מידע חדשות, בעיקר רשתות חברתיות כגון Facebook ו-Twitter, באמצעותן אנשים רבים משתפים מידע רב על אודותם מעידה כי משתנה תפיסת הפרטיות של האנושות והצורך בה?
- האם וכיצד ניתן להשתמש בטכנולוגיות מידע חדשות לצורך הגנה על הפרטיות, קרי כמגן ולא רק כחרב?
- מה טיבו של משטר ההסדרה הראוי בנושא פרטיות במידע, לאור השינויים הטכנולוגיים?

בראש ועדת ההיגוי המקצועית של הכנס עמד ד"ר עומר טנא מהמכללה למנהל, ובנוסף לראש רמו"ט יורם הכהן היו חברים בה עו"ד כריס קונר, שותף במשרד עורכי הדין הבינלאומי Hunton & Williams ועו"ד ג'ולס פולונצקי, העומד בראש קבוצת החשיבה Future of Privacy Forum.

תוכנית הכנס גובשה על מנת לבחון שאלות אלה. השתתפו בה מיטב המומחים בעולם מהממשל, האקדמיה, ארגוני זכויות האדם וחברות הטכנולוגיה בתחום המתפתח של הגנת הפרטיות במידע.

התמה המרכזית של הכנס, כמו גם שמו **פרטיות:דורות** (**privacy:generations**), היא כי אנו עדים לדור חדש של טכנולוגיות מידע חדשות בהן משתמש דור חדש של משתמשים צעירים, וכי שינוי דורי זה חייב להביא לדור חדש של רגולציה בתחום הגנת פרטיות, אשר מפנימה את השינוי.

את הכנס פתח שר האוצר של מדינת ישראל, ד"ר יובל שטייניץ אשר התייחס בדבריו למתח שבין חובת השקיפות והגנת הפרטיות אשר מגנה על המתחם הפרטי של אנשים.

לאחר מכן נשא דברים מר לורנס סטריקלינג, ראש ה-NTIA (National Telecommunication and Information Administration) במשרד המסחר האמריקאי, אשר הציג את היוזמות שמקדם הממשל האמריקאי בראשות הנשיא ברק אובמה בנושא הגנת הפרטיות, לרבות עיקרי התוכנית שגיבש משרדו להתמודדות עם הנושא.

אחרון הדוברים בפתיחת הכנס היה ראש רמו"ט, יורם הכהן, אשר פתח את דבריו בהצגת סרט שהוכן על ידי רמו"ט לכנס, המציג את אתגרי הפרטיות של זמננו. סרט זה זכה לתשואות רבות, ומשמש עד היום את רמו"ט לצורך הצגת מצב הפרטיות בימינו. ראש רמו"ט הציג בדבריו את טיבה של הזכות לפרטיות, מערכת האיזונים המורכבת שמתקיימת בינה ובין

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

ערכים נוגדים, פיתוחן של טכנולוגיות חדשות לעיבוד והפצה של מידע וקיומו של דור חדש של משתמשי מחשב, המחייבים אותנו לעדכן את תפיסת הרגולציה של הפרטיות במידע.

המושב המליאה הראשון של הכנס הוקדש ל[היכן אנו כיום? השינוי הבין-דורי בתפישת הפרטיות], דיון רב משתתפים ובין-דורי בשאלת ההבדלים בתפיסת הפרטיות בין דור ה"מדברי" לדור הפייסבוק והטוויטר. לאחר מכן פנה הכנס לשלושה מסלולים: טכנולוגיות חדשות, משתמשים חדשים ורגולציה חדשה. הנושאים שנדונו היו:

- [תוכניות ציות תאגידיות וסוכני אחריותיות] – עסק בהתפתחויות האחרונות במדיניות פרטיות תאגידית וקידום מודל האחריותיות (accountability) בארגונים המנהלים מידע אישי;
- [מאזכרי פרטיות (Privacy nudges): כלים ותוספים (add-ons) מקוונים לשמירה על פרטיות] – עסק באמצעים טכנולוגיים לשמירה על הפרטיות ולייידוע המשתמשים על שימושים שנעשים במידע על אודותם;
- [עולם חדש חכם? אינטרנט של חפצים (Internet of things)]- עסק בהשפעתו של המחשוב הנוכח בכל (Ubiquitous computing), מקום בו כמות אמצעי המחשוב שתהא קשורה לאדם תהא גדולה, ואלה יכילו פרטי מידע שונים לגביו, על פרטיותו;
- [הסכמה: אשליה או מציאות?] – עסק בבחינת השאלה האם יסוד ההסכמה, העומד בבסיסן של כל תפיסות הגנת הפרטיות, הוא עדיין מנגנון תקף לשימוש במידע אישי;
- [תפקיד הממונה על הגנת מידע אישי ופרטיות בארגון (CPO)]- עסק בניתוח התפקיד המתפתח של הממונה על הגנת מידע אישי ופרטיות בארגונים המעבדים מידע אישי;
- [קניין רוחני (IP) לעומת הגנת מידע אישי (DP): שיקולי פרטיות בעת אכיפת זכויות] – עסק במתח שבין הרצון לאכוף זכויות קניין רוחני לבין הפגיעה בפרטיות הגלומה בשימוש במידע האישי שנצבר במהלך השימוש בנכס הקנייני;
- [מערכות זהות: הגדרה עצמית של מידע (Informational self determination)] - עסק בזהות הדיגיטלית שנבנית לאנשים בעולם של רשתות חברתיות, והזכויות העומדות להן כתוצאה מכך;

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

- פילוח התנהגותי (Behavioral targeting): הערכת עשור של דיונים – עסק בניתוח העולם של שימוש במידע אישי הנצבר משימוש במערכות חינמיות למטרות שיווק ממוקד;

היום הראשון של הכנס נחתם במושב מליאה שני אשר עסק בסדר היום הרגולטורי של רשויות הגנת המידע האישי ברחבי העולם.

היום השני של הכנס נפתח במושב מליאה שלישי אשר עסק בעיצוב לפרטיות (Privacy by design), נושא אשר קודם מאוד על ידי רמו"ט. בהמשכו עסקו המסלולים השונים בנושאים הבאים:

- הזכות להישכח – עסק בתופעה שהרשת אינה שוכחת מידע, בן שהועלה על ידי האדם ובין על ידי אחרים, ומידע זה ממפותח לעד במנועי חיפוש וניתן לגישה בכל עת.
- פרטיות בשוק האפליקציות (APPs)- עסק בעולם המתפתח והולך של יישומונים (apps) בטלפונים חכמים, האוגרים מידע אישי רב כגון נתוני מיקום ושימוש.
- אתיקה של כריית מידע (analytics): מגבלות האנונימיזציה – עסק במגבלות של מערכות להתממה (אנונימיזציה) של מידע ככלי להגנה על הפרטיות ומתן אפשרות לשימושים מסויימים במידע.
- פרטיות, הגנת הצרכן והגבלים עסקיים – עסק בדומה, בשונה וביחס שבין ההסדרה של הגנת צרכן והגבלים עסקיים והסדרה הגנת הפרטיות
- איך הגענו לכאן? פרטיות, דת ותרבות – עסק במקורותיה הסוציולגים, התרבותיים והמשפטיים של הזכות לפרטיות
- התנגשות דינים – עסק בהתנגשות בין מערכות הסדרה שונות של שימוש במידע אישי לגבי מידע ברשת האינטרנט.
- מגמות חדשות במחקר רפואי: רפואה מותאמת אישית (personalized medicine)- עסק בפיתוחים חדשניים של תרופות מותאמות אישית על בסיס פרופיל גנטי מדויק של החולה, והשלכותיה על פרטיות.
- האח הגדול פוגש את האח הקטן: גישת המדינה לנתונים במגזר הפרטי – עסק בגישה של גופי אכיפת חוק אל מידע אישי הנאסף ומנוהל על ידי גורמים פרטים

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

הכנס הסתיים במושב מליאה רביעי, דיון מרתק על עתידה של הפרטיות: רגולציה בראי נורמות חברתיות.

רוב המושבים אוישו בנציגים מובילים מהאקדמיה, גופי ממשל, ארגוני זכויות אדם, רשויות הגנת מידע אישי ומגזר עסקי, כך שהדיון במסגרתם נתן מקום לכלל הדעות הרלוונטיות.

לצורך הכנס הוקם אתר אינטרנט ייעודי (www.privacyconference2010.com) בו מפורסמת תוכנית הכנס ומידע רב על אודותה. לאחר סיום הכנס הועלו לאתר זה צילומי וידיאו של רוב המושבים שהתקיימו בו.

במסגרת הכנס יוחד חצי יום לדיון סגור של רשויות הגנת הפרטיות בלבד (closed session). במסגרת זו העלתה רמו"ט לדיון בין רשויות הגנת המידע האישי את הסוגייה של שיתופי פעולה בין רשויות פיקוח על פרטיות לרשויות פיקוח אחרות הפועלות באותה טריטוריה (כגון היחס בין רשות הגנת מידע אישי לרגולטורים בנושא הגנת צרכן, הגבלים עסקיים, שוק ההון, ניירות ערך, אבטחת מידע, בטחון לאומי וכד').

סוגייה זו זכתה להתעניינות רבה של הרשויות המשתתפות. לקראת הכנס הפיצה רמו"ט שאלון שנועד למפות איזורי שיתוף פעולה ומחלוקת עם רשויות אחרות. בדיון הסגור הוצגו הממצאים מהשאלונים ונערך דיון פתוח על נושא זה.

הפורום הסגור של רשויות הגנת המידע האישי קיבל מספר החלטות:

- החלטה לקבל לכנס את רשויות הגנת המידע האישי הפדרליות הבאות: אלבניה, בולגריה, מקסיקו, מולדובה ורשות הסחר הפדרלית של ארה"ב, את רשויות הגנת המידע האישי האיזוריות הבאות: נובה סקוטיה (קנדה) ו-IAPDF (מקסיקו), את הארגון הבינלאומי הבא: ארגון הפיקוח המשותף על EuroJust.
- מספר החלטות אדמינסרטיביות הקשורות בניהול הכנס, לרבות החלטה על קיומו בשנת 2011 במקסיקו.
- החלטה הקוראת לקיומו של כנס בינלאומי בין-ממשלתי לקידום גיבוש מסגרת בינלאומית מחייבת להגנת מידע אישי ופרטיות
- החלטה לשינוי ושיפור אופן הפעולה של הכנס הבינלאומי, בהיבטים של קבלת חברים חדשים ומתן מעמד של צופה (observer) וכן הקמת מועצת מנהלים בת חמישה חברים לניהול הכנס, בהשתתפות נציגי ארבעת הרשויות אשר ארגנו את

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

הכנסים האחרונים ומארחת הכנס הבא (קנדה,צרפת/גרמניה, ספרד, ישראל ומקסיקו).

- החלטה המכירה בחשיבות תפיסת ה"עיצוב לפרטיות" (Privacy By Design) כמכשיר להגנת פרטיות במידע, ומעודדת רשויות הגנת מידע לקדם נושא זה במסגרת פעילותן.

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) אירועים נוספים בשבוע הפרטיות במידע

במקביל לשני הכנסים המרכזיים, התקיימו בשבוע הפרטיות במידע עוד מספר כנסי משנה אשר עסקו בפרטיות במידע.

א) כנס ה"קול הציבורי" – החופש והפרטיות של צרכנים דיגיטליים

הכנס של ארגון ה"קול הציבורי" (public voice), קואליציה של ארגוני זכויות אדם מרחבי העולם. הכנס שלהם, אשר נקרא "החופש והפרטיות של צרכנים דיגיטליים", נערך בבוקרו של ה-25 לאוקטובר.

לאחר ברכות פתיחה על ידי ראש רמו"ט, עסק הכנס בנושאים הבאים:

- שנה לאחר הצהרת מדריד (לתקנים בנושא פרטיות במידע)
- נושאים מתפתחים בנושא הגנת פרטיות במידע
- בניית תשתית בינלאומית להגנת מידע אישי ופרטיות
- המאבק כנגד סורקי גוף (body scanners) ותעודות זהות ביומטריות
- פיתוח השיח בין רשויות הגנת מידע אישי וגופי זכויות אדם

ב) המחקר העכשווי בנושא פרטיות – היבטים גלובליים

במושב זה אירחה רמו"ט מספר חוקרים אשר הציגו את עיקרי מחקריהם בנושאי ההיבטים הגלובליים של פרטיות במידע:

- עו"ד כריס קונר הציג את מחקרו בנושא "ההסדרה של העברות מידע בינלאומיות והגנת פרטיות: עבר, הווה, עתיד"
- מר ריצ'ארד פרסל הציג את מחקרו בנושא "היישום של הנחיות ה-OECD על ידי הסקטור הפרטי"
- פרופ' אהרון האופטמן וד"ר יאיר שרן הציגו את מחקרם בנושא "אתגרי בהערכת המשמעות הטכנולוגית והאתית של פרטיות"
- פרופ' קן במברגר הציג את מחקר השוואתי בינלאומי בנושא "פרטיות על קרקע המציאות"

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) היבטי פרטיות ב"רשת חכמה" (SMART GRID)

כנס זה, אשר אורגן על ידי הגב' אן קבוקיאן, נציבת הפרטיות של מחוז אונטריו בקנדה, עסק ב[היבטים היישומים של שמירה על הפרטיות ביוזמות המערבות "רשת חכמה" (Smart Grid)].

ד) פרטיות במכשירים ניידים

כנס זה אורגן על ידי ארגון ה-GSMA, הארגון המאגד את המשתמשים בטכנולוגיות סלולריות GSM ועסק ב[שאלות הייחודיות של פרטיות במכשירים סלולריים.]

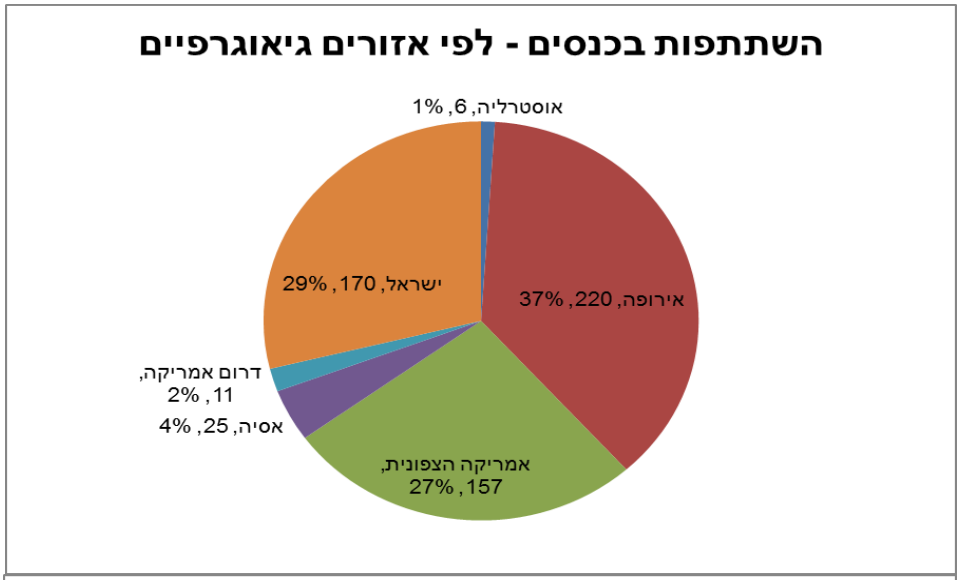
ה) הטמעת פרטיות בתוכניות ציות בישראל

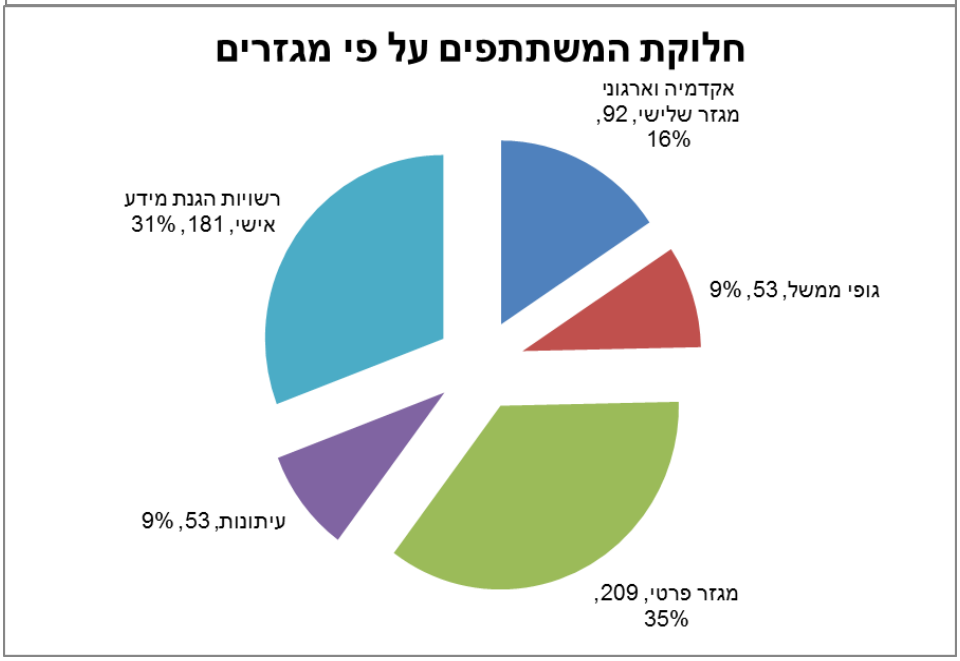
כנס זה אורגן על ידי חברת Privacy Laws & Business מבריטניה, המוציאה לאור ירחון בנושא פרטיות בהיבט הגלובלי, כמו גם מארגנת כנסים בנושא. הכנס עסק [בהטמעת ציות להוראות הגנת הפרטיות לחברות גלובליות הפועלות בישראל], לאור פעילותה של רמו"ט כרגולטור של הגנת מידע אישי.

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

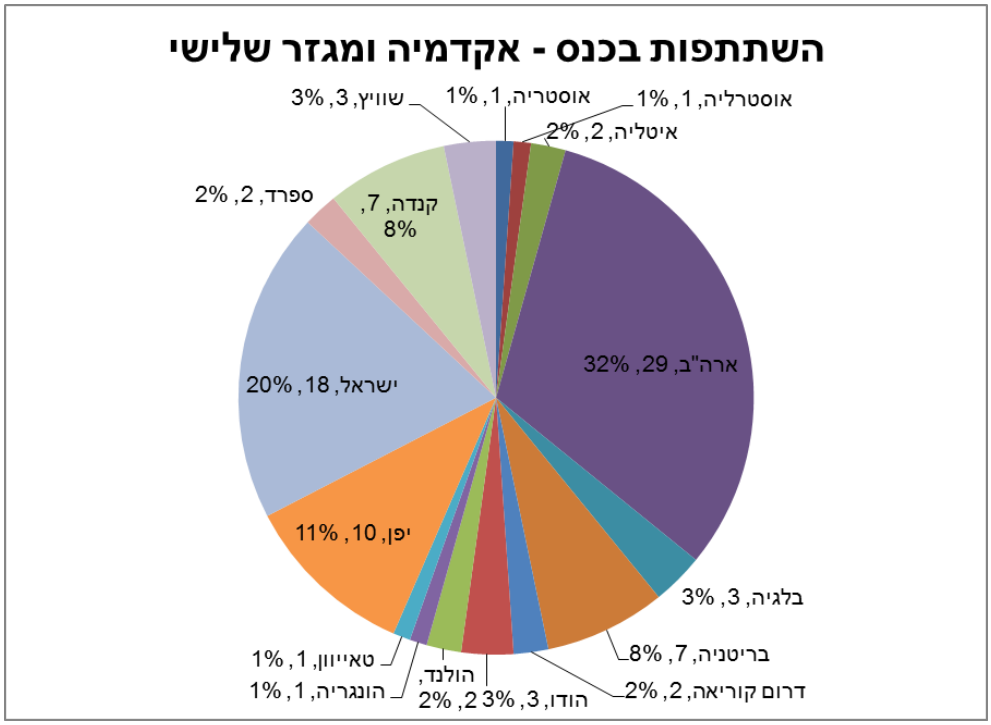
4) נתונים אודות ההשתתפות בכנסים

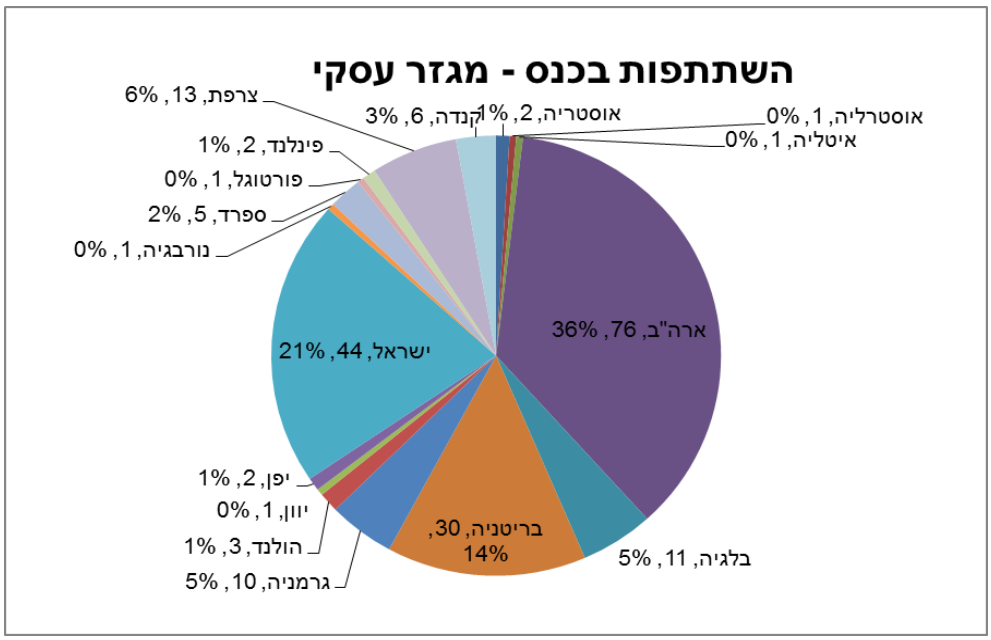
לשני הכנסים הגיעו כ-600 אנשים, כ-450 מהם מחו"ל. האורחים מחו"ל הגיעו מארבע יבשות (אמריקה הצפונית והדרומית, אירופה, אסיה ואוסטרליה) והיו בהם נציגים מרשויות הגנת מידע אישי, גופי ממשל, אוניברסיטאות וארגונים ללא כוונת רווח ומגזר פרטי. תמהיל המשתתפים מובא בשקפים הבאים:



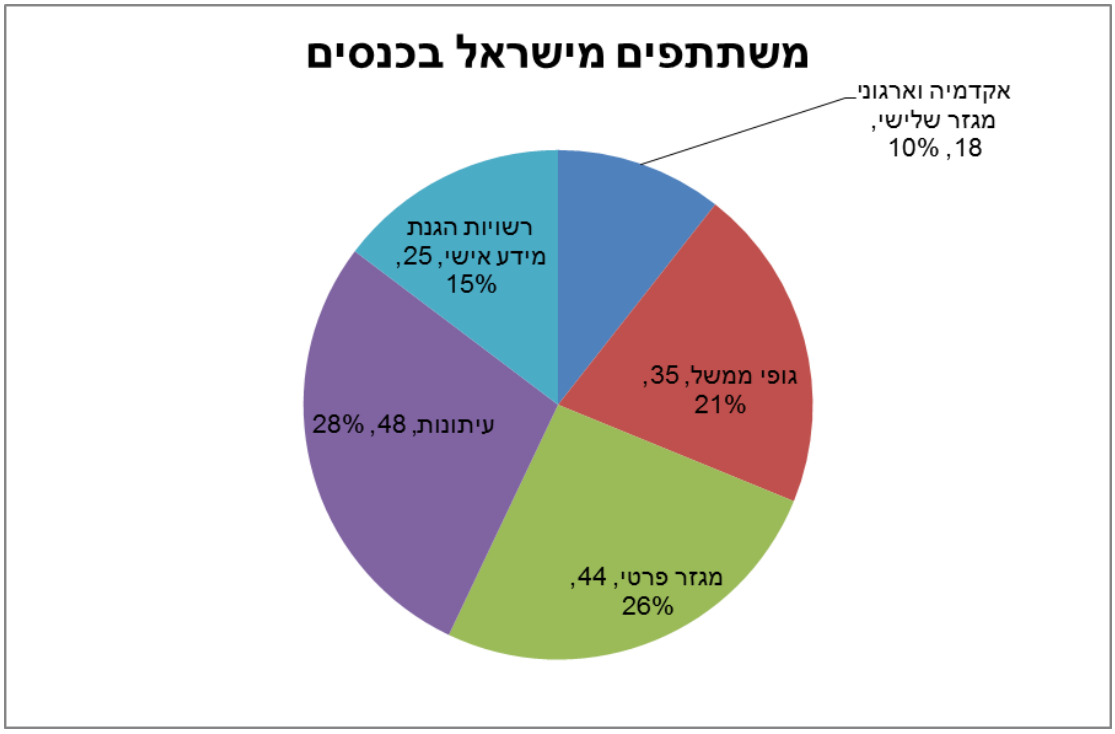


קרית הממשלה, ת.ד. 7360, תל אביב 61072. טל' 03-7634050 פקס: 02-6467064
The Government Campus, P.O.Box 7360. Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-6467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il





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



ב. החלטת הנציבות האירופית על רמת הגנת הפרטיות בישראל

במהלך שנת 2010 הסתיים תהליך ההכרה של הנציבות האירופית כי מדינת ישראל מקיימת רמת ההגנה על מידע אישי ופרטיות בישראל מספקת (adequate) את הסטנדרט הקבוע בדירקטיבה האירופית להגנת מידע אישי (EC/95/46) ועל כן עומד בדרישות סעיף 25(6) לדירקטיבה המאפשר העברה של מידע אישי על אודות אזרחים אירופאיים לישראל.

ההחלטה האירופית מנתחת את רמת ההגנה המשפטית על מידע אישי ופרטיות בישראל, וקובעת כי רמו"ט (ILITA – The Israeli Law, Information and Technology Authority) היא רשות הגנת מידע אישי (Data Protection Authority) ההולמת (Competent) את דרישות הדירקטיבה, כרשות האוכפת את דיני הפרטיות המקומיים.

החלטה זו של הנציבות היא תקדימית ברמה עולמית, שכן עד היום ניתן מעמד זה למספר מועט של מדינות (קנדה, שוויץ וארגנטינה ומספר הסדרי off-shore בתעלה הבריטית). החלטה זו מקילה באופן משמעותי על חברות ישראליות להציע שירותי עיבוד מידע אישי ללקוחות אירופים בלי מגבלות רבות החלות על מתחריהן ברחבי העולם. בצד זה, רמו"ט

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

תידרש להמשך חיזוק תשתית האכיפה שלה, ולוודא כי המשק הישראלי מתנהג בהתאם לעקרונות הקבועים בחוק הגנת הפרטיות.

החלטת הנציבות מובאת כנספח ב' לפרק זה.

ג. פרוייקט ה-TWINNING עם הרשות הספרדית להגנת מידע אישי

במהלך שנת 2010 התממשה מרביתה של תוכנית הצימוד (twinning) בין הרשות הגנת המידע הספרדית (AEPD) ורמו"ט. תוכנית זו, במימון הנציבות האירופית בתקציב של כמליון אירו, נועדה לחזק את תשתית הידע של רמו"ט כרגולטור מודרני של הגנת מידע אישי. התוכנית הושקה במחצית שנת 2009 לתקופה של 18 חודשים, והוארכה בסופו של עניין עד ל31 לינואר 2011.

במסגרת התוכנית נערכו מגוון של פעילויות במסגרתן הגיעו לישראל מיטב המומחים מאירופה בהיבטים השונים של הגנת מידע אישי. בתוכנית ה-twinning קבעה שלושה יעדים:

- חיזוק הידע המקצועי של רמו"ט כרגולטור של הגנת מידע אישי, לרבות הכשרת הצוות בסוגיות בינלאומיות של הגנת מידע אישי וגיבוש נוהלי עבודה.
- קיום סדנאות לציבור בנושאים מגזריים הקשורים בהגנת פרטיות, כגון ניהול מידע פרטי והגנת הפרטיות במגזר הציבורי ובגופי אכיפת חוק, ובמגזרי התקשורת, האינטרנט, הבנקאות, הביטוח, השיווק והדיוור ישיר, החינוך וקטינים, בשוק העבודה, בתחבורה, בהעברות מידע בינלאומיות, במצלמות מעקב ותפקיד הממונה על הפרטיות בארגון.
- העלאת מודעות לנושא הפרטיות בציבור הישראלי, על ידי קיום כנסים הפתוחים לציבור ופרסומם. פעולה משלימה לכך הייתה קיומו של סקר מקיף על אודות תפיסת הפרטיות של הציבור הישראלי. תוצאות הסקר השני שהתקיים בסוף שנת 2010 מובא כנספח א' לפרק זה.

בתוכנית התקיימו 28 פעילויות במסגרתן ביקרו 112 מומחים מ-16 מדינות האיחוד האירופי: ספרד (56%), בריטניה (12%), צרפת (6%), איטליה (4%), גרמניה (4%), הולנד (4%), סלובניה (3%), נורבגיה (2%), אירלנד (2%), צ'כיה (1%), שבדיה (1%), פורטוגל (1%), פינלנד (1%), ליטא (1%), פולין (1%) וקפריסין (1%). פעילויות אלה סיפקו לרמו"ט תמונה מפורטת ועדכנית

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

על תפישת הגנת המידע באירופה במגזר הציבורי והמגזר הפרטי, לרבות המגזרים הכלכליים העיקריים הנ"ל.

בנוסף, נערכו במסגרת התוכנית ובמימונה על ידי 24 עובדי רמו"ט 5 סיורים מקצועיים ברשויות הגנת מידע אישי באירופה (שני ביקורים בספרד, וביקור אחד בבריטניה, איטליה וצרפת). במסגרת הסיורים למדו עובדי רמו"ט להכיר לעומק ארבע רשויות הגנת מידע אישי אירופאיות והאופן שבהן הן פועלות, וקיבלו מידע מקיף על אודות המבנה הארגוני שלהן, סמכויותיהן, אופן פעולתן, תקציבן, הכשרת העובדים והקצאת המשאבים. על בסיס מידע זה, אמורה רמו"ט לגבש את התוכנית האסטרטגית שלה לשנים הקרובות.

תוכנית ה-twinning הניעה תהליכים רבים ברמו"ט, אשר מיעוטם בא לידי ביטוי כבר בשנת 2010, ורובם ישפיעו על התוצרים של רמו"ט בשנים הקרובות, כמו גם על אופן תפקודה. הידע וההבנה שנרכשו במהלך ניהול התוכנית בקרב עובדי רמו"ט, כמו גם החשיפה של הנושא לציבור הרחב הם בעלי ערך רב.

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. פרוייקט ה-ACCOUNTABLITIY

רמו"ט השתתפה בשנת 2010 במספר פגישות בינלאומיות במסגרת פרוייקט קידום האחריותיות (accountability) בהגנת מידע אישי. מדובר בפרוייקט משותף למרכז למדיניות ומנהיגות של משרד עורכי הדין הבינלאומי Hunton & Williams ורשויות הגנת מידע אישי מרחבי העולם. בשנת 2010 שמשה הרשות הספרדית להגנת המידע אישי (AEPD) כרשות העמיתה של התוכנית, והתוכנית נוהלה במשותף על ידי המרכז והרשות הספרדית.

במסגרת הפגישות מגובשת תפיסת אחריותיות (accountability) בניהול מידע אישי על ידי גופים פרטיים, ומגובשים המציינים (indicators) לזיהוי ארגון כבעל גישה אחריותית, כמו גם התהליכים שעל הארגון לבצע על מנת לעמוד בגישה זו.

קידום התפיסה של אחריות הארגון יאפשר למגזר הפרטי להמנע ממגבלות בירוקרטיות המוטלות על ידי רגולטורים, וזאת בתנאי שיוכח כי הוא מקיים באופן נאות את אופן הציות להוראות החוק בהקשר של הגנת הפרטיות במידע

ח. הצטרפות לרשת בינלאומית לאכיפת הגנת פרטיות - GPEN

במהלך 2010 הצטרפה רמו"ט לקבוצה המייסדת של הרשת הבינלאומית לאכיפה הגנת מידע אישי (GPEN - Global Privacy Enforcement Network), מהלך המובל על ידי רשות הסחר הפדרלית של ארה"ב (Federal Trade Commission), שהיא הרגולטור בנושא הגנת צרכן והגבלים עסקיים.

מדובר ברשת שיתוף פעולה בין רשויות הגנת מידע אישי ברחבי העולם, הפועלת בחסות ארגון ה-OECD על בסיס הנחיה שגובשה בארגון בשנת 2007 לקידום שיתוף הפעולה בנושא אכיפת פרטיות ברחבי העולם.

בשלביה הראשונים GPEN משמשת כמרכז לחילופי מידע בין רשויות הגנת מידע אישי, תוך כוונה לשפר את שיתוף הפעולה באכיפה של נושא הפרטיות במידע, שהוא מטבעו נושא בינלאומי.

רמו"ט רואה חשיבות רבה בקידום שיתוף פעולה בינלאומי באכיפת הפרטיות במידע, אשר מטבעה בעולם מקושר באינטרנט היא משימה גלובלית ולא רק מקומית. המחוקק הישראלי

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

יצטרך לתת את דעתו לשינויים נדרשים בחקיקה, אשר תאפשר שיתוף פעולה כזה בין רמו"ט כרגולטור של הגנת מידע אישי, וגופים מקבילים ברחבי העולם.

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. דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2010 (מוגש למועצה להגנת הפרטיות מכח 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

ג. מבוא

בשנת 2010 הוציאה רמו"ט את יכולות האכיפה שלה מהכח אל הפועל, והגבירה באופן משמעותי את נוכחותה במשק הישראלי, הציבורי והפרטי כאחד.

בשנה זו הוטלו קנסות מינהליים ב-12 תיקי פיקוח שנוהלו מכוח סמכויות רשם מאגרי מידע. קנסות אלו הוטלו במקום בו הושגו ראיות ברמה המספקת להוכחת קיומה של הפרה של סעיף 31א לחוק הגנת הפרטיות, התשמ"א-1981 (בפרק זה – **החוק**) ברמה הנדרשת בהליך הפלילי[5]. במקום בו ממצאי הפיקוח לא סיפקו את רמת הוודאות הנדרשת במשפט הפלילי, אך על פי רמת הראיות הנדרשת בהליך מנהלי ניתן היה לקבוע כי בוצעה הפרה של החוק, קבעה רמו"ט כי התקיימה הפרה של הוראות החוק על ידי הגורם המפוקח. במקרה ראשון הוגשה תביעה ייצוגית כנגד אחד הגופים המפוקחים עקב קביעה כאמור.

במקום בו רמו"ט הטילה קנס מינהלי או קבעה הפרה, פרסמה רמו"ט את החלטתה באתר האינטרנט של רמו"ט בקישור:

http://www.justice.gov.il/MOJHeb/ILITA/Pirsumim/enforcementact.htm.

כמו כן, במקרים קונקרטיים, הנחתה רמו"ט את הגורמים המפרים לפעול לתיקון ליקוים או לשנות מפעילותן.

בשנה זו ניתן דגש על מענה מהיר לפונים לרמו"ט לצורך הגשת תלונה. בעקבות פעילות זו, בכ-90% מן הפניות ניתן מענה ענייני בתוך פחות מ-30 יום.

ד. נתונים

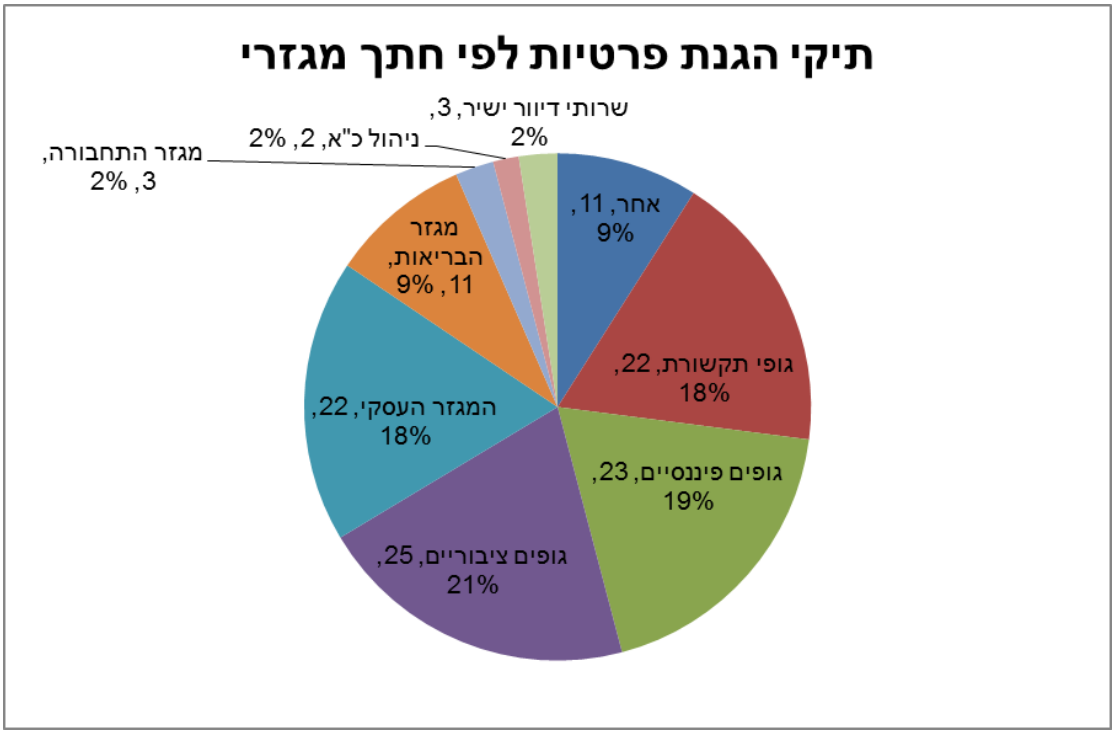
בתחום הגנת הפרטיות הוגשו בשנת 2010 233 תלונות, המהוות כ-80% מכלל התלונות שהגיעו לרמו"ט. ביחס לשנת 2009, עלתה כמות הפניות בתחום הגנת הפרטיות ב-117%, אולם נתח הפניות בתחום הגנת הפרטיות מכלל הפניות שהגיעו לרמו"ט, ירדה ב-8%. עליה דרמטית זו בכמות הפניות מיוחסת לחשיפה ההולכת וגוברת של רמו"ט בתקשורת ובציבוריות הישראלית ותהליכי העלאת מודעות שנעשים על ידי רמו"ט (דוגמת תוכנית ה-twinning והכנס הבינלאומי).

[5] מעל לספק סביר.

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

במהלך השנה נפתחו ברמו"ט 76 תיקי פיקוח בנושא הגנת פרטיות, המהווים 76% מכלל תיקי הפיקוח שנפתחו בשנה זו. בנוסף נמשך טיפול ב-46 תיקי פיקוח בתחום זה שנפתחו קודם לשנת 2010.

1) כמות התיקים שנוהלו לפי חתך מגזרי



2) הנושאים העיקריים שהטרידו את הציבור

הנושאים העיקריים שהטרידו את הציבור בתלונותיו, בהתאמה לסעיפי החוק השונים היו כדלקמן:

א. שימוש במידע שלא למטרה לשמה נמסר (סעיף 8(ב) לחוק) - כ-36%;

ב. פניות בלתי חוקיות בדיוור ישיר (סעיף 17ו לחוק) - כ-24%;

ג. אי מתן הודעה בטרם איסוף מידע למאגר מידע (סעיף 11 לחוק) – כ-10%;

ד. חוקיות מקורות המידע על בסיסם נעשתה פניה בדיוור ישיר (סעיף 17ה לחוק) – כ-10%;

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. אבטחת המידע במאגרי המידע (סעיף 17 לחוק) – כ-9% ;

ג. תיקי פיקוח נבחרים

1) מגזר ציבורי

א) עיריית רמת גן וחברת קידום

ברמו"ט התקבלה תלונה מתלמידת תיכון הלומדת ברמת גן על קבלת דיוור מחברת קידום שנועדה להציע למתלוננת, כתלמידת תיכון, הנחה בהשתתפות בקורס הכנה לבחינה הפסיכומטרית.

בעקבות פיקוח שביצעה רמו"ט התברר כי –

א. אגף החינוך של העירייה העביר כ-1500 מדבקות לחברה הכוללות שם וכתובת של תלמידי תיכוני העיר רמת גן, ללא קבלת הסכמה מפורשת של התלמידים או של האפוטרופוס שלהם.

ב. מקור המידע הינו מאגר מידע שבבעלות העירייה, ומטרתו הרשומה "רישום ושיבוץ ילדי תושבי רמת גן הלומדים במוסדות חינוך". בפנקס מאגרי המידע לא הייתה רשומה מטרת "שירותי דיוור ישיר".

חברת קידום שלחה מכתב פנייה לתלמידי תיכון בעיר רמת גן, ללא ציון כי הפניה היא בדיוור ישיר, ללא צירוף מספר הרישום של המאגר, ללא מתן הודעה על זכות מקבל הפניה להימחק מהמאגר בצירוף המען אליו יש לפנות לשם כך וללא ציון זהותו ומענו של בעל המאגר שבו מצוי המידע והמקורות שמהם קיבל בעל המאגר מידע זה.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי -

א. העירייה עשתה שימוש במידע שהיה ברשותה שלא למטרה לשמה הוקם המאגר, וכן עשתה שימוש במאגר לשרותי דיוור ישיר ללא רישום מטרה זו בפנקס, ומכאן כי העירייה הפרה את הוראות סעיפים 8(ב) ו-17(ד) בהתאמה. **על הפרות אלו הוטלו על העירייה קנסות מינהליים.**

ב. חברת קידום הפרה את הוראות חוק הגנת הפרטיות לנוכח אי קיום הוראות החוק הנוגעות למתן הודעה למקבל דיוור ישיר על מקור המידע על בסיסו נעשתה הפניה, ועל הזכות של מקבל הפניה להמחק מהמאגר ובכך הפרה את הוראות סעיף 17ו. **על הפרה זו הוטל קנס מינהלי על חברת קידום.**

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

ב) משרד התחבורה – כספי מג'יק

לרמו"ט הגיעה תלונה מאת נוסע בספינה, על כי בעת עלייתו לספינה נדרשו הנוסעים לאפשר סריקה ביומטרית של טביעת האצבע שלהם מבלי שניתן להם הסבר בנוגע למטרת האיסוף, לשימושים בו או לחובתם החוקית למסור את טביעת האצבע המבוקשת.

בפיקוח שביצעה רמו"ט התברר כי –

א. באנייה קיים מאגר מידע ממוחשב אודות הנוסעים המכיל גם מידע רגיש כהגדרתו בחוק.

ב. סריקת טביעת האצבע נלקחה, בעקבות דרישה של משרד התחבורה המעוגנת בנוהל אוניות נוסעים זרות (להלן - אנ"ז), ומצורפת למאגר.

ג. לנוסעים לא נמסר מידע מוקדם על תהליך סריקת טביעות אצבע והכנסתם למערכת.

ד. על אף שהחברה הודיעה כי המידע נמחק מהמאגר בסיום ההפלגה, אין כל מידע ודאי מה נעשה במידע הממוחשב.

בעקבות ממצאים אלה פנתה רמו"ט למשרד התחבורה, שבשל דרישתו בוצע איסוף המידע הביומטרי, לבירור סיבת דרישת איסוף המידע הביומטרי. לאור תשובות המשרד הורתה רמו"ט לשנות את הנוהל ולהוסיף בו את המרכיבים הבאים –

א. ציון בנוהל אנ"ז כי חוק הגנת הפרטיות חל על מידע ממוחשב הנוגע לנוסעים באנייה הפועלת לפי נוהל זה;

ב. הוספת הנחיות קונקרטיות בנוהל בנוגע לסוגיות הבאות –

1) חובת ההודעה על אוסף המידע, כאמור בסעיף 11 לחוק;

2) אחריות קב"ט הספינה למידע שנאסף מתוקף הנחיות הנוהל;

3) אחסון (מיקום) המידע ומורשי גישה;

4) חובת מחיקת המידע עם סיום ההפלגה תוך מתן הנחיות כיצד תבוצע המחיקה ועל מי האחריות לביצוע. בנוסף, הגדרת המקרים החריגים בהם יש צורך בשמירת המידע;

5) הנחיית סוכני האניות או בעלי או מפעילי המיזם, על חובתם לפרסם את מדיניות הפרטיות של מאגר המידע באתר האינטרנט של החברה ובדפי מידע שימסרו לנוסעים עם רכישת הכרטיסים, באופן בולט וברור, תוך ציון הפרטים הנדרשים בסעיף 17ו(א) 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

נוהל האנ"ז תוקן על פי דרישת רמו"ט.

ג) משרד התחבורה – חברת הפניקס

לרמו"ט הגיעה תלונה אודות מידע המועבר ממשרד התחבורה לידי חברות הביטוח במסגרת ניהול תביעות על תאונות המעורבים בהם כלי רכב.

בעקבות פיקוח שביצעה רמו"ט התברר כי –

א. העברת המידע לחברות הביטוח בעקבות אירוע ביטוחי מעוגנת בסעיף 82 לפקודת התחבורה [נוסח חדש] ובתוספת החמישית לפקודה זו, ומרבית המידע שהועבר מוסדר בחקיקה ;

ב. הועבר מידע עודף אודות כל הבעלים הקודמים של הרכב, ובכלל זה שמותיהם ומספרי הזיהוי שלהם (ת.ז או ח.פ), ללא שההעברה הוסדרה בחקיקה.

בעקבות ממצאי הפיקוח פנתה רמו"ט למשרד התחבורה והצביעה על הפער בין המידע הנמסר בשאילתא לבין הסמכות על פי חוק.

משרד התחבורה קיבל את מסקנות רמו"ט והתחייב **לבצע תיקון במערך הממוחשב אשר ימנע את העברת המידע העודף האמור.**

ד) מפלגת חד"ש

לרמו"ט הגיעה פניה אשר טענה כי חתך מפנקס הבוחרים, אודות בוחרים מהמגזר הערבי, מצוי באתר אינטרנט הפתוח לעיון הציבור.

בעקבות הפניה איתרה רמו"ט את מפעיל אתר האינטרנט, אשר הסיר את התכנים פוגעי הפרטיות מהאתר **באופן מיידי**.

מהבדיקה התברר, כי פעיל המפלגה, אשר סייע בהערכות המפלגה לבחירות, הגדיר בטעות את התכנים האמורים כתכנים הנגישים לכלל הציבור.

ה) הנהלת בתי המשפט

לרמו"ט הגיעה תלונה בה נטען כי פורסם באופן אלקטרוני, לכאורה, פסק דין שניתן בהליך שהתנהל בדלתיים סגורות כאשר הפרסום כלל פרטים חסויים. פסק הדין פורסם, לטענת המתלונן, באתר האינטרנט הרשמי של הרשות השופטת (www.court.gov.il), וכן באתרים פרסום מידע משפטי נוספים.

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

בעקבות פיקוח שביצעה רמו"ט התברר כי קיים ליקוי אבטחה המאפשר נגישות לפרטים מזהים של צדדים שפרטיהם נחסו על פי סעיף 70(א) לחוק בתי המשפט, למי שאינם מורשי גישה למידע האמור והם המו"לים של פסקי דין.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי –

א. לאור חובת הסודיות הקבועה בסעיף 70(א) לחוק בתי המשפט, הנגשת פסקי דין חסויים למי שאינו מורשה על פי דין מהווה פגיעה בפרטיות לפי סעיפים 2(7), ו-2(10) לחוק הגנת הפרטיות.

ב. הנגשת מידע מוגן פרטיות לגורמים שאינם מורשים מהווה מסירת מידע אסורה מגוף ציבורי בניגוד לסעיף 23ב(א) לחוק;

ג. הופרה חובת אבטחת המידע הקבועה בסעיף 17 לחוק הגנת הפרטיות.

הנהלת בתי המשפט לא חלקה על ממצאי הפיקוח ומשמעותם, **והתחייבה לתקן את הכשל האבטחתי**.

2) מגזר פרטי

א) חברת AIG

לרמו"ט הגיעה תלונה בה נטען כי חברת AIG ישראל, חברה לביטוח בע"מ, השתמשה במספר הטלפון החסוי שנמסר לה לצורך הפעלת ביטוח נסיעות לחו"ל, לשימושים אחרים שאינם קשורים במטרת מסירת המידע, הצעה שיווקית של ביטוח משכנתא, מבלי שקיבלה את הסכמתו של המלין.

בעקבות פיקוח שביצעה רמו"ט התברר כי –

א. המלין מסר פרטים לחברה לצורך קבלת שרות מסוים ולולא נמסרו הפרטים לא ניתן היה להפעיל את הביטוח. תקופת ההתקשרות עם החברה הוגדרה על ידי המלין לתקופה קצרה וקצובה (תקופת השהות בחו"ל). המלין לא נשאל ועל כן גם לא הביע את הסכמתו לקבל מהחברה מידע שיווקי.

ב. בנוסף, המלין דאג כי מספר הטלפון שלו יהיה חסוי מאחר ואינו מעוניין שיפנו אליו מבלי הסכמתו.

ג. המלין לא מסר הסכמה מדעת כנדרש בחוק לשימושים נוספים ע"י החברה.

ד. במהלך ההתקשרות נשאל המלין על ידי נציג החברה האם ברצונו לקבל הצעות ביטוח רכב וסירב.

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. החברה לא ביקשה במהלך השיחה את הסכמת המלין להשתמש במידע השמור במאגר המידע שלה למטרות שיווקיות מטעמה.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי החברה הפרה את –

א. הוראות סעיף 1 לחוק הגנת הפרטיות הקובע כי לא יפגע אדם בפרטיות של זולתו ללא הסכמתו;

ב. הוראות סעיף 2(9) שימוש במידע שלא למטרה לשמה נמסר;

ג. הוראות סעיף 11 לעניין ההודעה שנדרש מבקש מידע לשם החזקה במאגר מידע ושימוש בו, למסור לאדם. **בגין הפרת הוראות סעיף זה, הוטל על החברה קנס מינהלי.**

ב) חברת דיילקום

ברמו"ט נתקבלה בקשת רישום מאגר מידע בשם "ספר טלפונים" מאת חברת דיילקום.

בקשת הרישום, תשובות החברה לדרישות למידע נוסף, ומידע נוסף על מעורבות החברה ופעילותה במתן שירותים למפלגות בתקופות הבחירות הארציות והמקומיות, העלו חשדות כנגד החברה על שימוש, לכאורה, במידע שמקורותיו אינם חוקיים, ועל כן הוחלט על ביצוע פיקוח.

בעקבות פיקוח שביצעה רמו"ט התברר כי –

א. חלק ממאגר המידע כלל מידע שמקורו בפנקסי הבוחרים של הבחירות הארציות ושל הבחירות של הרשויות המקומיות;

ב. נעשה שימוש במידע שבמאגר המידע שלא למטרות הבחירות לפי חוק הבחירות לכנסת.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי החברה עשתה שימוש במידע שמקורו בפנקס הבוחרים שלא למטרת מאגר פנקס הבוחרים, ובשל כך ביצעה הפרה של סעיף 8(ב) לחוק.

לפיכך החליטה רמו"ט כי –

א. החברה הפרה את הוראות סעיף 8(ב) לחוק, **ובגין הפרה זו הוטל עליה קנס מינהלי;**

ב. בקשת רישום מאגר המידע סורבה בהתאם לסמכות רשם מאגרי מידע בסעיף 10(א)(1) לחוק;

ג. על החברה לבער מיידית את מאגר המידע וכל עותק ממנו המצוי בשליטתה.

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) בנק הפועלים

לרמו"ט הגיעה תלונה בה נטען כי בנק הפועלים, סירב לבקשות המתלונן להציג בפניו את המידע שבמאגרי הבנק ואשר הביא להחלטת הבנק לסמן אותו כ"סיכון עסקי".

בעקבות פיקוח שביצעה רמו"ט התברר כי –

א. בתקופה שבין 2007 - 2009 פנה המלין לבנק מספר פעמים בבקשת עיון במידע שנשמר עליו במאגרי הבנק;

ב. למעט מכתב אחד שנשלח מאת הבנק אשר נתן מענה כללי ביותר, ולא קיים את זכות העיון, הבנק לא השיב על פניותיו של המתלונן;

רק לאחר פניית רמו"ט לבנק, זומן המלין לבנק לפגישה בה הוצגו למלין מידע ומסמכים; טענת הבנק היתה כי למתלונן נמסר מידע רב בעל פה, אך לא היתה ביכולתו של הבנק להוכיח את האמור.

בעקבות ממצאי הפיקוח ולאור תקנה 5 לתקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), תשמ"א-1981, בה נקבע כי דין אי מתן תשובה למבקש תוך 21 יום מיום קבלת הבקשה כדין הודעת סירוב, קבעה רמו"ט כי קיים ביסוס עובדתי ומשפטי להפרה של בנק הפועלים את הוראות סעיף 13 לחוק.

על בנק הפועלים הוטלו שני קנסות מינהליים בגין הפרת הוראות סעיף 13[6].

ד) המשביר לצרכן

לרמו"ט הגיעה תלונה על כך שהמשביר לצרכן החדש בע"מ העביר מסר שיווקי, בהתבסס על מידע אודות תפקידו של אדם במקום עבודתו, ללא ציון הפרטים הנדרשים בסעיף 17ו(א) לחוק.

בעקבות הפיקוח שביצעה רמו"ט עלה כי –

א. המשביר לצרכן שלח מסר שיווקי בדיוור ישיר, בהתבסס על מידע ממאגר לשירותי דיוור ישיר של חברת bdi-coface הכלל מידע אודות 20,000 חברות ואנשי הקשר שלהן;

ב. במסר לא צוינו הפרטים הנדרשים בסעיף 17ו(א) לחוק;

ג. לא צוין כי הפניה היא בדיוור ישיר;

[6] רק לגבי שתי פניות ניתן היה לבסס ברמה הפלילית הנדרשת לצורך הטלת קנס מינהלי.

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. לא צוין מספר הרישום של המאגר המשמש לשירותי דיוור ישיר (מאגר בי די איי);

ה. לא ניתנה הודעה על זכותו של מקבל הפניה להימחק מהמאגר בצירוף המען שאליו יש לפנות;

ו. לא צוינו מקורות המידע.

לפיכך קבעה רמו"ט כי החברה הפרה את הוראות סעיף 17ו(א) לחוק, **ובגין הפרה זו הוטל על החברה קנס מינהלי.**

ה) בנק לאומי

ברמו"ט נתקבלה תלונה בגין שימוש במידע ממאגר קרן ההשתלמות מגדל פלטינום השתלמות לטובת גיוס לקוח, בניגוד לחוק, על ידי פקידת ייעוץ השקעות בסניף בנק לאומי בקניון חיפה.

בעקבות הפיקוח שביצעה רמו"ט עלה כי –

א. לפקידים בסניף הייתה גישה בלתי מוגבלת למאגר המידע של קרן ההשתלמות;

ב. בניגוד לנוהלי וחוזרי הבנק בעניין, שלפה הפקידה תדפיס יתרה של המתלונן מבלי לקבל הסכמה מפורשת מאת המתלונן, וזאת בניגוד לחוק, להנחיות רשם מאגרי מידע, ולהתחייבויות הבנק;

ג. השימוש האמור במידע מקרן ההשתלמות היה נוהג מקובל וחלק משיטת עבודה של פקידי הסניף ולא מדובר באירוע חד פעמי.

בעקבות פעולות הפיקוח נקט הבנק בצעדים הבאים –

א. הפצת חוזרים והנחיות לאחר המקרה, אשר מסדירים נקיטת אמצעים למניעת מקרים דומים בעתיד;

ב. חסימת הנגישות למאגר המידע של קרן ההשתלמות.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי -

א. שליפת תדפיס המידע ושימוש בו למטרות ייעוץ על ידי נציגת הבנק הינו שימוש במידע שלא כדין, המהווה פגיעה בפרטיות לפי סעיף 2(9) לחוק הגנת הפרטיות;

ב. השימוש במידע כאמור, הינו שימוש בניגוד למטרת מאגר המידע של קרן ההשתלמות, ובכך מהווה הפרה של סעיף 8(ב) לחוק הגנת הפרטיות. **בגין הפרת הוראות החוק הוטל קנס מינהלי על בנק לאומי.**

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. אי חסימת מאגר המידע של קרן ההשתלמות בניגוד להנחיות הספציפיות של רשם מאגרי מידע וראש רמו"ט מהווה הפרה של הוראת הרגולטור ומחדל אבטחת מידע חמור.

ו) ביטוח ישיר

לרמו"ט הגיעה תלונה כנגד חברת איי.די.איי חברה לביטוח בע"מ הידועה גם בשם "ביטוח ישיר" על כי סירבה לבטח רכבו של אדם על בסיס צווי עיקול אשר הגיעו אליה כצד ג'. אחד מהצווים הוטל בשנת 2002.

בעקבות הפיקוח שביצעה רמו"ט עלה כי –

א. בחברה נרשמו על שם המתלונן שני עיקולים בעקבות קבלת צו עיקול לצד שלישי מלשכת ההוצאה לפועל, שמטרתו דרישה מהחברה להודיע ללשכה על קיומו או העדרו של רכוש שהצו מבקש לעקל.

ב. החברה סירבה לבטח את המתלונן בהתבסס על מידע שנמצא במאגרי המידע שלה אודות עיקולי צד ג'.

ג. מקור המידע על נתוני עיקולי צד ג' הינו "מאגר ההוצאה לפועל" (מס' 980034030).

בעקבות ממצאי הפיקוח קבעה רמו"ט כי -

א. בהתאם להוראות פרק ד' לחוק ההוצאה לפועל, תשכ"ז – 1967 (להלן – חוק ההוצל"פ), נשלחים באופן שגרתי צווי "עיקול אצל צד שלישי" לבנקים, חברות ביטוח, קופות גמל, מוסדות פיננסיים וארגונים אחרים. בדומה, צווי עיקול זמניים נשלחים ל"מחזיקים" מכוח פרק כ"ח לתקנות סדר הדין האזרחי, תשמ"ד – 1984.

ב. הודעת העיקול הנשלחת לצדדים השלישיים ולמחזיקים, כוללת את שמו ומספר זהותו של החייב או הנתבע, ועשויה לכלול פרטי נכסים וזכויות השייכים לחייב ואת גובה יתרת חובו או הסכום הנתבע ממנו. נתונים אלה מעידים על מצבו הכלכלי של החייב ולכן הינם ידיעה על ענייניו הפרטיים וכן "מידע רגיש" אודותיו, כמשמעות המונח בסעיף 7 לחוק.

ג. המידע הכלול בצו העיקול נמסר לצד השלישי אך ורק למטרת קיום הוראות הצו: איתור נכסי החייב, הקפאתם תחת ידי המחזיק בהם ומסירתם לידי ההוצאה לפועל ככל שיורה כך צו שיפוטי. בהתאם, הצד השלישי רשאי לשמור את המידע על החייב רק ככל הנדרש לקיום הוראות צו העיקול.

ד. סעיף 7ב(ה) לחוק ההוצל"פ קובע, כי מי שהגיע אליו לפי החוק מידע על חייב לא יעשה בו כל שימוש ולא יגלה אותו לאחר, אלא במידה הנדרשת לביצוע הוראות חוק ההוצל"פ או על פי צו של בית משפט.

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. שימוש במידע הכלול בהודעת עיקול צד ג' החורג ממטרות הצו הקבועות בחוק ההוצל"פ, פוגע בפרטיותו של החייב מפני שהוא מהווה הפרה של חובת סודיות שנקבעה בדין לגבי ענייניו הפרטיים של אדם, כאמור בסעיף 2(7) לחוק.

ו. חריגה ממטרות צו העיקול פוגעת בפרטיות החייב משום שהיא מהווה שימוש בידיעה על ענייניו הפרטיים של אדם שלא למטרה לשמה נמסרה, כאמור בסעיף 2(9) לחוק.

ז. שימוש במידע הכלול בהודעת העיקול החורג ממטרות הצו, מפר גם את סעיף 8(ב) לחוק האוסר להשתמש במידע ממאגר מידע (שלענייננו הוא מאגר ההוצאה לפועל) "אלא למטרה לשמה הוקם המאגר". **בגין הפרה זו הוטל על החברה קנס מינהלי**

ח. הצד השלישי אינו רשאי לעשות במידע כל שימוש אחר החורג מקיום מטרות הצו, לרבות שימוש לצרכי הצד השלישי עצמו.

ט. גם אם הצד השלישי ממשיך להחזיק במידע לאחר תום תקופת צו העיקול מטעמים לגיטימיים הנובעים מהצו עצמו (כגון הצורך להתגונן מטענות בדיעבד שלא קיים את הצו כהלכה), אין הוא רשאי לעשות במידע שימוש למטרות זרות לצו העיקול כגון החלטה על אי מתן שירות או מוצר (אלא אם האדם נתן הסכמה חופשית ומודעת ספציפית לשימוש הנוסף).

י. יצוין, שלצד השלישי עומדים כלים חוקיים לברר מידע כלכלי אודות כל אדם, לרבות חייב לגביו נשלחה לצד השלישי הודעת עיקול, באמצעות הזמנת דו"ח אשראי מבעל רישיון שניתן בהתאם לחוק שירות נתוני אשראי, התשס"ב – 2002, ובכפוף לתנאים ולמגבלות המפורטים באותו חוק.

בעקבות הטלת הקנס המינהלי ביקשה החברה לבטל את הקנס, אולם בקשתה נדחתה על ידי הגורם המוסמך לנושא ברמו"ט.

כמו כן, בשל חשיבות הנושא, החליטה רמו"ט כי העניין נשוא התיק יובהר בהנחיית שוק ספציפית לנושא זה.

על עמדת רמו"ט בתיק זה, הגישה החברה, בפברואר 2011, עתירה לביהמ"ש המחוזי בת"א (עת"מ 24867-02-11) המתבררת בימים אלו.

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) שופרסל

לרמו"ט הגיעה תלונה על חברת שופרסל בע"מ, בה נטען כי החברה העבירה מסר שיווקי בדיוור ישיר, אשר לא הכיל את הפרטים הנדרשים מכח הוראות סעיף 17ו(א) לחוק.

בעקבות הפיקוח שביצעה רמו"ט עלה כי –

א. במהלך שנת 2010 רכשה שופרסל מחברת גילון בע"מ מידע אודות תושבים לפי בתי אב באזור פתח תקווה, מעל גיל 18 ;

ב. את המידע האמור היא הצליבה אל מול מידע שבידה על מנת למצוא חתך אנשים שאינם חברי מועדון שופרסל ;

ג. במהלך יולי 2010 שלחה שופרסל, תוך שימוש במידע שרכשה, מסר שיווקי בדיוור ישיר בין היתר למתלונן ;

ד. המידע הנדרש לפי ס' 17ו(א) לחוק לא נכתב באופן ברור ובולט היות ו –

1) המידע נכתב באותיות קטנות משמעותית מיתר המידע שבמסר השיווקי ;

2) המידע הובלע במשפט המתחיל במידע שיווקי אודות תקפות השוברים.

3) בעקבות ממצאי הפיקוח קבעה רמו"ט כי החברה הפרה את הוראות סעיף 17ו(א) לחוק, **ובגין הפרה זו הוטל על החברה קנס מינהלי.**

ח) חבר אוסקר החזרי מס – הכשלת פיקוח

בעקבות תלונה שהגיעה לרמו"ט אשר העלתה חשד לגבי חוקיות מקורות המידע של חברת אוסקר החזרי מס, התבצע פיקוח אשר במסגרתו הופעלה סמכות רשם מאגרי מידע מכח סעיף 10(ה1) לחוק ונדרשו ידיעות מחברת אוסקר.

משלא השיבה החברה לפניית רמו"ט, על אף תזכורות בנושא זה, הוחלט לבצע פיקוח במשרדי החברה על מנת לבחון את הנעשה בה באופן בלתי אמצעי.

בהגיע מפקחי רמו"ט לחברה, סירב אחד ממנהליה, מר נוי מורג, לשתף פעולה עם מפקחי רמו"ט ובכלל זה להכניסם לחברה, על אף שהובהר לו כי בהתנהגות זו הוא מבצע, לכאורה, עבירה פלילית ומפר את הוראות סעיף 288א לחוק העונשין.

בעקבות תוצאות הפיקוח, ולמען הסר ספק, נשלחה לחברה דרישת ידיעות נוספת ובה נכתב במפורש כי אי מילוי הדרישה מהווה עבירה פלילית כאמור לעיל. למצער, החברה עמדה בסירובה לשתף פעולה בכל דרך שהיא עם מפקחי רמו"ט.

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

לפיכך, ובשל ההתנהלות החריגה של מנהלי החברה ובא כוחה, הוגשה על ידי רמו"ט תלונה במשטרה על הפרת סעיף 288א לחוק העונשין. לאחר מספר חודשים נעצרו מנהלי החברה, בשל חשדות לביצוע עבירות לכאורה בתחום ההונאה. לאחרונה, השלימה המשטרה את פעולות החקירה לעניין הפרת הוראות סעיף 288א על ידי מנהלי החברה ובימים אלו אנו ממתינים להחלטת המשטרה באם להגיש כתב אישום כנגדם בעבירה זו.

ט) סלקום

ברמו"ט נתקבלה תלונה של תלמידת תיכון שאינה לקוחת סלקום, אשר קיבלה דיוור ישיר מחברת סלקום, המציע לה להצטרף כלקוחה במבצע המיועד לחיילים, מאחר שהיא עומדת להתגייס לצה"ל.

בעקבות הפיקוח שביצעה רמו"ט עלה כי -

א. הורי הנערה הם לקוחות סלקום, וסלקום טייבה את המידע על לקוחותיה (ביניהם הורי הילדה) באמצעות רכישת מידע מחברת תכלית (חברה לשירותי דיוור ישיר), על בסיס נתוני הלקוחות שהיו בידיה.

ב. בנוסף, סלקום רכשה מידע אישי דמוגרפי מפורט אודות קרובי משפחה מדרגה ראשונה של לקוחותיה, כגון המידע על הנערה.

ג. המידע שרכשה סלקום על קרובי משפחה של לקוחותיה פולח, בין היתר לפי איפיוני אוכלוסיה וגיל. לאחר מכן, סלקום שלחה פנייה אישית שיווקית בדיוור ישיר לחברי קבוצת גיל פוטנציאלית לגיוס לצה"ל.

ד. נוסח הדיוור של סלקום לא עמד בחובות החוק בפניה אישית לאדם:

1) הדיוור נשלח מבלי לציין בו כי הפניה היא בדיוור ישיר;

2) מספר הרישום של המאגר ממנו נלקחו פרטי הנמען לא צוין בפניה;

3) לא נתנה הודעה על זכות מקבל הפניה להימחק מהמאגר בצירוף המען אליו יש לפנות לשם כך;

4) לא צוינה זהותו ומענו של בעל המאגר שבו מצוי המידע והמקורות שמהם קיבל בעל המאגר מידע זה.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי בפעולות חברת סלקום החברה הפרה –

א. את הוראות סעיף 8(ב), בכך שעשתה שימוש במידע על לקוחותיה, לאסוף מידע נוסף שלא לשם מטרת הקמת המאגר ממנו נלקח המידע, והכל ללא הסכמתם;

ב. את הוראות סעיף 17ו(א) בכך שלא העבירה הודעה כנדרש בעת פניה בדיוור ישיר.

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

בעקבות החלטת רמו"ט ועל בסיסה הוגשה תובענה ייצוגית כנגד חברת סלקום בנושא נשוא התלונה.

י) מגדל

ברמו"ט נתקבלה תלונה בנוגע לאיסוף מידע עודף, לכאורה, של חברת מגדל על לקוחותיה ללא מתן הודעה כנדרש מכח הוראות סעיף 11 לחוק.

בעקבות הפיקוח שביצעה רמו"ט עלה כי -

א. החברה בחרה לשלב בטופס, באופן עמום ומסורבל, דרישת מידע שנדרש ישירות לצורך אספקת השירות המתחייב מפוליסת הביטוח, ועדכון רשומותיה על פי חוזרי הממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר, עם דרישת מידע שהיא וחברות הקבוצה בה היא מצויה מעוניינות בו.

ב. החברה לא הבהירה ללקוחותיה בצורה בהירה וברורה מה מטרת איסוף המידע ומהם השימושים שייעשו במידע שייאסף. כמו כן החברה לא הבהירה על גבי הטופס כי איסוף המידע אינו נדרש לצורך אספקת השירות נשוא הדיווח.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי -

א. קבלת הסכמה רחבה, כזאת המלווה בהסבר עמום ומסורבל, וללא הפרדה בין הסכמה למידע הנדרש לצורך מתן השירות לבין הסכמה למידע שלא נדרש, מעלה חשש באשר לעמידה בדרישות ההסכמה מדעת שבחוק, ובכך לחוקיות מנגנון קבלת ההסכמה שנעשה בו שימוש בפניה.

ב. דווקא לאור העירוב וטשטוש הגבולות בין המידע החיוני למתן השירות לבין המידע הוולונטרי, ולאור הסמיכות של טופס בקשת המידע לדו"ח המחוייב לפי דין, חייבת הייתה החברה לכתוב בטופס בשפה פשוטה וברורה, ברחל בתך הקטנה, שמסירת המידע היא וולונטרית לגמרי ואיננה נדרשת למתן השירות. **החברה לא עשתה כן ולפיכך נקבע, כי החברה הפרה את הוראות סעיף 11 לחוק בהתנהלות זו.**

ג. על החברה לבער את כל המידע שנאסף על ידה שלא כדין.

בעקבות עמדת רמו"ט הודיעה חברת מגדל כי היא **חדלה מאיסוף מידע** כאמור לעיל וכי **היא לא עשתה שימוש במידע שנאסף**. כמו כן הודיעה חברת מגדל על כוונתה **למחוק את כל המידע העודף כאמור בדרישת רמו"ט.**

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) חברת רותם חינוך בע"מ מפעילת "אור-אל חוויה לבר מצוה"

ברמו"ט נתקבלה תלונה על משלוח דיוור ישיר לביתו של נער בגיל בר מצוה לצורך שיווק שיעורי הכנה לבר מצווה לנוער בחתך הגיל המתאים. החברה נדרשה לתת מענה בדבר מקורות המידע על בסיסם נערכה הפניה. בסמוך לכך הגישה החברה בקשת רישום מאגר ונדרשה לדווח ולהציג את מאגר המידע שלה ומקורותיו.

בעקבות פיקוח שביצעה רמו"ט נמצא כי –

א. תשובות החברה היו חלקיות, בלשון המעטה, ועל פניו לא נתנו הסבר מניח את הדעת לעניין מקורות המידע של החברה ;

ב. מהמידע החלקי שהציגה החברה לבסוף עלה כי יש במאגרי המידע שלה מידע שלא מתקבל על הדעת שנתקבל ממקורות גלויים או בהסכמת נושאי המידע.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי התעורר חשד סביר בנוגע לחוקיות מקורות מאגר המידע של החברה. לחברה ניתנה הזדמנות לטעון והיא בחרה שלא לעשות כן.

לפיכך החליטה רמו"ט כי –

א. **בקשת הרישום נדחית** בהתאם לסמכות רשם מאגרי מידע בסעיף 10(א)(1) לחוק ;

ב. **על החברה לבער מיידית** את מאגר המידע וכל עותק ממנו המצוי בשליטתה.

החברה הגישה תצהיר מדווח כי ביערה את המאגר.

יב) JOBSPLACE.CO.IL

לרמו"ט הגיעה תלונה כנגד האתר jobsplace.co.il בטענה כי האתר פירסם את קורות החיים של המלין באתר האינטרנט ללא הסכמתו, וכי ניתן לאתר את קורות החיים גם במנוע החיפוש של חברת גוגל.

בעקבות הפיקוח שביצעה רמו"ט עלה כי -

א. בניגוד לטענות החברה קורות חיים ואף המלצות שהועברו אליה, היו חשופים בעת ביצוע חיפוש במנועי החיפוש ;

ב. החברה לא הרימה את הנטל להוכיח כי המשתמשים מודעים ומסכימים כי המידע אודותם, בקורות החיים או ההמלצות יהיו חשופים לחיפוש ישיר של מנועי החיפוש.

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. נדחתה טענת החברה כי ניתן להסיק מהעובדה כי משתמש שמפרסם מודעה מסויימת ומצרף קורות חיים והמלצות לבקשת עבודה מסוימת ברשת האינטרנט, נותן את הסכמתו לפרסום המידע האמור גם לכלל משתמשי הרשת.

בעקבות ממצאי הפיקוח הורתה רמו"ט לחברה לנקוט בצעדים לשם קבלת הסכמת המשתמשים לפרסום המידע למנועי החיפוש או לחלופין לחסום את הגישה למידע באתר החברה, למנועי החיפוש. **החברה מילאה אחר הדרישות וחסמה את המידע המצוי באתר שלה למנועי חיפוש.**

יג) חברת הראל

לרמו"ט הגיעה תלונה על כי חברת הראל, אשר זכתה במכרז חשכ"ל לביטוח כלי רכב של עובדי מדינה, מבקשת מכל מי שפונה אליה לקבלת הצעת מחיר בנושא ביטוח כאמור, למלא פרטים אישיים, ולהסכים לתנאי שימוש הכוללים, בין היתר, "הסכמה" להעברות מידע בין חברות קבוצת הראל.

ככל הנראה בשל תכתובת בסוגיות הנוגעות לפיקוח, **חברת הראל שינתה את הדרישה לקבלת מידע אשר היתה קיימת באתר** ובכך מיצוי הליך הפיקוח התייתר.

יד) טנא קט

לרמו"ט הגיעה פניה בשם יולדת אשר טענה כי חברת טנא קט עשתה שימוש במידע אודותיה ללא הסכמתה.

מהפיקוח שרמו"ט ביצעה עלה כי היולדת חתמה על טופס הסכמה בו פסקה מפורשת המצהירה על איסוף המידע למאגר מידע העברתו לחברות אחרות, מחיקתו לאחר שנתיים, ויידוע על זכותה של היולדת להמחק מהמאגר בכל רגע נתון.

עם זאת, רמו"ט פנתה לחברה על מנת שתתקן את הטופס כך שיופיע בו המידע הבא –

א. ציון מספר המאגר ומי הוא בעליו של המאגר;

ב. כיצד מועבר המידע לחברות האחרות (האם הן מחזיקות במידע או מקימות מאגר משל עצמן);

ג. פרטי הקשר להעברת בקשה למחיקה מהמאגר למימוש זכות היולדת על פי הטופס.

כמו כן רמו"ט דרשה כי עותק חתום יישאר בידי היולדת.

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

בעקבות דרישת רמו"ט תוקן הטופס כמבוקש והחברה התחייבה לפעול כמבוקש על ידי רמו"ט.

טו) חברת טלאול - סלקום

לרמו"ט הגיעה תלונה כי במהלך שיחה שיווקית של נציגת חברת סלקום ישראל בע"מ, לא מסרה הנציגה, למרות שנשאלה על כך, מהו מקור המידע שעל בסיסו בוצעה השיחה ומהו שם החברה המשווקת.

בעקבות הפיקוח שביצעה רמו"ט עלה כי –

א. חברת טלאול קונטקט סנטר בע"מ ביצעה את השיחה נשוא התלונה כמשווקת מטעם חב' סלקום. נציגת חברת טלאול הזדהתה כעובדת חברת סלקום.

ב. השיווק התבצע, בין היתר, על בסיס מידע שהתקבל מחברת "data-rings" המבצעת פעילות של שרותי דיוור ישיר.

ג. במהלך השיחה, ולמרות שנתבקשה, לא השיבה הנציגה למלין מהו מספרו הסידורי של מאגר המידע ממנו שלפה את המידע לצורך ביצוע השיחה ולא השיבה מהי החברה המשווקת בה היא מועסקת.

ד. מתשריט שיחה שנמסר עולה כי החברה אינה מטמיעה בקרב עובדיה את הצורך למסור מידע מקדים כאמור בסעיף 17ו(א) לחוק.

בעקבות ממצאי הפיקוח קבעה רמו"ט כי -

א. חברת טלאול הפרה את הוראות סעיף 17ו(א) לחוק.

ב. על החברה למלא אחר הוראות החוק במלואן, ובין היתר לפעול בנושאים הבאים –

1) הקפדה על קיום החובה לפי סעיף 17ו(א) בעת פניה לאנשים ;

2) הגברת הפיקוח על המשווקים (אנשי המכירות) מטעמה, ווידוא כי הם פועלים בהתאם לחוק ;

3) הבטחת אפשרות בירור תלונות בדרך של קיום שיחות מטלפונים מזוהים, כך שניתן יהיה לברר מה מקור השיחה.

חברת טלאול התחייבה לבצע הדרכות בנושא ולפעול למילוי הוראות חוק 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

טז) מכללת הייטק

לרמו"ט הגיעה תלונה בה נטען כי בוצעה פנייה בדיוור ישיר באמצעות דוא"ל למרות משלוח דרישה להסרה מרשימת התפוצה.

בעקבות הפיקוח שביצעה רמו"ט עלה כי על אף שתי פניות של המתלונן למכללה, לא הסירה המכללה את פרטי ההתקשרות עמו.

לפיכך קבעה רמו"ט כי המכללה הפרה את סעיף 17ו(ד) לחוק לפיה באם הודיע אדם לבעל מאגר מידע על דרישתו להמחק מהמאגר לצרכי דיוור ישיר, יפעל בעל המאגר בהתאם לדרישה, ויודיע לאדם בכתב כי פעל על פיה.

מכללת הייטק עדכנה את נציגי רמו"ט בדבר הצעדים שננקטו על מנת למנוע הישנות של מקרים דומים בעתיד.

יז) ארגון המורים

ברמו"ט נתקבלו תלונות כנגד ארגון המורים בבתי הספר העל יסודיים בסמינרים ובמכללות מהן עלה לכאורה, כי ארגון המורים או מי מטעמו, עשה שימוש במידע ממאגר מידע שבארגון המורים, לשם משלוח דיוור ישיר לצרכי תעמולת בחירות בבחירות הכלליות לכנסת של מפלגה בשם "מהפך בחינוך".

בעקבות הפיקוח שביצעה רמו"ט עלה כי הארגון שלח דיוור ישיר לחבריו המודיע על הקמת מפלגת "מהפך בחינוך", מבלי שפירט את כל הנדרש בסעיף 17ו (א) לחוק, וכשאופן משלוח הדיוור אינו מאפשר למקבלו לדעת, כי השולח הוא הארגון. עם זאת, לא נמצאו ראיות מספיקות לביסוס קביעת הפרות נוספות של החוק.

בעקבות ממצאי הפיקוח הורתה רמו"ט מהארגון לוודא כי להבא לא יבוצע דיוור ישיר מבלי לקיים את הוראות החוק.

יח) פנקס הבוחרים – מתמודד לראשות עיריית רחובות

המפקח על הבחירות במשרד הפנים פנה לרמו"ט בעקבות אי הסכמתו של מתמודד לראשות עיריית רחובות להחזיר עותק מפנקס הבוחרים לעירייה שהועבר לידו לצורך התמודדות בבחירות. פניותיו של המפקח על הבחירות למתמודד לא נענו.

בעקבות התערבות רמו"ט, ולאחר שהובהר לו המצב המשפטי, השיב המתמודד את התקליטור לידי המפקח על הבחירות.

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

יט) תלונה מהולנד

בתיק זה, טיפלה רמו"ט לראשונה בתלונה שהגיעה מחו"ל (הולנד). בתלונה טענה הפונה כי אתר אינטרנט המפרסם קשרי משפחה של משפחות יהודיות, פרסם פרטים אודותיה ואודות בני משפחתה.

בעל האתר, המתגורר בישראל, הצהיר כי המידע המצוי באתר נאסף ממקורות גלויים בלבד, עם זאת לאור בקשת המתלוננת התחייב למחוק את המידע נשוא התלונה.

י"ב. תיקי מבדק

1) מגזר ציבורי

ו) כרטיס חכם בתחבורה הציבורית

פרויקט הכרטיס החכם בתחבורה ציבורית הינו פרויקט לקידום השימוש בכרטיס אלקטרוני אישי הניתן לטעינה ("כרטיס חכם"), שנועד לשמש אמצעי תשלום בתחבורה הציבורית. הכרטיס החכם, הקרוי "רב-קו", ומערך הכרטוס מבוסס על התקינה האירופאית ה-Calypso[7] מטרת הפרויקט הינה לאפשר אמצעי תשלום אחד לכלל אמצעי התחבורה הציבורית במדינת ישראל, לרבות חברות האוטובוסים, רכבת ישראל והרכבת הקלה.

ההסדרה המשפטית של הפרוייקט בתקופת הזמן שנבדקה (עובר לאוקטובר 2010) מבוססת על הסכם בין משרד התחבורה למפעילי השירות. ההסכם קובע הוראות הנוגעות להתקנה ולהפעלת מערכת כרטוס חכם, הפצה והנפקת כרטיסים חכמים, הבטחת יישום הסדרי נסיעה, שחזור כרטיס והפקת דו"חות למשרד התחבורה, וכן הוראות הנוגעות להעברת תשלומים מהמדינה למפעילים.

[7] תקן קליפסו (Calypso) הוא תקן כרטוס אלקטרוני המגדיר את הדו-שיח המאובטח בין הכרטיסים לבין המסוף. התקן פותח על-ידי קבוצת שותפים אירופיים.. בתקן נלקחו בחשבון בחירות פונקציונאליות מסוימות, כדי לענות על הצרכים של מפעילי התחבורה, כגון: טכנולוגיה ללא מגע, טרנזקציה מהירה ובטוחה (אבטחה מבוזרת), תקשורת בזמן הטרנזקציה, יישום תחבורתי גמיש לבניית המערכת שלב-אחר-שלב, מוצרים ממוקדים שיאפשרו כיסוי של כל המשתמשים והכנסת שירותים חדשים, יכולת שדרוג ועמידה בתקנים הקיימים, מיקרו-מעבד, ממשק כפול והתאמה לתקנים ISO 7816-1, 2, 3, 4 וכן CEN 1545.

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

ברמה המשפטית הרשאות האיסוף והשימוש במידע אישי אודות נוסעים בעלי הכרטיסים הנצבר במהלך השירות מבוססות על טופס קצר שהכתיב משרד התחבורה למפעילים, עליו נדרש לחתום כל מי שמבקש כרטיס חכם.

לאור היקף הפרויקט, סוג המידע הנאסף והמצב המשפטי, ביצעה רמו"ט מבדק מול מספר חברות תחבורה על מנת לבחון את השלכות הפרויקט ואופן יישומו. **סיכום הפיקוח מצורף כנספח א' לדו"ח זה.**

בעקבות ממצאי הפיקוח, הסיקה רמו"ט את המסקנות הבאות –

א. ההסדרה החוזית של משרד התחבורה מחייבת את מפעילי התחבורה הציבורית לאסוף מידע רב ומזוהה אודות מבקשי השירות. מדובר בפרטים דמוגרפים מזהים, תמונה בפורמט דיגיטלי, ובנתוני מיקום ונתונים מפורטים הקשורים באופן השימוש בכרטיס;

ב. המערכת אוספת ואוגרת בבסיס נתונים מרכזי מידע מפורט ומזוהה אודות נסיעות;

ג. נושאים אלה אינם מובאים לידיעת הנוסעים בבהירות הנדרשת לפי סעיף 11 לחוק;

ד. המדינה כגורם מנחה ומעצב המערכת מצדה, לא הסדירה עד לשלב זה, בהסכם ההתקשרות בין מפעילי השירות לבינה את פריטי המידע שאיסופם נדרש, אלא רק ציינה את פרטי המידע המינימלים הנדרשים בעת הפקת הכרטיס. משרד התחבורה לא הסדיר את הרשאת חברות התחבורה לאסוף מידע נוסף וכן לא הגבילה את השימוש במידע זה.

ה. למרות שעפ"י הסכם ההתקשרות בין הממשלה לבין מפעילי השירות, על המפעיל לאפשר למשתמש להימנע מהטבעת פרטיו האישיים על גבי הכרטיס, באם הסדרי הנסיעה המשויכים לכרטיס אינם מוגבלים לשימושה של אוכלוסייה ייעודית, בפועל, עולה מן הממצאים כי אפשרות זאת אינה מובאת במקרים רבים בפני המבקש להנפיק כרטיס חכם.

ו. הסכם ההתקשרות בין המדינה לבין מפעילי השירות קובע כי זמן שמירת המידע יהיה לכל הפחות 24 חודשים מבלי הוספת קביעה לעניין הגבלת משך זמן שמירת המידע. בפועל, קיים חוסר אחידות לעניין משך זמן שמירת המידע בין המפעילים השונים.

ז. הוראות ההסכם מאפשרות שיקול דעת נרחב למשרד התחבורה לאפשר למפעיל השירות לעשות בנתונים שאסף שימוש אחר מעבר לשימוש הנדרש לצורך מימוש ההסכם.

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

לאור האמור לעיל, ובנוסף להמלצות שעלו מדו"ח המבדק, פנתה רמו"ט לעו"ד מלי סיטון, היועצת המשפטית של משרד התחבורה בדרישה לפעולה במספר סוגיות עקרוניות –

א. <u>תכנון לפרטיות</u>

1) על רקע היותה של הזכות לפרטיות במידע זכות חוקתית, התערבות או פגיעה בה צריכה להעשות בהתאם למבחני המידתיות הקבועים בחוק היסוד. כחלק מעקרון המידתיות, רמו"ט סברה כי על משרד התחבורה לבחון חלופות, הפוגעות פחות בפרטיות, מאשר המימוש הטכנולוגי-עסקי המוצע. הליך של תכנון לפרטיות (privacy by design) הינו מימוש חובת המידתיות החלה על משרד התחבורה מכח הזכות החוקתית לפרטיות.

2) איסוף מידע העשוי לפגוע במידה רבה בפרטיות המשמשים בתחבורה הציבורית (כדוגמת תיעוד תחנת המוצא, מספר הקו, כיוון הקו, זהות הרכב ושעת השימוש של משתמש ספציפי), ושמירת המידע בבסיס נתונים מרכזי, כאשר ניתן להשיג את תכלית האיסוף באמצעות פגיעה פחותה בפרטיות המשתמשים, עומד בניגוד לחוק יסוד כבוד האדם וחירותו וחוק הגנת הפרטיות.

3) מממצאי הפיקוח עלה חשש שלא ניתנה מלוא תשומת הלב להיבטי הפרטיות בעת עיצוב המערכת והסדרתה. מכאן שבעת בחינה של נושא זה ייתכנו בהחלט שינויים במתווה שמשרד התחבורה עיצב עד כה. על משרד התחבורה להפנים את היבטי הפרטיות השונים ולוודא כי הפרוייקט אינו אוסף מידע שאינו נדרש למימושו המוצלח.

ב. <u>שקיפות והסכמה</u>

1) הוראות סעיף 11 לחוק, קובעות חובה על אוסף מידע במאגר מידע, להודיע למי שהמידע נאסף אודותיו מהו מקור הסמכות של איסוף המידע, היכן המידע יישמר, לאיזו מטרה ישמש המידע ולמי יועבר המידע המצוי במאגר.

2) חובת השקיפות, נועדה לאפשר למוסר המידע להיות מודע לשימוש שייעשה במידע אודותיו. זהו מרכיב משמעותי מדרישת ההסכמה מדעת הנדרשת על פי חוק הגנת הפרטיות.

3) המקור המשפטי המבקש להכשיר את השימוש במידע במסגרת הפרויקט, הינו הצהרה של המנוי המנוסחת באופן לקוני וגורף, הכולל אף ויתור גורף על זכותו לפרטיות בנתוני המיקום. על פני הדברים נראה כי ההצהרה האמורה אינה מאפשרת הסכמה מדעת של המנוי, במיוחד לנוכח ממצאי הפיקוח בדבר אי הצגת החלופה לרכישת כרטיס אנונימי על ידי החברות כפי שנדרש בהסכם עמם.

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. <u>בקרה</u>

1) במקום שבו רשות ציבורית מחליטה לבצע פרויקט באמצעות מפעילים פרטיים, היא אינה מתנערת מאחריותה לאופן בו מתנהל הפרויקט גם בהיבטים של השימוש במידע.

2) מממצאי הפיקוח עלה כי לא נדונו ולא הוסדרו דרכי הפיקוח של משרד התחבורה על אופן ניהול הפרויקט, ועל עמידת החברות בדרישות העולות מכח ההסכם.

3) משרד התחבורה נדרש לבחון אמצעי בקרה טכנולוגיים ונוהליים לוודא כי האופן בו מיושם ההסכם תואם את העקרונות אותם יתווה המשרד.

בעקבות הפיקוח ופעילות המחלקה המשפטית במסגרת ליווי חוק ההסדרים מוסדר נושא זה בחקיקה וכן בהנחיה אשר תנתן במהלך שנת 2011 על ידי רמו"ט למפעילי הכרטיס.

ה. חקירות פליליות

במהלך שנת 2010 הושלמה מצבת כוח אדם ראשונית במחלקת האכיפה והחקירות אשר מונה 6 אנשים: 5 חוקרים ומנהל מעבדה פורנזית.

1) קבלת סמכויות פליליות והכשרות

בחודש יוני 2010, נתקבלה הרשאה מאת השר לביטחון פנים לבצע חקירות פליליות עבור חוקרי המחלקה.

במקביל לתחילת העבודה השוטפת עברו החוקרים הדרכה והכשרה הולמים הכוללים, בין היתר, קורס מיומנויות חקירה, סדנאות תשאול ותשאול מתקדם, קורס חוקר מחשב מיומן וקורס חקירות פורנזיות במחשבים ביחידת תהיל"ה של משרד האוצר.

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) תיק מ.נ.ר

עיקר עבודתה של מחלקת אכיפה וחקירות אמור להיות בפעילות העבריינית הפלילית בתחום זה. עם זאת, בתחילת עבודת המחלקה נוהלו גם מספר תיקי פיקוח במישור המנהלי[8].

במסגרת זו מחלקת אכיפה ניהלה תיק פיקוח בעל מאפיינים פליליים בטרם קיבלו חוקרי המחלקה סמכויות חקירה פליליות. לפיכך, מישור ההתייחסות ביחס לסמכויות שהופעלו ולהפרות הרלבנטיות היו פיקוחיות-מנהליות.

תיק הפיקוח נסב על שימוש שלא כדין במאגר מידע בלתי חוקי אודות כלל תושבי מדינת ישראל, לצרכים מסחריים.

חברת מ.נ.ר מערכות מידע בע"מ (להלן- מ.נ.ר), הינה בית תוכנה, המתמחה בפיתוח מערכות לניהול תיקי הוצאה לפועל ובמתן שירותי מחשוב למשרדים העוסקים בגביית חובות.

החברה פיתחה רכיב לאיתור חייבים המאפשר למצוא פרטים אישיים אודות האדם נשוא החיפוש במטרה לסייע בהליכי גבייה במסגרת תהליך הוצאה לפועל

רכיב זה נמכר ללקוחות מ.נ.ר יחד עם קובץ המכיל מידע אודות מרבית אזרחי מדינת ישראל וכולל תאריכי לידה, פרטי התקשרות ומספרי תעודת הזהות של ההורים. באופן המאפשר מיפוי קשרי משפחה, יחסי שכנות ואיתורו של אדם.

מ.נ.ר מכרה את הרכיב בצירוף מאגר המידע לכ-80 לקוחות שונים, מרביתם משרדי עורכי דין.

במהלך פעולות האכיפה הוצא על ידי רמו"ט בפעם הראשונה צו להעתקה וחיפוש במחשב ובחומר מחשב לפי פקודת סדר הדין הפלילי (מעצר וחיפוש) תשכ"ט-1969. בעותקי התוכנות, ובמאגרי מידע שנתפשו בחיפוש בוצעו פעולות חקירה מתקדמות של רמו"ט לניתוח המידע וזיהוי ההפרות.

ביום 16/06/2010 הוטלו על מ.נ.ר קנסות מנהליים בסך 258,000 ₪ נוכח 86 הפרות שונות שעיקרן שימוש במאגר המידע שלא למטרה לשמה הוקם, הפרה של הוראות

[8] ראה דו"ח שנתי 2009 המדגים את תוצאותיו של תיק מועצה מקומית זיכרון יעקב ותיק נקודת שיווק וסחר בו הופעל לראשונה המנגנון של הטלת קנסות מנהליים והוטלו קנסות בגובה של 177,000 ₪.

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

סעיף 8 ביחד עם סעיף 31א(א)(1) לחוק. המפוקח ניצל את זכותו שבדין וביקש להישפט חלף הקנס, והתיק הפלילי ינוהל על ידי פרקליטות חיפה (פלילי).

הדגשת ההיבטים הפליליים של המעשה והעלאת המודעות לעצם קיומן של הסנקציות הקבועות בחוק מהווים איתות ברור לחשיבות שמייחסת רמו"ט לעצם השמירה על הוראות החוק, כמו גם לאכיפה הנוקשה בה תנקוט בעתיד במקרים של הפרתו, לרבות הפעלת סנקציות אישיות כלפי נושאי משרה בתאגיד. עוד יצויין כי הקנס הוטל על החברה כחוליית ההפצה של מידע ותוכנות, שעיקר פעילותן מבוסס על עותק לא חוקי של מאגר מידע, אודות אזרחי מדינת ישראל.

3) תיק חקירה פלילי

מחלקת אכיפה וחקירות ניהלה במהלך שנת 2010 חקירה סמויה ופתחה בחקירה גלויה בתיק פלילי ראשון המתנהל ברמו"ט מכוח סמכויות החקירה הפליליות המוקנות לה. על תוכן החקירה מוטל עדיין צו איסור פרסום ע"י בית המשפט. נוכח עובדה זו אין זה המקום להרחיב אודות פעילות 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

ו. הטלת קנסות מנהליים

לנוחות הקוראים מצורפת בזאת טבלה המרכזת של כל הקנסות המינהליים שהוטלו על ידי רמו"ט בנושאי הגנת הפרטיות בשנת 2010:

מועד קביעה	שם הנקנס	סעיף החוק שהופר	תיאור ההפרה	הערות
23/11/2010	שופרסל בע"מ	סעיף 17ו(א)(1)	במסר שיווקי שנשלח בדיוור ישיר על ידי החברה, לא צוינו באופן ברור ובולט הפרטים הנדרשים בחוק.	
02/11/2010	איי.די.איי חברה לביטוח בע"מ (ביטוח ישיר)	סעיף 8(ב)	החברה קיבלה החלטה שלא לספק שרות ביטוח לפלוני, תוך שימוש במידע שהגיע אליה, כצד ג' מההוצאה לפועל זאת בניגוד לאיסור בסעיף 7ב בחוק ההוצאה לפועל.	החברה הגישה בקשה לביטול הקנס. הבקשה נדחתה.
15/09/2010	המשביר לצרכן החדש בע"מ	סעיף 17ו	פניה דיוור ישיר שלא בהתאם להוראות סע' 17ו לחוק.	
16/6/2010	מ.נ.ר מערכות מידע בע"מ	סעיף 8	סחר במידע בלתי חוקי ממאגר מרשם האוכלוסין	החברה הגישה בקשה להישפט
14/04/2010	בנק לאומי לישראל בע"מ	סעיף 8(ב)	שימוש במאגר המידע של קרן השתלמות מגדל פלטינום שלא למטרה שלשמה הוקם המאגר	
21/02/2010	קרית חיים ארלוזורוב - אגודה הדדית בע"מ	סעיף 8(ב)	שימוש בפנקס הבוחרים שמקורו במרשם האוכלוסין שלא למטרה לשמה הוקם המאגר	הנקנסת הגישה בקשה להישפט. טרם הוחלט בעניינה. במקביל המתלונן מקדם קובלנה בעניין נשוא התלונה
08/02/2010	בנק הפועלים	סעיף 13	הבנק לא השיב למלין תוך 21 יום מיום קבלת בקשה למתן זכות עיון	

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

01/02/2010	דיילקום בע"מ	סעיף 8(ב)	שימוש בפנקס הבוחרים שמקורו במרשם האוכלוסין שלא למטרה לשמה הוקם המאגר	
01/02/2010	דיילקום בע"מ	סעיף 9	מסירת פרטים לא נכונים בבקשת רישום	
28/01/2010	קבוצת קידום בע"מ	סעיף 17ו	פניה בדיוור ישיר שלא בהתאם להוראות סעיף 17ו	
28/01/2010	עיריית רמת גן	סעיף 8(ב)	העברת רשימת תלמידים לחברה מסחרית ללא הסכמה ושלא למטרות לשמן הוקם המאגר	
28/01/2010	עיריית רמת גן	סעיף 17ד	ביצוע פעולת שרותי דיוור ישיר מבלי שמטרת המאגר בפנקס כללה פעילות כאמור	
14/01/2010	איי אי ג'י ישראל חברה לביטוח בע"מ	סעיף 11(2)	אי מסירת הודעה לנושא המידע על מטרות השימוש במידע אודותיו	

ו. רישום מאגרי מידע

1) נתונים

בשנת 2010 הוגשו 366 בקשות רישום – ירידה של כ-10% בבקשות הרישום החדשות ביחס לשנת 2009.

במהלך שנת 2010 נגבו 2,328,963 ₪ עבור תשלום אגרות הרישום והאגרות התקופתיות. יצויין כי אגרות אלו הן אגרות ייעודיות אשר נועדו לממן, בין היתר, את פעילות ההסברה והאכיפה של רמו"ט בתחום הגנת הפרטיות, ועל כן מוטלות על הגורמים שיש בידם מאגרי מידע.

בהשוואה לנתוני השנתיים הקודמות ישנן שתי מגמות מובהקות –

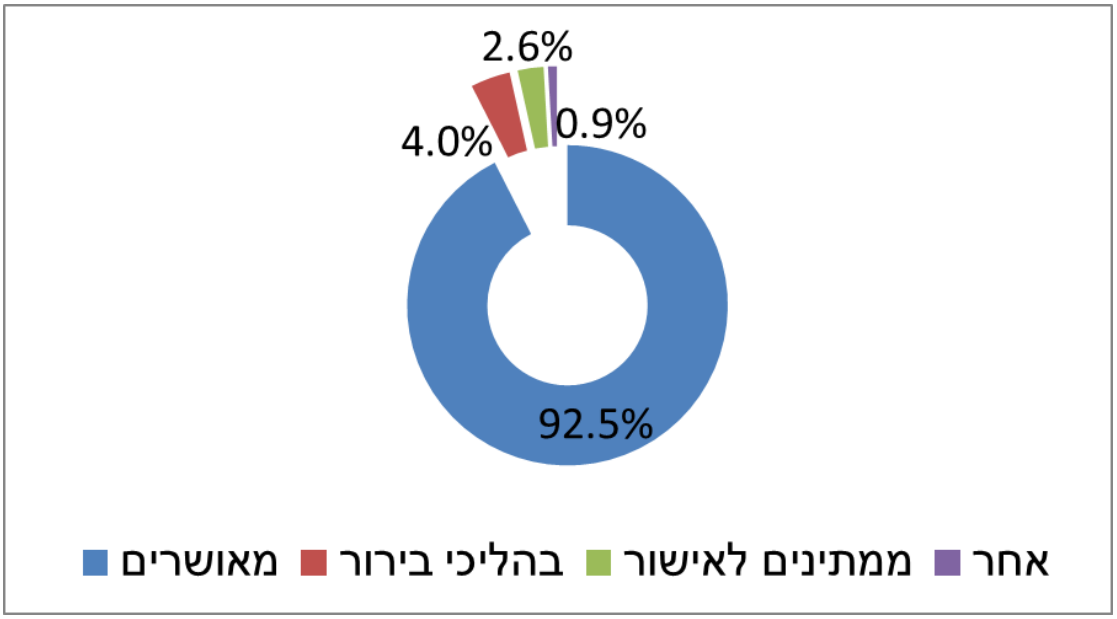
א. אחוז הדיווחים על זכאות לפטור מתשלום האגרה השנתית מכלל בעלי המאגרים אליהם מופצת הדרישה לתשלום אגרה תקופתית עולה בהתמדה (בשנת 2008 – 8.8% ; בשנת 2009 – 11.8% ; בשנת 2010 – 16.5%) ;

ב. אחוז הבקשות לביטול רישום מאגרי מידע הוכפלה בשנה זו ביחס לשנים קודמות (בשנת 2008 – 0.9% ; בשנת 2009 – 0.7% ; בשנת 2010 – 1.4%) ;

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

מגמות אלו מוסברות על ידי שינוי מדיניות הרישום בתחום המגזר הרפואי[9] ובתחום הבעלות במאגרי מידע על מאגרים המוחזקים בידי בתי"ס[10], אשר הוביל לכך שבעלי מאגרים שהיו חבים בעבר ברישום ובתשלום אגרה, רישומם התייתר או לחלופין ניתן להם פטור מאגרה בשל שינוי הבעלות במאגר.

במהלך שנת 2010 המשיכה הפעילות עליה דווח בשנה הקודמת, לצמצם את כמות המאגרים הממתינים לאישור רשם מאגרי מידע. להלן מפורט סטטוס תהליך רישום המאגרים בפנקס נכון לתחילת ינואר 2011 –



[9] הנחיית רשם 1-2009 http://www.justice.gov.il/NR/rdonlyres/6F8F05C5-90E5-4A3A-A36F-6E5667C9A963/20009/120091.pdf

[10] כאמור בסיכום בין רשם מאגרי מידע למשרד החינוך כפי שבא לידי ביטול בחוזר מנכ"ל משרד החינוך http://cms.education.gov.il/educationcms/applications/mankal/etsmedorim/3/3-6/horaotkeva/k-2010-3a-3-6-8.htm

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) נושאים עקרוניים שעלו מהליך הרישום

במהלך שנת 2010, אגב הטיפול בבקשות הרישום, התבררו מספר נושאים חדשניים בבירור בקשות רישום. להלן עיקרם:

א) דויטשה בנק – מאגר ניטור פעילות עובדים

בבקשת רישום שהגיש הבנק הגרמני הפועל בישראל, הוא ביקש לרשום מאגר מידע שמטרתו מעקב אחר עובדי הבנק. בעקבות הגשת הבקשה נבחן אופן ביצוע המעקב על מנת לוודא כי הבנק, בביצוע מעקב כאמור, פועל על פי הוראות חוק הגנת הפרטיות.

בעקבות הבדיקה שערכה רמו"ט, הוחלט לאשר את רישום המאגר בכפוף לתנאים הבאים –

א. הסכמת הרשם לרישום המאגר כוללת אישור רק לחוקיותו של מאגר הכולל מידע שנצבר כתוצאה מניטור של הודעות דואר אלקטרוני ומסרים מיידיים של עובדים, בזמן אמת, הנעשה לפי מילות מפתח, למטרת בדיקת עמידה בהוראות דין ורגולציה באופן שהוצג על ידי הבנק;

ב. יש להוסיף על ההודעה שהבנק מעביר לעובדיו, באופן מפורש ושאינו משתמע לשני פנים כי הנהלת הבנק עשויה לקרוא את הודעות העובדים, ולא להסתפק במונח שאינו בהכרח מוכר לכל העובדים ("monitoring");

ג. על ההודעה לעובדים לנקוב במפורש בכל סוגי האפליקציות שיהיו כפופות לניטור;

ד. את נוסח ההודעה של הבנק יש לתרגם מאנגלית לעברית ולהחתים את העובד על נוסח בשתי השפות. יש לרענן את ההליך ולהחתים את העובדים מחדש כל חצי שנה;

ה. נוסח מפורט של מדיניות הניטור של החברה צריך להיות זמין לעובדים בכל עת באופן שוטף.

כמו כן, הפנתה רמו"ט את יועציה המשפטיים של הבנק לעמדת היועץ המשפטי לממשלה בערעור שהוגש בעניין איסקוב, שנכון למועד מתן החלטת רמו"ט בבקשת הרישום, טרם נתקבלה בו החלטה.

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

ב) מנהרות הכרמל

אגב בקשת הרישום של חברת מנהרות הכרמל בע"מ, המפעילה מערך ניטור ותיעוד של נסיעות במנהרות הכרמל, התבררו סוגיות משפטיות בנוגע לאיסוף מידע על ידי מנהרות הכרמל, לשימושים במידע ולאופן אבטחתו.

במסגרת הבדיקה לצורך אישור הרישום, נדרשה החברה על ידי רמו"ט:

א. לבצע תסקיר השפעה על הפרטיות (privacy impact assessment) על מנת לוודא כי בעת החלטה על אופן מימוש הפרויקט בהיבטים של הגנת הפרטיות יילקחו בחשבון שיקולים הנוגעים לאופן ניהול מידע אישי בהתאם להוראות החוק.

ב. לדווח על סקר סיכוני אבטחה ולפרט את אמצעי האבטחה המיושמים בפרוייקט, ולהציג בפני רמו"ט את המתכונת בה החברה מבקשת ההסכמות לשימוש במידע אישי מלקוחותיה.

ג) דחיית בקשות לרישום מאגרי מידע

במהלך 2010 הוחלט על דחיית בקשתן של שתי חברות לרישום מאגר מידע בפנקס –

א. **חברת דיילקום** – ראו דיווח לעיל בנוגע לתיקי פיקוח (סעיף 2.2.2 לדו"ח)

ב. **חברת אור אל חויה לבר מצוה** – ראו דיווח לעיל בנוגע לתיקי פיקוח (סעיף 2.2.10 לדו"ח).

GAMINGVC - בקשת רישום של חברה המעניקה שרותי תמיכה לאתרי אינטרנט המפעילים הימורים במדינות בהן מותר להמר, הגישה בקשת רישום עבור פעילותה זו. בבחינת בקשת הרישום, נבחנה הסוגיה המשפטית האם הרשם רשאי לסרב לרשום את המאגר לאור אי חוקיותם של הימורים מקוונים בישראל.

לאחר בירור שאלה זו מול המחלקה הכלכלית בפרקליטות, הובהר כי המצב המשפטי אינו ברור דיו באופן המאפשר סירוב של הרשם לרשום את המאגר האמור.

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. פירוט הפעלת סמכויות רשם שירותי נתוני אשראי ושירותי מידע על עוסקים, מכוח חוק שירות נתוני אשראי, התשס"ב-2002 ותקנות שירות נתוני אשראי, התשס"ד-2004.

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. בעלי רישיונות

1) חברת לב אמון יזמים בע"מ

במהלך שנת 2010, ובעקבות פעולות פיקוח, שיפורטו בהמשך, החליט הרשם לבטל את רישיון שלב א' שניתן לחברת לב אמון יזמים בע"מ. ההחלטה התקבלה לאחר שהחברה לא הצליחה לעמוד בחובותיה בהיבטי התפעול ואבטחת המידע, ברמה הנדרשת לפי חוק שירות נתוני אשראי, התקנות מכוחו ודרישות הרשם.

בעקבות החלטת הרשם, החליטה החברה להפסיק את פעילותה גם כבעלת רישיון שירות מידע על עוסקים.

2) בעלי רשיונות תקפים

להלן בעלות הרישיון כיום מכח חוק שירות נתוני אשראי –

מספר רישיון	סוג רישיון	שם בעל הרישיון	כתובת אתר האינטרנט של בעל הרישיון
539000042	שירות נתוני אשראי	די. אנד בי. החברה לנתוני אשראי בע"מ	www.dbcredit.co.il
539000034	שירות נתוני אשראי	בי.די.איי ביזנס דאטה ישראל בע"מ	http://www.bdi.co.il
539000026	שירות מידע על עוסקים	בי.די.איי ביזנס דאטה ישראל בע"מ	http://www.bdi.co.il
539000018	שירות מידע על עוסקים	דן אנד ברדסטריט ישראל בע"מ	http://www.dbisrael.co.il

ד. תיקוני חקיקה

בתחילת השנה סיימה רמו"ט את הטיפול בסגירת רישיון שירות נתוני אשראי של חברת CIA. בעקבות פעילות רמו"ט בתחום זה נבחנו מחדש הוראות החוק הנוגעות לתנאי הסף למתן רישיון וכן לסמכויות הרשם בעת סגירת רישיון, לחובות בעל רישיון בסגירת פעילות ולאמצעי האכיפה הקיימים בידי רמו"ט, תוך מטרה להציע תיקוני חקיקה, ראשית ומשנית, למחלקת ייעוץ וחקיקה לאור ניסיון רמו"ט בפרקטיקה של סגירת רישיון שירות נתוני אשראי.

בעקבות דיווחי תקלה שהועברו על ידי אחת מבעלי רישיון שירות נתוני אשראי, נתגבש הצורך בתיקון תקנה 80 לתקנות שירות נתוני אשראי, התשס"ד-2004, המסדירה את

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

חובות בעל הרישיון והרשם בעת קרות תקלה. התיקון המוצע מקובל על מחלקת ייעוץ וחקיקה (אזרחי) והועבר לאישור הכנסת במסגרת תיקון התקנות המצוי על שולחנה של וועדת הכלכלה. התיקון מציע, בין היתר, את ההסדרים הבאים –

א. על בעל הרישיון להודיע לרשם על התקלה לאלתר, ולא יאוחר מיום עבודה אחד מעת גילוי התקלה;

ב. פירוט הנתונים שעל בעל הרישיון להעביר לרשם, וזאת על מנת לאפשר לרשם להבין באופן מיידי את מהות התקלה וחומרתה;

ג. מתן סמכות לרשם להורות לבעל הרישיון להודיע לאנשים אודותם נמסר דו"ח האשראי הפגום (ככל שנמסר), על התקלה שהתרחשה. מטרת התיקון היא לאפשר לנושאי המידע להיות מודעים למידע השגוי שיצא אודותם, כך שככל שיהיה שימוש לרעה במידע האמור, תהיה להם האפשרות להתגונן, ובמידת הצורך להיפרע, מגורם הנזק;

ג. תשלום בעלי הרישיונות לבנקים

ב-16.6.10 ניתן פסק דין על ידי ביהמ"ש העליון בבג"ץ 1018/09 **די אנד בי החברה לנתוני אשראי בע"מ ובי.די.איי קופאס בע"מ נ' שר המשפטים** שעניינו, טענת בעלות הרישיונות על כי תקנה 83 לתקנות שירות נתוני אשראי, התשס"ד-2004, הותקנה מחוסר סמכות, וטענות הנוגעות לפרשנות שהוצגה על ידי רמו"ט ומשרד המשפטים לעניין תקנות 82 ו-83. פסק הדין ניתן לאחר שהעותרות חזרו בהן מהעתירה.

בעקבות החלטת ביהמ"ש העליון, אכפה רמו"ט את ביצוע הוראות התקנות, העוסקות בתשלום בעלי הרישיונות למקורות המידע.

ד. פיקוח על בעלי רישיונות לשירותי נתוני אשראי

תיקי פיקוח בתחום נתוני אשראי כוללים שלושה סוגי תיקים –

א. תיקי פיקוח הנפתחים בעקבות פניה של אדם;

ב. תיקי פיקוח הנפתחים בעקבות פעילות יזומה של רמו"ט;

ג. תיקי פיקוח הנפתחים בשל בקשות של בעלי הרישיונות וכוללים בתוכם ביצוע פעולות פיקוח.

בכוונת רמו"ט להפריד בין הליכי מתן הרישיון, ומתן אישורי רשם הנדרשים אגב מתן רישיון לבין פעולות פיקוח הדורשות שימוש בסמכויות הרשם ובסמכויות המפקחים

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

מטעמו. הליך זה מחייב חיזוק תשתית כח האדם אשר קיים במחלקת רישום ופיקוח, האחראית הן על מתן הרשיונות והן על הפיקוח.

1) נתונים

בתחום נתוני אשראי הוגשו בשנת 2010 50 תלונות המהוות כ-17% מכלל התלונות שהגיעו לרמו"ט. ביחס לשנת 2009, עלתה כמות הפניות בתחום נתוני אשראי ב-350%, ונתח הפניות בתחום נתוני אשראי מכלל הפניות שהגיעו לרשות, עלה ב-8%.

במהלך השנה נפתחו ברמו"ט 11 תיקי פיקוח בנושא נתוני אשראי, המהווים 11% מכלל תיקי הפיקוח שנפתחו בשנה זו. כמו כן, המשיך הטיפול ב-8 תיקי פיקוח בתחום זה שנפתחו קודם לשנת 2010.

חלוקת התיקים לפי סוגיהם היא כדלקמן –

סוג התיק	כמות
תיקי פיקוח בשל מהלך ייזום	9
תיקי פיקוח בעקבות תלונה	8
תיקי פיקוח לצרכי אישור רשם	2
סה"כ	**19**

2) פעולות אישור לבעלי רשיונות

ז) חברת לב אמון בע"מ

במהלך השנה, ביצעה רמו"ט ביקורת מקיפה אצל חברת לב אמון יזמים בע"מ על מנת לבחון את עמידת החברה בדרישות לצורך בחינת עמידתה בדרישות החקיקה, ובדרישות רשם שירותי נתוני אשראי, בתנאים הנדרשים למתן אישור רישיון שלב ב'[11] לחברה.

[11] מתן רישיון שירות נתוני אשראי ניתן במהלך דו שלבי. רישיון שלב א' ניתן לאחר שהוכח כי החברה עומדת בדרישות התפעול ואבטחת המידע, ומאפשר העברת מידע ממקורות המידע. רישיון שלב ב' ניתן לאחר שהחברה הוכיחה כי המערכות שהקימה מצליחות לאסוף את המידע לשמרו ולהפיק ממנו דו"חות אשראי – בהתאם לתנאים הקבועים בחקיקה, והכל תוך הקפדה על רמת אבטחת מידע גבוהה.

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

בעקבות פיקוח שהתבצע בחברה במהלך פברואר 2010, ולמרות שהחברה הודיעה כי היא עומדת בחובותיה לצורך מתן אישור רישיון שלב ב', נתגלו כשלים מהותיים בסוגיות הנוגעות ליכולת התפעולית של החברה כמו גם לרמת אבטחת המידע בה.

בעקבות ממצאי הפיקוח, הונחתה החברה כיצד לפעול, תוך מתן התראה כי אי עמידה בדרישות אלו, יובילו לשלילת רישיון החברה.

לאחר מספר פעולות של החברה לקידום דרישות הרשם, נתגלה לבעליה, ולרשם שירותי נתוני אשראי, כי החברה אינה יכולה לעמוד בדרישות הרשם.

לפיכך, הודיע הרשם ביום 23.12.10 לבעלי החברה על כוונתו לבטל את רישיון החברה, בכפוף למתן זכות שימוע.

בתאריך 1.2.11, לאחר שמוצו טיעוני החברה, הודיע הרשם על ביטול הרישיון.

בעקבות ביטול רישיון שירות נתוני אשראי, הודיעה החברה לרשם ביום 7.2.11, על סגירת פעילותה גם בתחום שירות מידע על עוסקים.

ח) חברת בי.די.איי קופאס בע"מ

במהלך שנת 2010 נבחן המפרט המוצע של חברת בי.די.איי קופאס להקמת אתר DRP (Disaster Recovery Plan). בתאריך 9.12.10 ניתן אישור הרשם להקמת האתר. קיומו של אתר DRP הינו בעל חשיבות גבוהה בכך שהוא מאפשר את המשך הפעילות של שירות נתוני אשראי, גם בעת תקלה קריטית המתרחשת באתר הראשי של בעל הרישיון.

3) תיקי פיקוח נבחרים

ט) מתן זכות עיון

בעקבות תלונה שהגיעה לרשם על אי מתן דו"ח עיון, ללא עלות, על ידי שתי בעלות רישיון שירות נתוני אשראי, נתבצעה פעולת פיקוח סמויה על מנת לבחון טענה זו.

ממצאי הפיקוח עלה כי החברות עמדו הן בחובתן למסור את דו"ח העיון ללא עלות, והן בחובתן למסור את המידע תוך 7 ימים.

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) אבטחת מידע

במהלך שנת 2010 בוצעו פעולות פיקוח בתחום אבטחת המידע בשתי החברות. בשתי החברות, נמצאו ליקויי אבטחת מידע, אולם לא ברמה היוצרת ליקוי קריטי המצדיק נקיטת סנקציות כנגד החברות. המשך הטיפול והמעקב על ממצאי הפיקוח, יתבצע במהלך שנת 2011.

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

8. דין וחשבון של רשם גורמים מאשרים בדבר הפעלת סמכויותיו בשנת 2010 לפי תקנה 16ל לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב–2001

מוגש לוועדה למדע וטכנולוגיה מכח תקנה 16 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס״ב-2001

א. פעולות פיקוח על הגורם המאשר – חברת קומסיין

1) נתונים

בתחום חתימה אלקטרונית הוגשו בשנת 2010 7 תלונות המהוות כ-2.5% מכלל התלונות שהגיעו לרמו״ט. ביחס לשנת 2009, עלתה כמות הפניות בתחום חתימה אלקטרונית ב-75%, אולם נתח הפניות בתחום חתימה אלקטרונית מכלל הפניות שהגיעו לרשות, ירד ב-0.5%.

במהלך השנה נפתחו ברמו״ט 13 תיקי פיקוח בנושא חתימה אלקטרונית, המהווים 13% מכלל תיקי הפיקוח שנפתחו בשנה זו. כמו כן, המשיך הטיפול ב-3 תיקי פיקוח בתחום זה שנפתחו קודם לשנת 2010.

חלוקת התיקים לפי סוגיהם היא כדלקמן –

סוג התיק	כמות
תיקי פיקוח לצרכי אישור רשם	11
תיקי פיקוח בשל מהלך ייזום	4

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

תיקי פיקוח בעקבות תלונה	1
סה"כ	**16**

2) עדכון מסמך הנהלים של קומסיין

בספטמבר 2010 בתום הליך בחינה מקיף אישר רשם גורמים מאשרים הפועל במסגרת רמו"ט (בדו"ח זה – **הרשם**) את מסמך הנהלים החדש של חברת קומסיין בהתאם לתקנות לפי חוק חתימה אלקטרונית, התשס"א-2001 (בדו"ח זה – **החוק**).

מסמך הנהלים של הגורם המאשר מהווה את תקנון השירות שלו, ומסדיר את התחייבויותיו והצהרותיו כלפי לקוחותיו וכלפי מי שמסתמך על התעודה האלקטרונית שהנפיק.

הליך עדכון מסמך הנהלים נדרש בשל עדכון התקן הבינלאומי לפיו ערוכים מסמכי הנהלים בתחום זה (rfc 3647 ietf), בשל הצורך לאפשר לקומסיין פעילויות נוספות, ובשל הצורך לעדכן את מסמך הנהלים בעקבות לקחים וממצאים מפיקוחים בעבר.

במסגרת הדיונים על מסמך הנהלים נבחנו בצורה מעמיקה שורה של תהליכים והסדרים הקשורים בפעילות חברת קומסיין. דגש משמעותי בתהליך ניתן להגנה על אינטרסים של בעלי התעודות האלקטרוניות - לקוחות קומסיין. ההנחה היא כי המוצר "תעודה אלקטרונית" הינו מוצר מורכב וללקוחות עשוי להיות קושי להבין את ההיבטים השונים הקשורים אליו או לנהל משא ומתן אפקטיבי עם הגורם המאשר לגבי תנאי השירות. כמפורט בקצרה להלן.

במסגרת זו נקבע כי הגורם המאשר לא יוכל להגביל את אחריותו לתעודות המונפקות לצורך מילוי דרישת חתימה בחיקוק או לפי דרישה של רשות מרשויות המדינה אל מתחת ל- 500,000 ₪ לתעודה אלקטרונית.

יצויין כי קומסיין ביקשה שסכום תקרת האחריות יעמוד על 10,000₪ (וזאת לעומת 500,000 ₪ שאליהם התחייבה במסמך הנהלים שאושר לה בעבר). הרשם התנגד נחרצות לבקשה זו משום שכיום מרבית הלקוחות הנזקקים לחתימה אלקטרונית ולתעודה אלקטרונית עושים זאת על מנת לקיים דרישה של רשויות המדינה. ללקוחות אלה אין ברירה או יכולת לבחור במוצר אחר. בנוסף, ללקוחות אלה אין כל דרך להגן על עצמם מפני רשלנות של קומסיין.

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

השימושים הנפוצים כיום בחתימה אלקטרונית, הינם לדיווחים לרשות ניירות ערך, לרשות המסים ולצורך הגשת מכרזים מקוונים. ככאלה הם עשויים להיות קשורים בפעולות כספיות בסכומים גבוהים יותר. אין כל הצדקה, לשיטת הרשם, לגלגל על לקוחות הגורם המאשר את הסיכונים במקרים שבהם נקבע כי יש לגורם המאשר חבות אזרחית. יודגש כי הגבלת האחריות שביקשה קומסיין לקבוע נועדה לחול גם במקרים שבהם נקבע שהתרשלה.

בפיקוח שהחל בשנת 2010 (לאחר אישור המסמך וכניסתו לתוקף) על בסיס מידע שהגיע לרשם, התברר כי בניגוד מוחלט לאמור במסמך הנהלים המחייב אותה, המשיכה קומסיין לקבוע הגבלת אחריות בסכומים נמוכים מזה שאושר בתעודות.

בעקבות הבירור הציעה קומסיין לחזור בה ממגבלה זו ביחס לכל התעודות התקפות שהונפקו על ידה, לרבות אלה שהונפקו לפני ספטמבר 2010 . לאחר אישור הצעה זו על ידי הרשם, שלחה קומסיין בהנחיית הרשם הודעה אישית לבעלי תעודה כאמור, וכן פרסמה באתר האינטרנט שלה ובשני עיתונים יומיים, על ביטול המגבלה האמורה. המעקב אחר הטיפול בנושא זה נמשך בשנת 2011. ההתחייבות של קומסיין מפורסמת באתר הרשם.

במסגרת אישור מסמך הנהלים אושר עוד לקומסיין להנפיק תעודות אלקטרוניות לשימוש תאגידי על גבי שרת, בהתאם לנהלים מתאימים. התערבות הרשם נועדה לצמצם את הסיכונים הכרוכים בהנפקה של אמצעי חתימה, שהינו אישי מטבעו, על גבי רכיב המצוי ברשת הארגונית ולכאורה לא נמצא בשליטתו הבלעדית של בעל אמצעי החתימה, כהגדרתו בחוק.

בהתאם לאישור יכולה קומסיין להנפיק תעודה אלקטרונית כאמור רק לגבי מורשה חתימה בתאגיד, משום ההנחה כי החתימה נעשית במסגרת האחריות הכוללת של התאגיד.

נושא תעודות אלקטרוניות על שרת נמצא בבחינה נמשכת על ידי הרשם, בשל היתרונות התפעוליים הכרוכים במימוש זה של חתימה אלקטרונית.

3) כשל פרסום רשימת תעודות בטלות (CRL)

בתאריך 1.11.2010 דיווח לרשם צד מסתמך על תעודות אלקטרוניות, כי אירעה תקלה בפרסום רשימת התעודות המבוטלות (CRL) של חברת קומסיין, באופן שכל התעודות שהונפקו על ידי החברה זוהו כלא תקפות כאשר הושוו למול רשימת

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

התעודות הבטלות (CRL – Certificate Revocation List). לחברת קומסיין נדרשו מספר שעות לאתר את מקור התקלה, שנבעה מאי פירסום קובץ CRL עדכני של שרת העוגן (Root CA).

בעקבות האירוע בוצע פיקוח על ידי רמו"ט, וכן בוצע תחקיר פנימי על ידי החברה שמסקנותיו הועברו לרמו"ט. ממצאי הפיקוח והתחקיר העלו תמונה מטרידה באשר להתנהלות קומסיין וקיום חובות הזמינות של מנגנון התעודות הבטלות על ידה.

מקור התקלה היה העובדה כי תוקף ה-CRL של ה-Root CA שמפרסמת קומסיין פג, ועל כן החל ממועד התפוגה נחזו כל שרתי הנפקת התעודות של קומסיין המנפיקים תעודות אלקטרוניות לחתימה אלקטרונית מאושרת כבטלים (Revoked)[12], וכתוצאה מכך נחזו כל התעודות האלקטרוניות ששרתים אלה הנפיקו כבטלות.

קובץ CRL עדכני של שרת ה-Root CA של קומסיין אמור להיות מופק, להחתם אלקטרונית על ידי שרת ה-Root CA ולהתפרסם כל חצי שנה. פעולה זו, המתבצעת ידנית, לא בוצעה על ידי החברה. הסתבר כי במערכות קומסיין לא הייתה קיימת מערכת המתריעה מראש על הצורך בפרסום קובץ CRL עדכני של ה-Root CA.

בנוסף, במקרה של אירוע חריג כפי זה, בו כל תעודות קומסיין הופכות לבטלות, נשלחו הודעות SMS באופן רצוף ל-6 בעלי תפקידים בחברת קומסיין המתריעות על תקלה. במקרה הנדון, חמישה מהעובדים ציינו כי ראו את ההודעות בשעות הבוקר, ועובד אחד ראה את ההודעות בשעה 3:00 לפנות בוקר, אולם לא התריע על הנושא היות והיה טרוד בעניינים אחרים.

במהלך הביקורת הסתבר, כי בשל רשלנות נוספת של קומסיין, קודם לתקלת ה-CRL, לא עבדו חלק ממערכות התיעוד בשל כשל במעקב אחריהן.

הנסיבות לתקלה, והאופן בו היא טופלה, והבעיות האחרות שאותרו, העידו על כשלים יסודיים בניהול החברה. בעקבות הממצאים הודיעה קומסיין על נקיטת צעדים מתקנים למניעת אירועים כאלה בשנית, ובשל כך הסתיים הטיפול במקרה.

[12] בפועל מדובר בכך שהתעודה האלקטרונית של שרת ההנפקה נחשבת כבטלה.

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

יצויין, כי לרשות הרשם לא עומדת סנקציה של עיצום כספי על אירוע בנסיבות החמורות המתוארות בסעיף זה. הפעלתה של סנקציית התליית הרישום במרשם הגורמים המאשרים, עד לתיקון מלוא הליקויים או לביצוע שינויים משמעותיים הקבועה בסעיף 14 לחוק לא הייתה אפשרית בשל היות קומסיין הגורם המאשר היחיד הרשום במרשם, והתלות גורמים רבים, פרטים וציבוריים, בשירות שהיא מספקת.

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) הארכת מועד אישור הגורם הרושם – ההוצאה לאור של לשכת עורכי הדין

בעבר אשר הרשם את ההוצאה לאור של לשכת עורכי הדין (להלן בפרק זה – **ההוצאה לאור**) כגורם רושם, קרי גורם המוסמך לזהות בשם הגורם המאשר את מבקשי התעודות האלקטרוניות. במסגרת האישור של ההוצאה לאור נקבעו תנאים הנדרשים לפעילות.

בדצמבר 2009, בוצעה ביקורת בהוצאה לאור בעקבותיה הוארך האישור לשלושה חודשים בלבד, בכפוף לקיום תנאים שבהחלטה. במרץ 2010 הוארך האישור לתקופה נוספת של חודש ימים להשלמת קיום התנאים ושיפור רמת האבטחה. בסוף אפריל 2010 הוארך האישור עד לתום השנה בכפוף לקיום כל הדרישות שנקבעו בעבר, בין היתר יישום שיפור האבטחה והגשת נהלים מתוקנים.

על מנת לתת להוצאה לאור ודאות תפעולית, האישורים נקבעו לתקופה ארוכה יחסית. לקראת סוף שנת 2010 נדרשה שוב הארכת תוקפו של האישור בארבעה חודשים על מנת לאפשר השלמה מסודרת של הדרישות.

בפיקוח שנעשה אגב הארכת האישור הסתבר כי קיים פער בין הליך ההזדהות של עובדי קומסיין וההוצאה לאור כפי שעוגן בנהלי החברה, לבין אופן ההזדהות בפועל. בנוסף, התברר כי ישנו ליקוי אבטחתי באופן ההזדהות.

בעקבות ממצאי הפיקוח הציעה החברה פתרון ברמת החומרה והתוכנה אשר אושר על ידי הרשם, וכן נערכו שינויים ברמת ניהול ההרשאות. מטבע הדברים, בשל סודות מסחריים ושיקולי אבטחת מידע, לא יועבר מידע מעבר למפורט בדו"ח זה.

5) אישור מתחמי עבודה נוספים

בשנת 2010, בשל הגידול בביקוש לתעודות אלקטרוניות, ביקשה קומסיין להוסיף אתרים פיזים לאתרים בהם היא נותנת שירות.

צוות הפיקוח של רמו"ט בחן את הבקשות ואת היבטי אבטחת המידע הקשורים בהפעלתם. לאחר ביצוע ביקורות באתרים אושר לחברה להרחיב את מתחם ההנפקה בסניף תל אביב (קרית עתידים) וכן במתחם חדש בחיפה.

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) אישור מנגנון שחרור מנעילה של כרטיס חכם

בהמשך להנחיית רשם 2010-1 (ראו להלן) בה אישר הרשם יישום מנגנוני שחרור מנעילה במטרה להקל על ציבור המשתמשים בתעודות אלקטרוניות, הגישה קומסיין ביולי 2010 הצעה ליישום פתרון של תהליך שחרור מנעילה של כרטיס חכם.

באוגוסט 2010 לאחר בחינת הנושא החליט הרשם לאשר לחברה להשתמש במנגנון כזה.

האישור האמור הותנה והתבסס על התחייבויות שלקחה על עצמה החברה והצהרות שנתנו, בין היתר, באשר לנטילת אחריות מלאה על הסיכונים הקשורים במימוש המנגנון.

7) בקשה לאישור גורם רושם נוסף

באפריל 2010 הגישה חברת קומסיין בקשה לאישור של חברה נוספת כגורם רושם. בשל ליקויים רבים בהליך הגשת הבקשה, הוחזרה הבקשה ביום בתחילת יוני 2010 לקומסיין להגשה מחדש.

בתחילת אוקטובר 2010, לאחר הגשת בקשה מתוקנת, ניתן על ידי הרשם אישור עקרוני לגורם הרושם הנוסף, אשר הותנה בקיומן של מספר דרישות.

הליך הבחינה של הבקשה בהתאם להנחיות נמשך בשנת 2011.

ב. בקשות רישום חדשות

1) עדכון הנחיות פנימיות לרישום

במהלך שנת 2010 עדכן הרשם את ההנחיה הפנימית המנחה אותו בעת רישום גורמים מאשרים (מבחנים לרישום גורם מאשר עפ"י חוק החתימה האלקטרונית, התשס"א-2001), הקשורה בבדיקות אבטחת המידע והאבטחה הפיזית של הגורמים המאשרים. בשל היבטי האבטחה של הנחיה זו, היא אינה מפורסמת.

ברמו"ט מבוצעת עבודת עדכון כוללת להנחייה זו, הקשורה באופן ההסדרה והפיקוח של גורמים מאשרים. במסגרת זו, פורסמה גם הנחיה 2010-2, כמפורט מטה, שעניינה ביצוע בדיקות לגורם מאשר בידי גורם חיצוני באופן שנועד להבטיח עמידה בהוראות החוק.

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) בקשת רישום של חברת סקיורנט גורם מאשר בע"מ

במהלך שנת 2010 טיפל הרשם בבקשת רישום חדשה של חברת פרסונל איי.די בע"מ (לשעבר סקיורנט גורם מאשר בע"מ), במסגרתה נעשה שימוש בהנחיה 2-2010 שנועדה לתת בידי הגורם המאשר שיקול דעת רב יותר באשר לאופן המימוש הטכנולוגי של השירות, תוך שמירה על תכליות ומטרות החוק.

במסגרת הטיפול בבקשת הרישום נערכו בדיקות מקיפות למסמך הנהלים של החברה (תקנון השירות), לנהלי העבודה שלה, ולהיבטי אבטחת מידע לוגיים ופיזים בפעולתה. הליך הרישום המשיך בשנת 2011.

ב. פרסום הנחיות רשם גורמים מאשרים

בשנת 2010 פורסמו 5 טיוטות הנחיה, מהן 4 נכנסו לתוקף.

1) הנחייה 1-2010

הנחיה 1-2010 עוסקת בקביעת דרישות חלופיות לסיסמת הגישה לאמצעי החתימה, כלומר ה"קוד הסודי" המשמש לגישה לביצוע החתימה האלקטרונית. נוסח ההנחיה מצ"ב כנספח א' לדו"ח זה.

קוד הגישה הוא רכיב חשוב מאוד במעטפת ההגנה על אמצעי החתימה של החותם, משום שהוא זה שמאפשר בפועל שימוש בתעודה האלקטרונית לצורך חתימה האלקטרונית. בהתאם לתקנות חתימה אלקטרונית נדרש אמצעי זה, ככל שאינו ביומטרי, לעמוד בהוראות תקן ישראלי 1495 חלק 3 העוסק בסיסמאות. אל הרשם הגיעו תלונות בנושא קושי בטיפול בסיסמא לפי תקן זה.

לאחר בחינה מקיפה של הנושא והתייעצות עם הגורמים הרלבנטים, ניתנה הנחייה המאפשרת הוראות מקלות יותר, שאינן פוגעות במידת האבטחה והבטיחות של השימוש בחתימה.

בנוסף, עקב תלונות הקשורות במצבים שבהם משתמש שוכח סיסמא, נקבע הסדר ספיציפי לנושא זה. בתמצית ייאמר כי לשחרור מנעילה של כרטיס יש חשיבות צרכנית רבה ללקוח, משום שהדבר מאפשר לו לחזור ולהשתמש בתעודה האלקטרונית שלו לחתימה אלקטרונית, מבלי שיידרש להנפיק תעודה אלקטרונית חדשה. מנגד, מנגנון שחרור מנעילה של אמצעי חתימה, טומן בחובו סיכון לשימוש

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

לרעה באמצעי החתימה, שכן ניתן באמצעות המנגנון להשתלט על אמצעי החתימה ולעקוף את מנגנוני ההגנה שלו.

על מנת לאזן בין שני צרכים אלה, כוללת ההנחיה אפשרות להגיש בקשה מתאימה לרשם בה מוצע מנגנון כזה. במועד הגשת הדוח הגישה חברת קומסיין בקשה מתאימה שנבחנה ואושרה[13]. בשל חשיבותו של נושא זה הוא עובר בחינה מחודשת.

2) הנחייה 2-2010

הנחיה 2-2010 נועדה לקבוע חובות מהותיות למערכות הטכנולוגיות הייעודיות המשמשות גורם מאשר בפעילותו, ודרכי דיווח אודותן. נוסח ההנחיה מצ"ב כנספח ב' לדו"ח זה.

בהתאם לתקנה 4 ו – 5 לתקנות חתימה אלקטרונית, נדרש גורם מאשר כתנאי סף לפעילותו ובכל עת, כי מערכות הליבה המשמשות את פעילותו יעמדו בתקן אבטחת המידע Common Criteria המוכר גם כתקן ישראלי 15408. תקן זה הינו תקן אבטחת מידע מחמיר, והיצע המוצרים העומדים בו אינו גדול. בנוסף, הוא מקשה על הגמישות התפעולית של הגורם המאשר משום ששינויים שמבוצעים במערכות הגורם המאשר עשויות לחרוג מגדר התקן. מבחינת פיקוח הרשם, נדרשה מעטפת בדיקות לוודא כי מוצרי הליבה מופעלים בהתאם להנחיות ולדרישות של התקינה.

על מנת לאפשר גמישות תפעולית לגורמים המאשרים, להקל על עבודת הפיקוח של הרשם, ולוודא כי מכלול הנושאים המהותיים הנדרשים לבטיחות ואבטחה של מערכת הליבה מטופלים, החליט הרשם ליישם בישראל, בשינויים מסויימים, תוצרים של עבודת ההסדרה האירופאית.

בין תוצרי העבודה של גורמי התקינה האירופאים, מצוי מסמך " Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements CWA 14167-1[14], כלומר ניהול מערכת של גורם מאשר.

מסמך זה מגדיר את הפונקציות החיוניות במסגרת מערכת כאמור, ומכסה את התחומים בהם יש דרישה מנדטורית לבדיקה של אבטחת המידע ומהימנות במערכת

[13] ראו לעיל.

[14] CEN Workshop Agreement, Security Requirements for Trustworthy Systems Managing Certifcates for Electronic Signatures – Part 1: System Security Requirements, June 2003.cbux;

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

ניהול תעודות אלקטרוניות של גורם מאשר, וקובע את הדרישות מהן. מטרת התקן להגדיר דרישות אבטחה כוללות מהמערכת. התקן נועד לשימוש על ידי מתכננים של מערכות המשמשות לניהול תעודות לחתימה אלקטרונית, כמו גם ללקוחות של מערכות כאלה.

בבירור עם רשמים מקבילים מאירופה, תקן CWA 14167-1 משמש מקור מקצועי לעניין הסטנדרט הנדרש ממערכת המנהלת את התעודות. בנוסף, הוא נקבע גם כמסמך בעל תוקף מנחה, בהתאם להוראות סעיף 3(5) לדירקטיבה.

להכרה בתקן ולשימוש בו במסגרת פעילות גורם מאשר יתרונות מבחינת הרחבת היצע המערכות שניתן להשתמש בהן לגורם מאשר, תוך התאמה של מעטפת האבטחה לארגון המסוים בה מוטמעת המערכת. כך למשל באירופה נעשה שימוש בתקן זה לצורך בחינה של מערכות בפיתוח עצמי על ידי הגורם המאשר.

אופן בדיקת התקן שונה מהבדיקות הנדרשות לצורך עמידה בתקן Common Criteria. מאחר שבישראל אין מעבדה מוסמכת לתקן זה, יש חשיבות לאפשרות הסתמכות על גורמי בדיקה נוספים. בהתאם למסמך עזר שפורסם למסמך CWA 14167-1, הידוע כ- CWA 14172-3, ניתן להסתמך על חוות דעת מקצועית של גורם מומחה בלתי תלוי לעניין אופן עמידה בתקן. בהתאם לכך נכללו בהנחייה 2-2010 הוראות ודרישות לעניין תנאי הכשירות של עורך חוות הדעת ולגבי אופן עריכתה.

ההנחיה נכנסה לתוקף ביולי 2010. נכון לסוף שנת 2010, למרות ארכות, הגורם המאשר הרשום, חברת קומסיין, לא עמדה בהנחייה, הן מבחינה מהותית (כלומר מימוש של עקרונות התקן במערכותיו) והן מבחינה טכנית, כלומר הצגת חוות דעת המפרטת את אופן העמידה בהנחייה. בעקבות זאת נדחה גם כניסתה לתוקף של הנחייה 4-2010, כמפורט מטה.

במסגרת הטיפול בהנחייה 2-2010 נחשפו פרטים חשובים ומשמעותיים על פעולת קומסיין. במסגרת זו התברר כי לקומסיין אמנם הייתה בעלת מערכת שהוסמכה לתקן כנדרש בתקנה 5, אולם אופן השימוש בפועל במערכת חרג מההסמכה, באופן שהמערכת לא עומדת לכאורה גם בדרישות תקנה 5 עובר להוצאת ההנחייה. חברת קומסיין מבצעת מאז דצמבר 2010, שינויים משמעותיים במערכות המידע שלה באופן שמעיד על כוונה לציית להנחיה. נושא זה ממשיך ומתברר במהלך 2011, וידווח בדו"ח 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

3) הנחייה 4-2010

הנחיה 4-2010 נועדה להשלים את מהלך עדכון האלגוריתמים ואורכי המפתחות לביצוע חתימה אלקטרונית לפי החוק, בהמשך לחוות דעת של ד"ר בני פנקס, וכפי שדווח בדוחות קודמים. נוסח ההנחיה מצ"ב כנספח ג' לדו"ח זה.

בתקופה הרלבנטית לדוח זה היה רשומה במרשם רק חברת קומסיין. מימוש הנחייה 4-2010 הוא בעל השלכות על מערכות המידע של הגורם המאשר מאחר שהוא מחייב חילול והנפקה של מפתחות חדשים לחתימה אלקטרונית של תעודות אלקטרוניות לחתימה אלקטרונית מאושרת בהתאם להנחייה.

מאחר שחברת קומסיין התקשתה לעמוד בהנחייה 2-2010 להנחת דעת הרשם, התקבלה החלטה שכל הקשור למימוש הנחייה 4-2010 לגבי מערכותיה יידחה עד לעמידה של המערכת להנחת דעת הרשם בהנחיה.

בתחילת שנת 2011 נדחה יישום ההנחיה שוב לבקשת גורמי המדינה בשל הצורך בהערכות ליישום ההנחיה. בהתאם לכך הנחייה 4-2010 נכנסה לתוקף בתחילת 2011 לעניין משתמש הקצה החותם, אולם לעניין החתימה של הגורם המאשר היא תכנס לתוקף בהמשך שנת 2011.

4) הנחייה 5-2010 - זיהוי חלופי

מטרת הנחייה זו לממש את ההסמכה בתיקון בתקנות חתימה אלקטרונית שנועד לאפשר שימוש במסמך זיהוי חליפי שני שאינו דרכון או רשיון נהיגה, והיא מממשת את תיקון התקנות המפורטות להלן. נוסח ההנחיה מצ"ב כנספח ד' לדו"ח זה.

במקביל לצורך יישום התקנות פנה הרשם לגורמים המנפיקים תיעוד עם תמונה על מנת לבחון אפשרות של הכרה בתיעוד זה כמסמך זיהוי נוסף. למועד עריכת דוח זה לא הגיעו תגובות רלבנטיות.

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. תיקוני חקיקה

בשנת 2010 היתה רמו"ט שותפה מרכזית בתהליכי חקיקה וחקיקת משנה אשר עדכנו את החוק. במסגרת זו הציגה רמו"ט היבטים מעשיים של יישום החוק למקבלי ההחלטות בממשלה ובכנסת, על בסיס הידע שנצבר אצלה בהפעלת סמכויות הרשם והתמקצעות בנושא משפט וטכנולוגיה.

1) חוק חתימה אלקטרונית (תיקון מס' 2), התש"ע-2010

ב- 07.07.2010 אושר תיקון מספר 2 לחוק לאחר דיון מקיף בוועדת המדע והטכנולוגיה של הכנסת. התיקון מבוסס על הצעת חוק ממשלתית שנועדה להסדיר הנפקת תעודות אלקטרוניות לחתימה אלקטרונית מאושרת על ידי המדינה באמצעות יחידותיה, ולקבוע ביחס לפעילות זו את ההרשאות הנדרשות. הצעת החוק קשורה לפרוייקט תעודת הזהות החכמה החדשה, אשר במסגרתו מבקשת הממשלה להנפיק תיעוד לאומי (תעודת זהות ודרכון) המבוסס על כרטיס חכם (SmartCard) המכיל שבב מחשב המבצע פעולות עיבוד קריפטוגרפיות.

במסגרת ההסדרה החקיקתית חוקק חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע-2009 במסגרתו תוקן חוק מרשם האוכלוסין, התשכ"ה-1965, וזאת על מנת להסדיר את השימוש בתעודה אלקטרונית לזיהוי.

במסגרת תיקון מספר 2 לחוק הוסדרה האפשרות של הממשלה לשמש כגורם מאשר לתעודות אלקטרונית על גבי התיעוד הלאומי, וכן ביחס לעובדיה. התיקון כולל גם הסמכה מתאימה לחקיקת משנה. במסגרת הדיונים בוועדת המדע הוגבלה היכולת של הממשלה לשמש כגורם מאשר על גבי תעודת הזהות לעניין שימושים שאינם קשורים בממשלה, ונקבע שהיא תהיה בתוקף לתקופה של שלוש שנים מתחילת הפיילוט הביומטרי.

במסגרת תיקון מספר 2 הוסיפה הוועדה פרק אכיפה חלופית המסמיך את רשם גורמים מאשרים (בפרק זה – הרשם), במקרה של העדר ציות של הגורם המאשר להנחייתו, להטיל עיצום כספי בסך 70,000 ₪. הפרק מבוסס על עבודת מטה שבוצעה

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

במשרד המשפטים בתחום האכיפה המנהלית החלופית ועל סמך הניסיון שנצבר ברמו"ט בשנים האחרונות בפיקוח על הגורמים המאשרים.

2) עדכון תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

במהלך 2010, בעקבות תלונות חוזרות של אזרחים בעניין רף הזיהוי המחמיר הנדרש בתקנות חתימה אלקטרונית, בוצע תיקון לתקנה 10 המרחיב את התיעוד עליו אפשר להסתמך בעת הנפקת תעודה אלקטרונית.

כרקע יצויין כי בשל תופעה של זיופי תעודת זהות, נקבע בתקנות כי לצורך הנפקת תעודה אלקטרונית, המהווה תעודת הזהות לעולם המקוון, נדרש זיהוי על בסיס שני מסמכי זיהוי ובמקביל בדיקה מקוונת במרשם האוכלוסין.

הוראות תקנה זו העלו קשיים לגבי אוכלוסיות שאין להן מסמך זיהוי רשמי נוסף מהסוג שנקבע בתקנות (רשיון נהיגה או דרכון). בהתאם לכך תוקנו התקנות לפי הצעת הרשות, באופן המקנה שיקול דעת לגורם המאשר ומאפשר לו להסתמך, אם אין לו חשד גם על אישור בדבר זהות מטעם עו"ד. התקנות הסמיכו את הרשם לקבוע טופס מתאים בנושא זה, שנקבע ופורסם, וכן להרחיב את אפשרויות הזיהוי למסמכי זיהוי רשמיים או מעין רשמיים נוספים. לאחר התקנת התקנות פרסם הרשם הנחייה בנושא זה (ראו לעיל הנחייה 2010-5).

ה. פעילות במסגרת FESA

ב- 13-14.04.2010 התקיים בורשה, פולין המפגש התקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית (Forum of European Supervisory Authorities – FESA), באירוח משרד הכלכלה הפולני והמכון הפולני לחקר המחשבים.

ארגון FESA הוקם באופן וולנטרי על ידי החברים, ואינו בעל מעמד רשמי של ארגון דיפלומטי אלא מהווה פורום להחלפת דעות ותיאום עמדות בין רשויות הפיקוח.

החל משנת 2007 רשם גורמים מאשרים הישראלי חבר בפורום זה כחבר משקיף, ובשנת 2008 הרשות למשפט טכנולוגיה ומידע אף אירחה את המפגש בתל אביב.

במפגש נכחו נציגים של רשויות הפיקוח מהמדינות הבאות: גרמניה, פולין, איטליה, בלגיה, הולנד, צ'כיה, שוודיה, איסלנד, לטביה, פינלנד, יוון, אוסטריה, שוויץ. כן השתתפו

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

נציג נציבות האיחוד האירופי, ושני חוקרים העוסקים במחקרים מטעם הנציבות לקידום המדיניות האירופית, ונציג הרשות האלבנית (שבסוף המפגש נבחר להיות חבר משקיף).

בנוסף הוזמנו נציגים של מספר גורמים פרטיים הפעילים בשוק זה להציג את פעילותם. במפגש הנוכחי נדונו מספר רב של נושאים בעלי רלבנטיות לישראל, ובהם עדכונים מנציבות האיחוד על מגמות ההסדרה והחקיקה, קידום סוגיות של תעודות זהות חכמות, הסדרה של רשימה ממוחשבת אחידה כלל אירופאית של "גורמים מאשרים", הצגה של פתרון חתימה המבוסס על טלפונים סלולרים, שירות וידוא תוקף חתימה אירופי ופולני, עדכונים על פעילות התקינה באירופה ובמיוחד על פורמט אחיד למסמכים חתומים וחתימות לטווח ארוך.

סיכום המפגש מצ"ב כנספח ה' לדו"ח 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

9. נספחים

נספחים לפרק 5 – פעילות בינלאומית של רמו"ט .I

1) נספח א' – הגנת הפרטיות בישראל – סקר תפיסות בקרב כלל האוכלוסייה

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

ShiluvMillwardBrown



הגנת הפרטיות בישראל
תפיסות בקרב כלל האוכלוסייה

מוגש למשרד המשפטים
דצמבר 2010

ShiluvMillwardBrown

מטרות ושיטה

מטרות	מעקב והשוואה לאורך זמן של עמדות כלל האוכלוסיה והמגזר העסקי בנושא חוק הגנה על פרטיות.
מי	581 גברים ונשים בגילאי 18 ומעלה, מתוכם: 500 יהודים ו-80 ערבים ישראלים במדגם ארצי, אקראי, ומייצג של אוכלוסיה זו.
מתי	במהלך חודש דצמבר 2010
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. הנתונים הושוו למחקר הקודם שנערך באוקטובר 2009.

ShiluvMillwardBrown



תמצית ממצאים ומסקנות

ShiluvMillwardBrown

תפיסות ביחס למידע אישי והגנה על הפרטיות:

- בישראל, קיימת תפיסה שהמידע האישי אינו מוגן כראוי, וחמור יותר שמערכת החקיקה אינה מסוגלת להתמודד עם הסוגייה:
  - 82% מהציבור סבורים כי המידע האישי אינו מוגן כראוי.
  - במקביל, החקיקה בישראל נתפסת בשיעור בינוני, אך בעליה בהשוואה לאשתקד (40% לעומת 34%), כמסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים.

מידת הבטחון של הציבור בנושא מידע אישי בידי ארגונים וחברות

- 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 ואף יותר אינו בוטח בהם בנושא, כשחוסר הבטחון העיקרי הוא לגבי חברות סקרים (63% לא בוטחים) ועמותות וארגונים שלא למטרות רווח (59% לא בוטחים). הבטחון הגדול ביותר הוא ברופאים ונותני שירותים רפואיים (77% בוטחים).
  - 55% מהציבור מדווחים, שכאשר הם מוסרים פרטים לגוף כלשהו הם **תמיד** שואלים לשם מה הם נדרשים (בעליה ממחקר אשתקד). 22% נוספים **בדרך כלל** שואלים (בירידה ממחקר אשתקד).

ShiluvMillwardBrown

מודעות לחוק הגנת הפרטיות וזכויותיו

- רוב הציבור (82%) סבור שמודעות הציבור לתחום ההגנה על מידע אישי נמוכה. בפועל, המודעות סבירה, למעט המודעות לרשם מאגרי המידע שהיא אכן נמוכה:
  - 61% מהציבור מאשרים כי ידוע להם שמי שאוסף עליהם מידע צריך לזהות עצמו, ולהציג את מטרת השימוש במידע, כדי שיוכל לשמור אותו במאגר מידע.
  - 78% מהציבור סבורים כי נדרשת הסכמתם לשם שימוש במידע אודותיהם.
  - 77% מהציבור סבורים כי החוק בישראל מאפשר להם לתבוע בהליך משפטי פיצויים בשל הפרת חוק הגנת הפרטיות.
  - 45% 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 23% מהציבור מודע ליחידת רשם מאגרי המידע
  - < 13% מהציבור (כ- 60% מהמודעים ליחידה) סבורים שהיחידה מוסמכת לברר ולטפל בתלונות של אנשים בנושא זה.
  - < רק 3% מהציבור (13% 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:
  - 67% מהציבור מודאגים מהשארת מידע אישי באינטרנט
  - רק 20% מהציבור סבורים כי העברת מידע על ידם באמצעות האינטרנט בטוחה יחסית, 72% אינם סבורים כך.
  - עם זאת, רק 13% מציבור גולשי האינטרנט בודקים **תמיד** מהי מדיניות שמירת הפרטיות של האתר אליו גלשו ו-16% בודקים **בדרך כלל**. 17% מגולשי האינטרנט בודקים **לעיתים רחוקות** ו-44% מהם **כלל לא** בודקים.
  - 47% מהציבור (50% מגולשי האינטרנט) שמעו על כלים או טכנולוגיות המגבילים או מונעים איסוף מידע מהמחשב האישי ע"י גורמים זרים (בירידה ממחקר אשתקד).
  - רק ל-26% מהציבור (כ-55% מהמודעים לכלים) יצא להשתמש בכלים אלו (בירידה לעומת מחקר אשתקד).
  - עיקר החסמים לשימוש בכלים אלו, בקרב המודעים להם, הם חסמים טכניים – חוסר מודעות לאופן התקנתם וחוסר מודעות לאופן השימוש בהם.

ShiluvMillwardBrown



הצגה גראפית של ממצאים ומסקנות

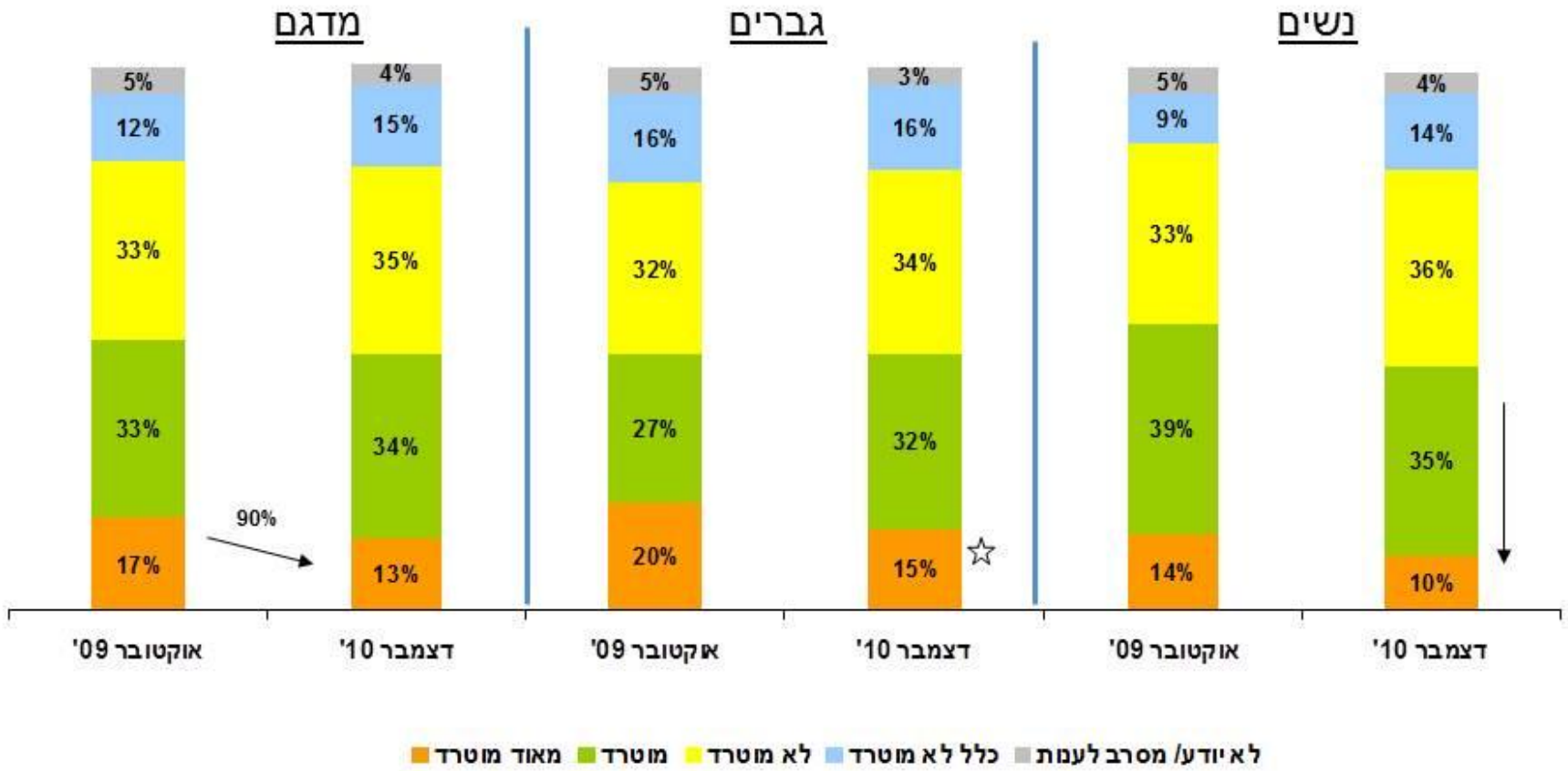
ShiluvMillwardBrown



תפיסות ביחס למתן מידע אישי והגנת הפרטיות

ShiluvMillwardBrown

המידה בה מוטרד הציבור מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי - בדיקה נעזרת



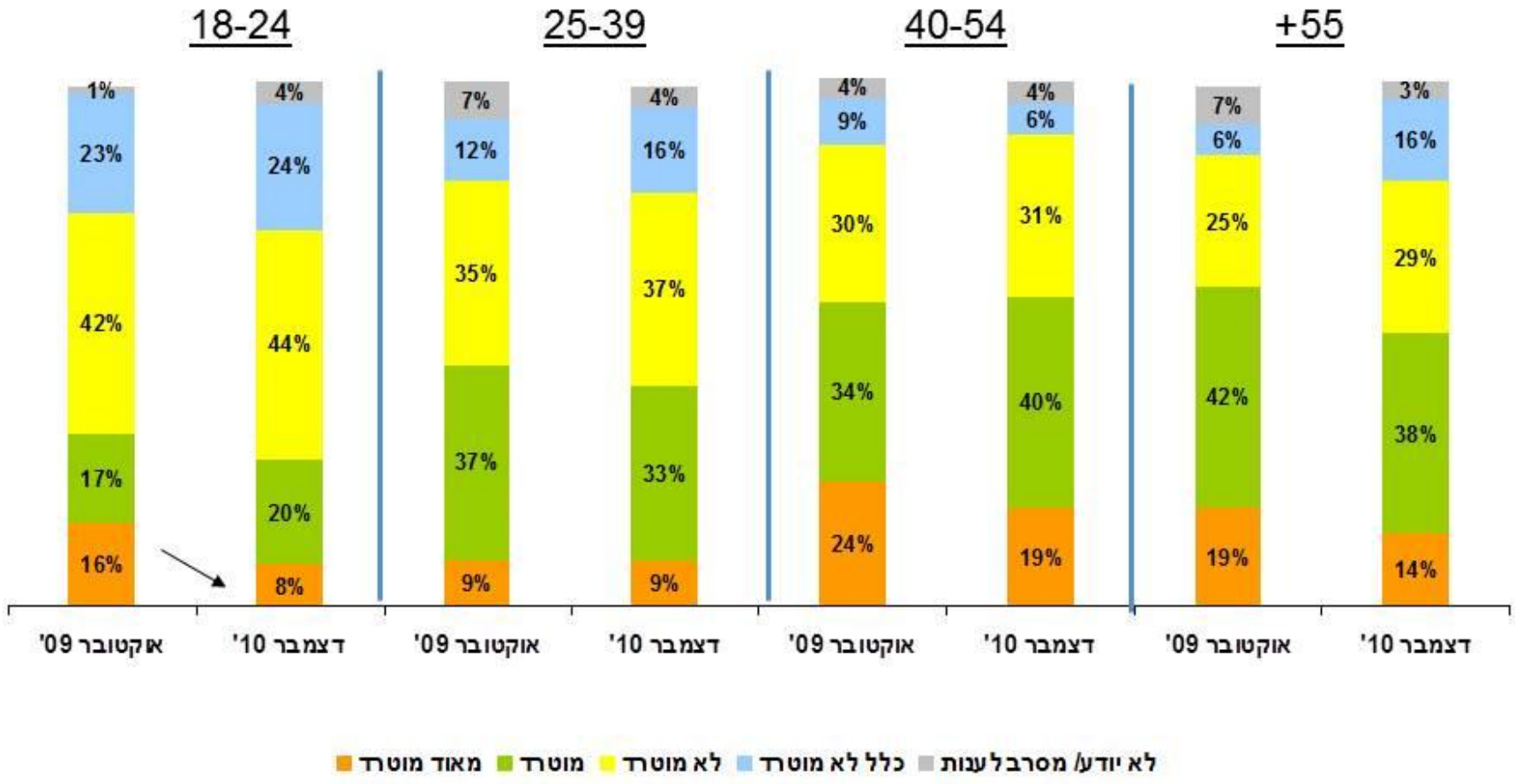
- כמחצית מהציבור מוטרד מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי לגבי אנשים.
- גברים מוטרדים במידה גבוהה יותר מנשים.
- בהשוואה לאוקטובר 09' חלה ירידה קלה בשיעור הנשים המוטרדות מ – 53% ל – 45%.

[Q1] מידע פרטי על אנשים נשמר בידי גופים ציבוריים ופרטיים. האם אתה מוטרד מהאופן בו מַגְנִים ארגונים אלה על המידע אודותיך

☆ **הבדל מובהק**

ShiluvMillwardBrown

המידה בה מוטרד הציבור מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי - בדיקה נעזרת



- הציבור מוטרד יותר ככל שהגיל עולה (מגיל 18 ועד 54).

[Q1] מידע פרטי על אנשים נשמר בידי גופים ציבוריים ופרטיים. האם אתה מוטרד מהאופן בו מַגִנים ארגונים אלה על המידע אודותיך

☆ הבדל מובהק

ShiluvMillwardBrown

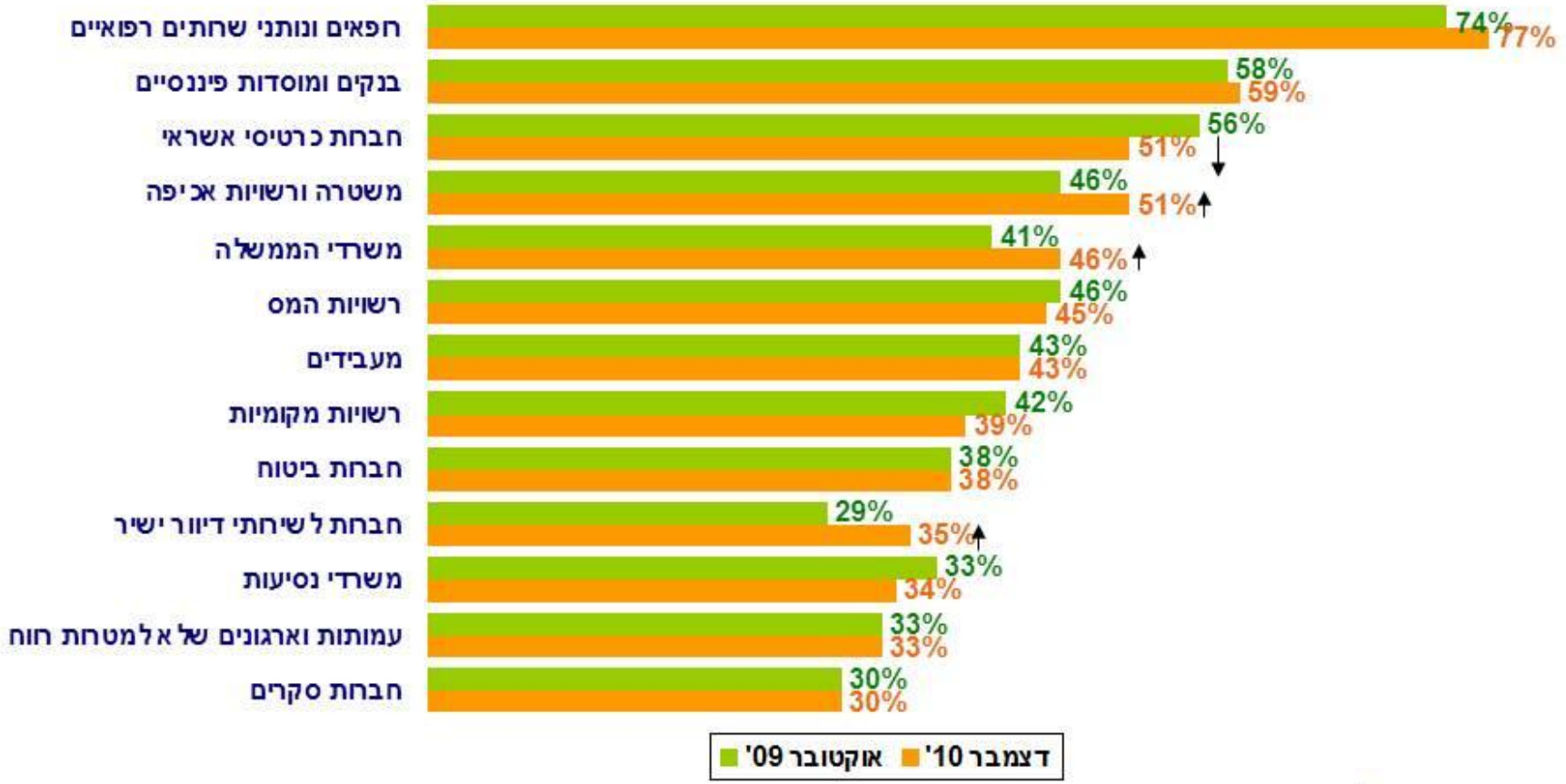


עד כמה הציבור בוטח בארגונים וחברות בנושא מידע אישי

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 סקרים, עמותות וארגונים שלא למטרות רווח, משרדי נסיעות וחברות לדיוור ישיר.
- הציבור לא בוטח מספיק ברשויות ממשלתיות כגון: רשויות מס, משטרה, רשויות מקומיות ומשרדי ממשלה.
- עם זאת, בהשוואה למחקר אשתקד חלו עליות במידת הביטחון של חברות לדיוור ישיר, משרדי הממשלה ובמשטרה ורשויות אכיפה. ירידה ברמת הביטחון חלה ביחס לחברות כרטיסי האשראי.

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
	אחוז מהמדגם	77	20	59	38	51	44
מין	גברים	77	21	60	38	49 ↓	47
	נשים	78	19	58	39	53	41
גיל	18-24	76	23	64	32	50	46
	25-39	78	18	62	37	51	47
	40-54	76	23	56	41	55	42
	+55	79	17	53	42	49	40
השכלה	יסודית או תיכונית ללא בגרות	79	16	58	35	44	47
	תיכונית עם תעודת בגרות	78	21	62	36	54 ↓	43
	על תיכונית או אקדמאית	78	20	58	41	54	42
אזור מגורים	ירושלים	75	19	59	36	47	47
	מרכז	71	25	53	44	54	40
	צפון	82	18	55	43	47	50
	דרום	75	20	70	28	58	37
	שרון	88	11	66	31	50	44
משלח יד	עצמאי	73	24	57	41	50	48
	שכיר	77	21	60	38	53	44
	ללא מקצוע	80	16	57	37	48	41

- בקרב מי שבוטח ברופאים ונותני שירותים רפואיים ייצוג יתר לתושבי אזור השרון.
- ככל שעולה הגיל יורד הביטחון בבנקים ובמוסדות פיננסיים. כמו כן קיים בטחון רב יותר במוסדות אלה בקרב תושבי הדרום.
- בעלי השכלה על תיכונית או אקדמאית בוטחים יותר בנושא שמירה על מידע אישי בחברות כרטיסי האשראי.

↓ השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת ניתוח סוציו דמוגרפי

		רשויות המס		משטרה והרשויות האכיפה		מעבידים	
		בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
	אחוז מהמדגם	45	49	51	45	43	48
מין	גברים	48	48	51	46	42	50
	נשים	43	50	51	44	44	46
גיל	18-24	43	51	48	49	40	53
	25-39	52	45	59	38	52	39
	40-54	44	49	52	44	45	49
	+55	40	52	43	51	31	55
השכלה	יסודית או תיכונית ללא בגרות	46	48	50	45	39	45
	תיכונית עם תעודת בגרות	48	44	57	40	44	50
	על תיכונית או אקדמאית	45	50	50	47	46	48
אזור מגורים	ירושלים	51	46	55	45	53	37
	מרכז	45	49	47	48	44	45
	צפון	47	45	49	45	37	56
	דרום	41	56	56	41	47	45
	שרון	43	50	53	45	39	51
משלח יד	עצמאי	47	49	47	50	46	45
	שכיר	49	48	56	41	49	45
	ללא מקצוע	39	51	44	48	31	54

- בקרב גילאי 25-39 גבוה יותר הבטחון ברשויות המס.
- הביטחון במשטרה וברשויות האכיפה גבוה בקרב גילאי 25-39, תושבי אזור הדרום ושכירים .
- ייצוג גבוה לבוטחים במעבידים בקרב הגילאים 25-39. כמו כן, בקרב הבוטחים במעבידים, ייצוג גבוה לשכירים.

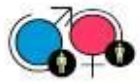
↓ השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת ניתוח סוציו דמוגרפי

		רשויות מקומיות		משרדי ממשלה		חברות ביטוח	
		בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
	אחוז מהמדגם	39	57	46	49	38	58
מין	גברים	39	59	48	48	40	56
	נשים	39	55	44	49	36	59
גיל	18-24	53	45	54	43	52	45
	25-39	40	57	53	45	38	61
	40-54	32	65	42	53	33	62
	+55	34	58	36	53	33	59
השכלה	יסודית או תיכונית ללא בגרות	43	52	46	45	46	45
	תיכונית עם תעודת בגרות	41	57	50	47	45	52
	על תיכונית או אקדמאית	37	58	46	50	32	65
אזור מגורים	ירושלים	38	55	52 ↓	47	41	53
	מרכז	41	56	38	55	33	62
	צפון	40	56	54	40	46	51
	דרום	36	58	46	49	32	61
	שרון	38	62	38	59	32	65
משלח יד	עצמאי	36	62	39	55	47	47
	שכיר	42	55	50	47	34	64
	ללא מקצוע	35	58	43	48	41	51







- גילאי 18-24 בוטחים יותר ברשויות המקומיות לעומת המבוגרים יותר וגם בעלי השכלה נמוכה.
- בקרב קבוצות הגיל 18-39, ובקרב תושבי הצפון. הבטחון במשרדי הממשלה גבוה יותר .
- בקרב הגילאים 18-24, בעלי השכלה תיכונית ומטה ותושבי הצפון ייצוג גבוה יותר לבוטחים בחברות הביטוח.

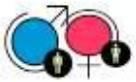
↓ השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

תפיסת הביטחון בהגנה על מידע אישי בקרב גופים וארגונים – בדיקה נעזרת ניתוח סוציו דמוגרפי

		משרדי נסיעות		עמותות וארגונים		חברת סקרים		חברות לשיחתי דיוור ישיר	
		בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח	בוטח	לא בוטח
	אחוז מהמדגם	34	57	33	59	30	63	35	53
מין	גברים	36	58	37	58	28	67	34	57
	נשים	32	56	29	60	31	59	36	50
גיל	18-24	33	61	43	52	38	60	48	39
	25-39	35	60	36	58	28	68	40	54
	40-54	31	59	30	62	22	70	32	61
	+55	36	47	25	64	32	51	22	56
השכלה	יסודית או תיכונית ללא בגרות	44	45	40	54	40	48	48	39
	תיכונית עם תעודת בגרות	30	58	39	55	30	62	40	51
	על תיכונית או אקדמאית	31	62	27	64	26	69	28	60
אזור מגורים	ירושלים	38	53	38	49	28	61	42	44
	מרכז	32	57	32	61	34	60	27	59
	צפון	37	53	32	62	33	58	44	46
	דרום	29	61	34	58	18	75	33	57
	שרון	31	65	32	61	29	65	25	66
משלח יד	עצמאי	43	52	37	57	28	65	35	53
	שכיר	27	63	33	61	26	67	34	57
	ללא מקצוע	41	49	32	56	36	54	37	48







- הבטחון במשרדי נסיעות גבוה יותר בקרב בעלי השכלה יסודית או תיכונית ללא בגרות ובקרב עצמאיים.
- בקרב גברים, גילאי 18-39 ובעלי השכלה תיכונית ומטה, הביטחון בעמותות וארגונים גבוה יותר.
- הבטחון בחברת סקרים גבוה יותר בקרב גילאי 18-24, בקרב בעלי נמוכה ובקרב אלו שללא מקצוע.
- הבטחון בחברת לשיחתי דיוור ישיר יורד עם הגיל. כמו כן, הוא גבוה יותר בקרב בעלי השכלה תיכונית ומטה ובקרב תושבי אזור ירושלים וצפון.

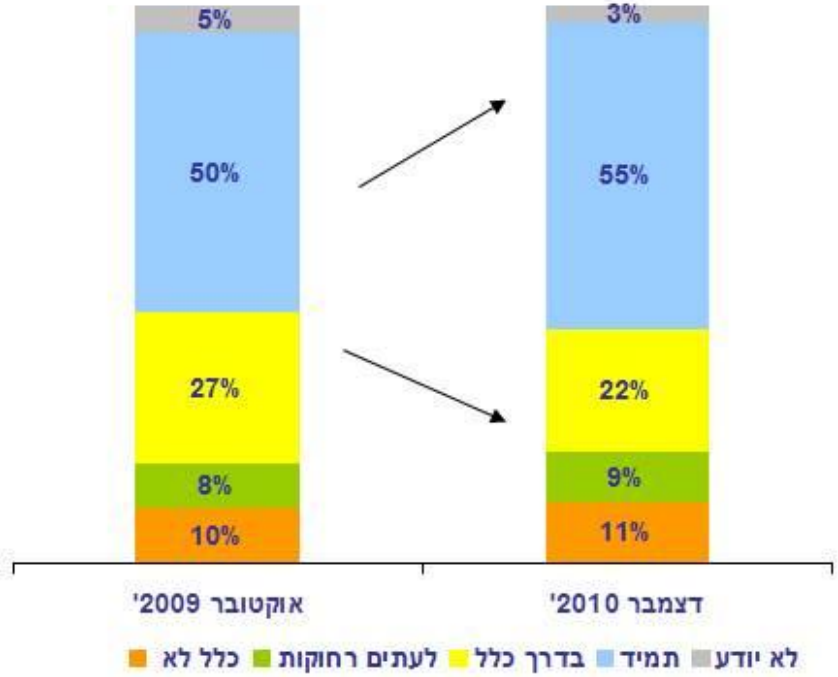
↓ השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

מתן פרטים אישיים והגנת הפרטיות - נעזר

כלל המדגם



- מרבית הציבור מדווח כי אינו נותן פרטים אישיים מבלי לברר את הסיבה: 55% ישאלו תמיד לשם מה הם נדרשים (בעליה לעומת מחקר אשתקד) בעוד ש-22% נוספים ישאלו בדרך כלל (בירידה לעומת מחקר אשתקד).

Q32. כאשר אתה מוסר פרטים לגוף כלשהו, האם אתה שואל לשם מה הם נדרשים?

נספח א' – הגנת הפרטיות בישראל – סקר תפיסות בקרב כלל האוכלוסייה

ShiluvMillwardBrown

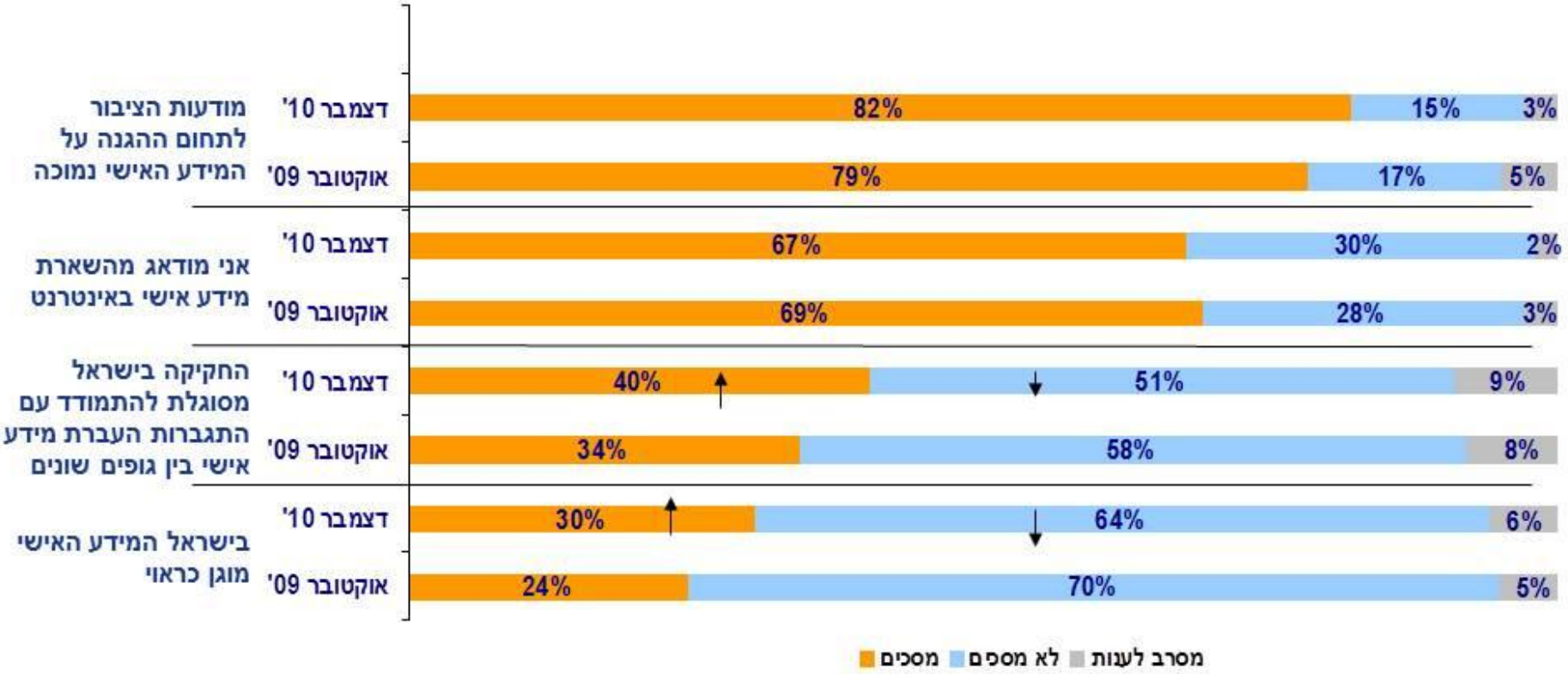


הגנה על הפרטיות בישראל

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת

כלל המדגם



- הציבור מוטרד בנושא ההגנה על המידע האישי ומהמודעות הנמוכה לתחום: 82% מהציבור חושבים שהמידע האישי אינו מוגן כראוי, כשני שלישים מודאגים מהשארת מידע אישי באינטרנט ורק 30% סבורים שהמידע האישי בישראל מוגן כראוי (בעליה ממחקר אשתקד).
- 40% מהציבור חושבים שהחקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי (בעליה ממחקר אשתקד).

Q15-18. [Q3] אקריא בפניך דעות שציינו אנשים שונים, עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים

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
אחוז מהמדגם	30	64	82	15
מין				
גברים	32	64	84	13
נשים	28	65	80	18
גיל				
18-24	41	54	73	21
25-39	29	64	83	16
40-54	27	69	88	11
+55	25	68	81	14
השכלה				
יסודית או תיכונית ללא בגרות	40	52	75	21
תיכונית עם תעודת בגרות	31	65	78	18
על תיכונית או אקדמאית	26	70	87	12
אזור מגורים				
ירושלים	41	55	84	15
מרכז	22	73	84	13
צפון	36	59	82	15
דרום	28	63	79	19
שרון	21	74	79	17
משלח יד				
עצמאי	25	69	76	21
שכיר	31	65	85	14
ללא מקצוע	30	62	80	15

- ההסכמה לתפיסה לפיה המידע האישי בישראל מוגן כראוי יורדת עם העליה בגיל וככל שעולה רמת ההשכלה. ההסכמה להיגד זה בולטת גם בקרב תושבי איזור ירושלים והצפון.
- בקרב הגילאים 25-54 בולטת יותר הסכמה לתפיסה לפיה מודעות הציבור לתחום ההגנה על מידע אישי נמוכה. שכירים מסכימים יותר לתפיסה זאת מול עצמאיים וכן בעלי השכלה על תיכונית או אקדמאית.

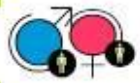
↑ השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

תפיסות בנושא מידת ההגנה על מידע אישי – בדיקה נעזרת ניתוח סוציו דמוגרפי

	אני מודאג מהשארת מידע אישי באינטרנט		החקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים	
	מסכים	לא מסכים	מסכים	לא מסכים
אחוז מהמדגם	67	30	40	51
מין				
גברים	63	35	43	49
נשים	71	25	37	54
גיל				
18-24	66	34	39	46
25-39	67	31	46	49
40-54	70	28	38	57
+55	67	28	35	52
השכלה				
יסודית או תיכונית ללא בגרות	61	36	41	44
תיכונית עם תעודת בגרות	70	28	41	52
על תיכונית או אקדמאית	69	29	38	54
אזור מגורים				
יחשלים	70	29	45	44
מרכז	68	27	32	62
צפון	65	33	46	44
דרום	64	35	34	56
שרון	77	23	47	43
משלח יד				
עצמאי	67	32	39	55
שכיר	71	27	43	50
ללא מקצוע	61	35	35	51







- בקרב נשים בולטת דאגה רבה יותר מהשארת מידע אישי באינטרנט. כך גם בקרב תושבי איזור השרון ובקרב שכירים.
- ההסכמה עם התפיסה לפיה החקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים גבוהה יותר בקרב גברים, גילאי 25-39, תושבי איזור הצפון ושכירים.

השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

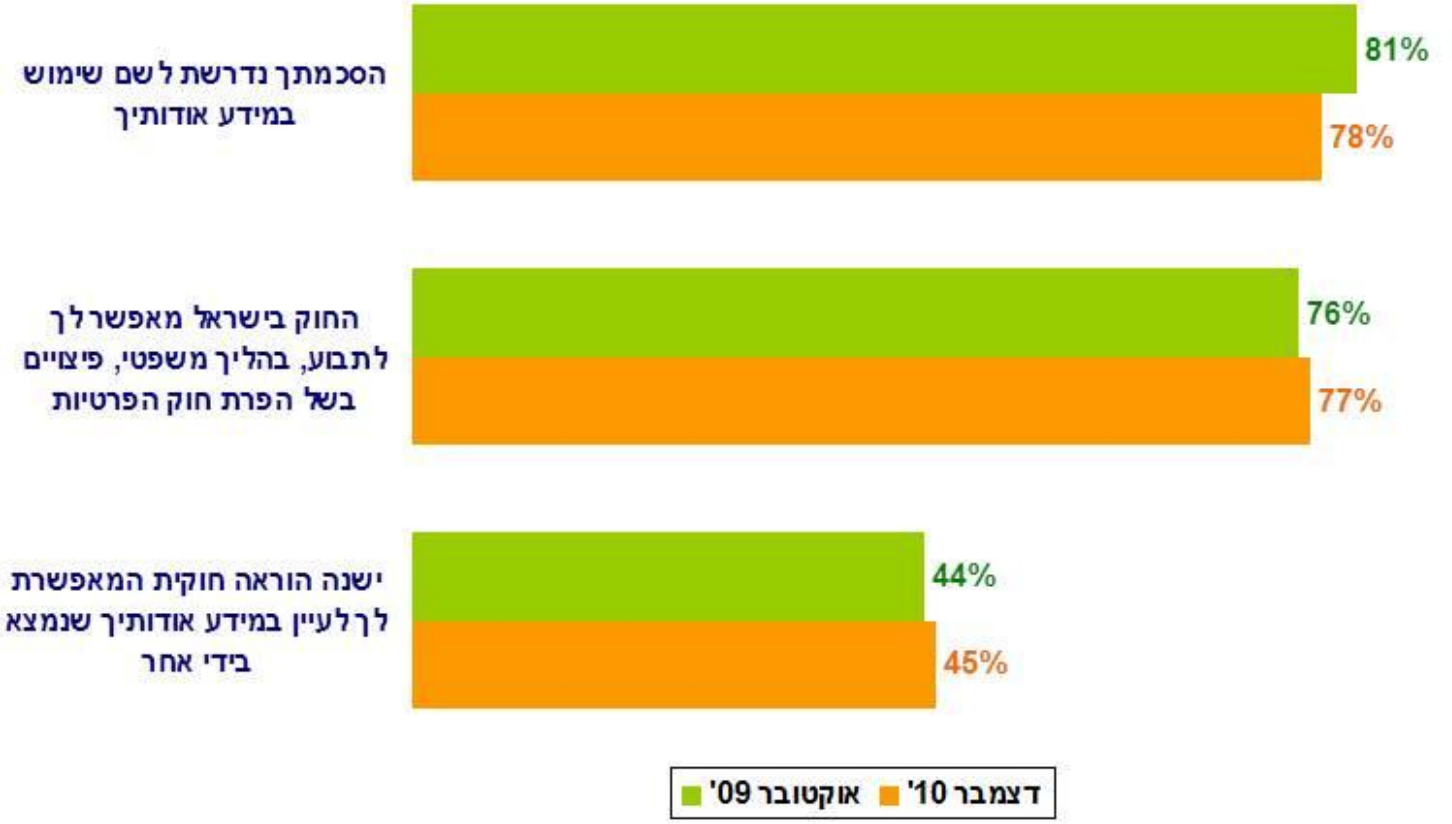


מודעות לחוק הגנת הפרטיות וזכויותיו

ShiluvMillwardBrown

תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת

% מצייני נכון בקרב כלל המדגם



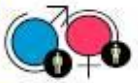
- נושא מתן הסכמה לשימוש במידע אישי ואפשרות תביעת פיצויים בשל הפרת חוק הפרטיות ידועים בקרב מרבית הציבור. יחד עם זאת, פחות ממחצית מהציבור מודעים להוראה החוקית המאפשרת עיון במידע אישי הנמצא בידי אחר.

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

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 שנמצע בידי אחר		החוק בישראל מאפשר לך לתבוע בהליך משפטי פיצויים בשל הפרת חוק הגנת הפרטיות	
	נכון	לא נכון	נכון	לא נכון	נכון	לא נכון
אחוז מהמדגם	78	18	45	36	77	9
מין						
גברים	77	18	48	36	77	11
נשים	79	17	42	35	77	8
גיל						
18-24	79	18	49	40	85	7
25-39	79	15	46	40	80	11
40-54	82	15	48	28	75	8
55+	72	24	37	37	70	9
השכלה						
יסודית או תיכונית ללא בגרות	70	26	46	39	73	9
תיכונית עם תעודת בגרות	83	16	50	35	81	11
על תיכונית או אקדמאית	80	16	43	34	77	9
אזור מגורים						
יחשלים	83	15	47	37	82	8
מרכז	74	20	43	35	75	11
צפון	79	19	43	40	80	12
דחם	75	17	48	32	75	5
שחן	87	11	47	33	73	6
משלח יד						
עצמאי	77	17	49	31	76	14
שכיר	83	16	48	35	82	7
ללא מקצוע	71	21	38	40	71	11







- בקרב גילאי 55+ פחות שכיחה התפיסה כי נדרשת הסכמה לשימוש במידע אישי. תפיסה זו שכיחה יותר בקרב בעלי השכלה תיכונית ומעלה, תושבי השרון ושכירים.
- גילאי 18-54 סבורים יותר מהמבוגרים יותר כי קיימת הוראה חוקית המאפשרת לעיין במידע אישי הנמצא בידי אחר.
- הסברה לפיה החוק מאפשר לתבוע בהליך משפטי פיצויים בשל הפרת חוק הפרטיות נפוצה יותר בקרב גילאי 18-39 ויורדת עם העליה בגיל, כמו כן היא נפוצה יותר בקרב שכירים.

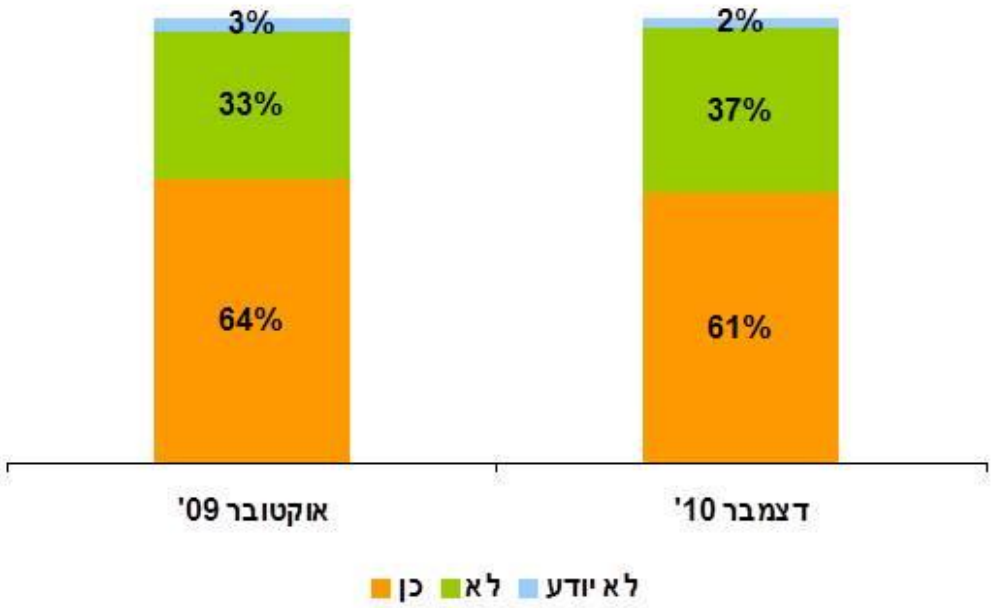
השוואה לאשתקד ↓

הבדל מובהק

ShiluvMillwardBrown

מודעות למשמעות החוק בנושא איסוף מידע – נעזר

כלל המדגם



- 61% מהציבור מודעים למתחייב מחוק הגנת הפרטיות בנושא איסוף המידע.
- בקרב מי שמודע ייצוג גבוה יותר לנשים, שכירים ולתושבי איזור השרון.
- אין הבדלים לעומת המחקר מאשתקד

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?

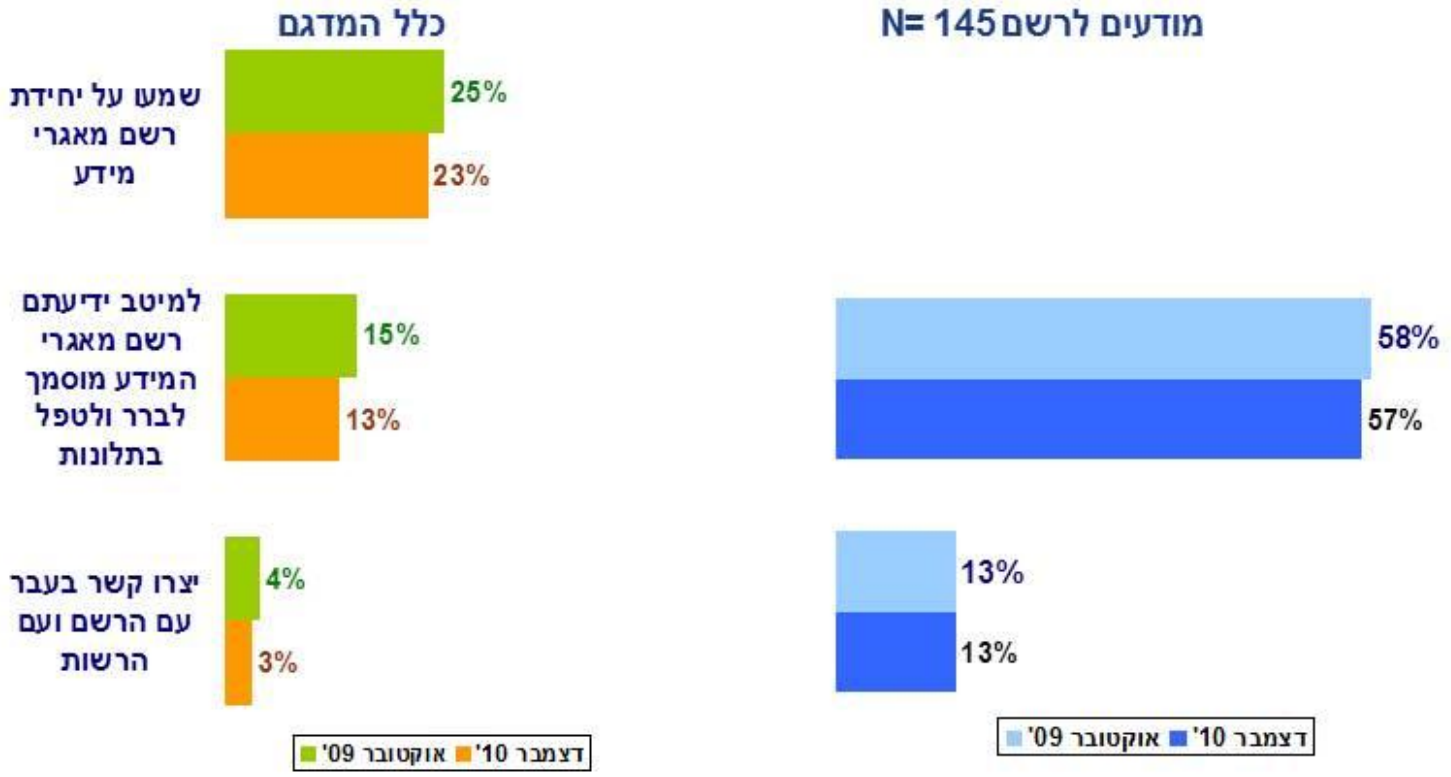
ShiluvMillwardBrown



רשם מאגרי המידע

ShiluvMillwardBrown

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?

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=131)	
	כן	לא	כן	לא
אחוז מהמדגם	23	76	57	20
מין				
גברים	25	75	56	18
נשים	21	76	58	23
גיל				
18-24	20	77	53	18
25-39	19	80	54	21
40-54	29	70	51	24
55+	22	75	70	16
השכלה				
יסודית או תיכונית ללא בגרות	23	74	63	19
תיכונית עם תעודת בגרות	18	81	58	28
על תיכונית או אקדמאית	24	75	55	20
אזור מגורים				
יחשלים	18	82	41	18
מרכז	27	71	69	14
צפון	21	78	50	36
דרום	24	73	60	8
שרון	19	79	44	21
משלח יד				
עצמאי	24	74	59	22
שכיר	24	75	54	19
ללא מקצוע	20	77	62	21

- מודעות גבוהה יותר ליחידת רשם מאגרי המידע בקרב גילאי 40-54.
- מודעות גבוהה יותר בקרב תושבי המרכז לסמכויותיו של רשם מאגרי המידע.

השוואה לאשתקד ↓

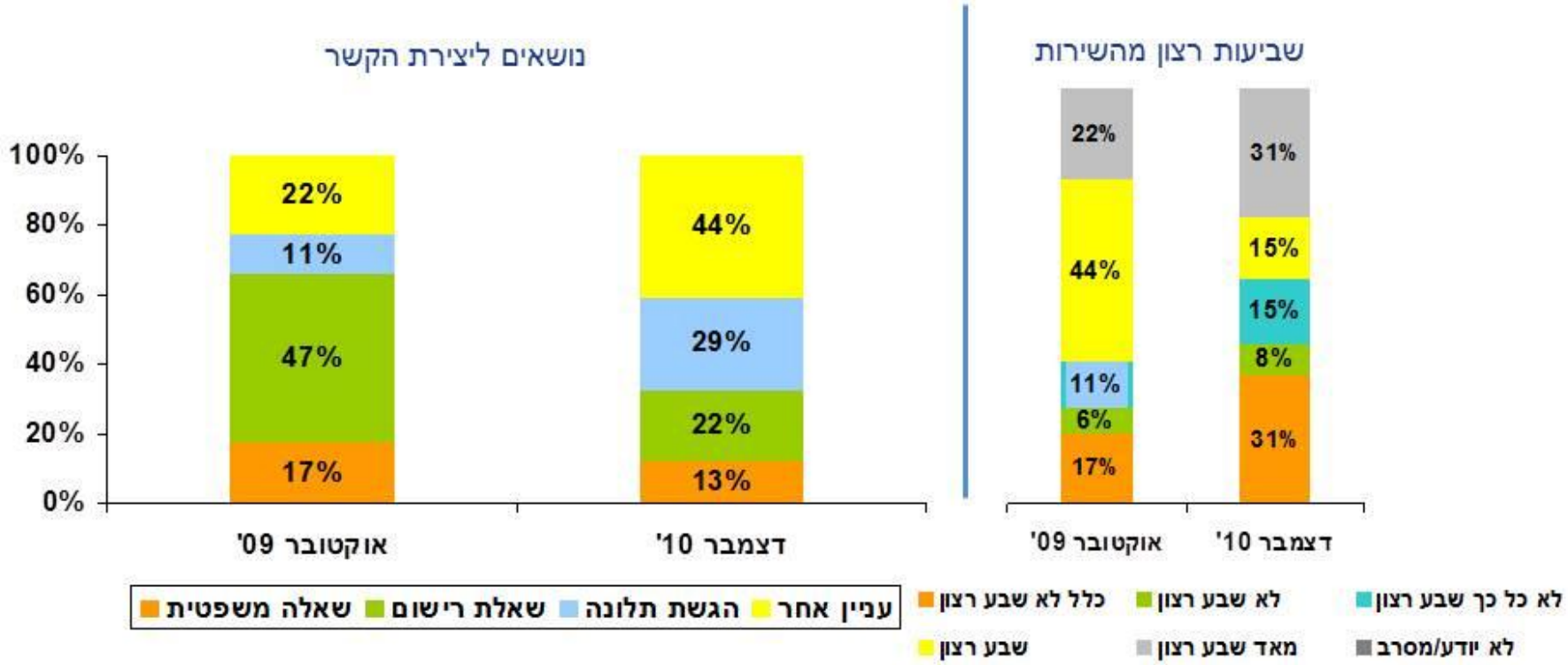
הבדל מובהק

ShiluvMillwardBrown

רשם מאגרי המידע - יצירת קשר ושביעות רצון – נעזר

בקרב יוצרי הקשר עם הרשם

*N=17



- כשליש 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?

* יש להתייחס בזהירות לממצאים כיוון שמדובר בתא סטטיסטי קטן

ShiluvMillwardBrown

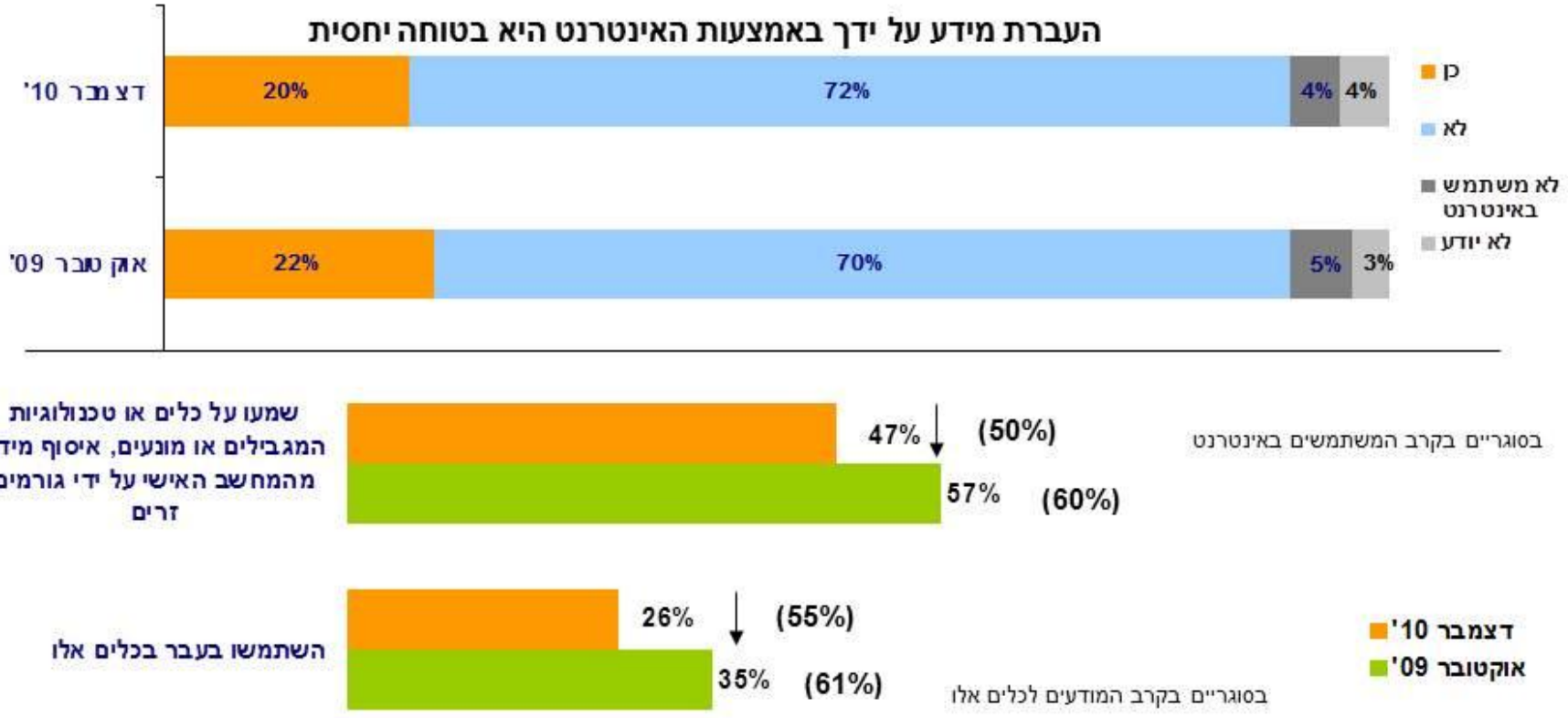


הגנה על מידע אישי באינטרנט

ShiluvMillwardBrown

תפיסות לגבי שימוש באינטרנט והגנת הפרטיות - נעזר

כלל המדגם



- שימוש באינטרנט להעברת מידע אישי אינו נתפס כבטוח.
- 47% מהמדגם מודעים לטכנולוגיות המגבילות איסוף מידע מהמחשב האישי (בירידה לעומת מחקר אשתקד), יחד עם זאת, כרבע מהציבור השתמשו בהן (גם כן בירידה ממחקר אשתקד).

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? משתמשים- N=555	
	כן	לא	כן	לא
אחוז מהמדגם	20	72	50	45
מין				
גברים	28	66	57	38
נשים	12	77	42	51
גיל				
18-24	19	77	55	40
25-39	24	71	57	39
40-54	21	70	49	47
55+	14	71	36	54
השכלה				
יסודית או תיכונית ללא בגרות	10	76	35	53
תיכונית עם תעודת בגרות	17	78	41	55
על תיכונית או אקדמאית	25	68	61	36
אזור מגורים				
יחשלים	16	79	48	47
מרכז	21	67	48	46
צפון	16	75	47	47
דרום	25	68	50	44
שרון	22	73	65	34
משלח יד				
עצמאי	18	76	60	37
שכיר	23	70	52	43
ללא מקצוע	15	74	40	52

- העברת מידע באמצעות האינטרנט נתפסת בטוחה יותר בקרב: גברים, גילאי 25-54, תפיסתה כבטוחה עולה עם עלית ההכנסה וגבוהה יחסית בקרב שכירים לעומת אחרים.
- גברים, גילאי 18-54, בעלי השכלה על תיכונית או אקדמאית, תושבי השרון ועצמאיים ושכירים המשתמשים באינטרנט שמעו יותר על טכנולוגיות המגבילות או מונעות איסוף מידע מהמחשב האישי לעומת אחרים.

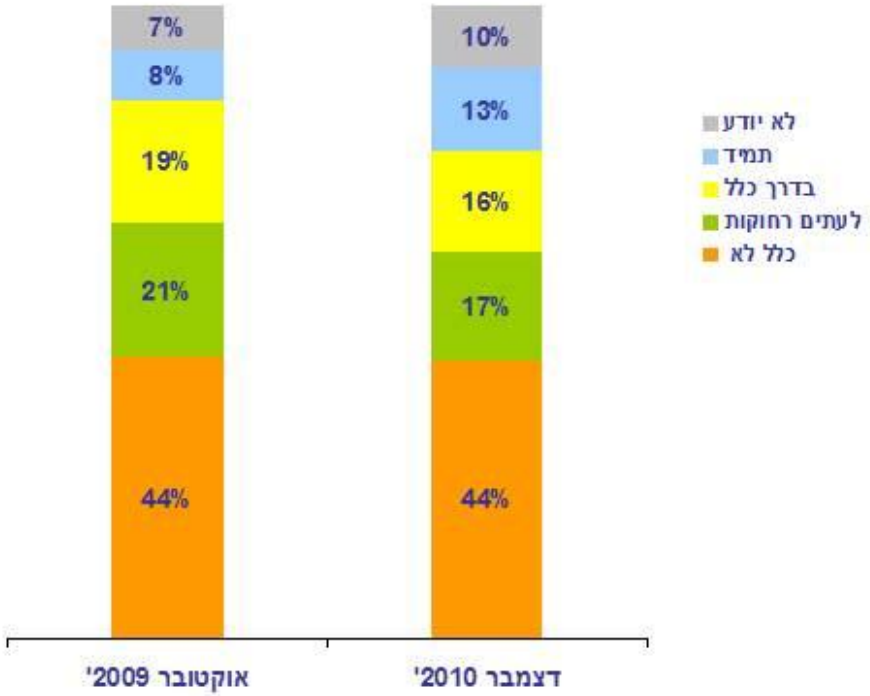
↓ השוואה לאשתקד

הבדל מובהק

ShiluvMillwardBrown

הרגלי גלישה באינטרנט והגנת הפרטיות - נעזר

בקרב גולשי האינטרנט
N=503

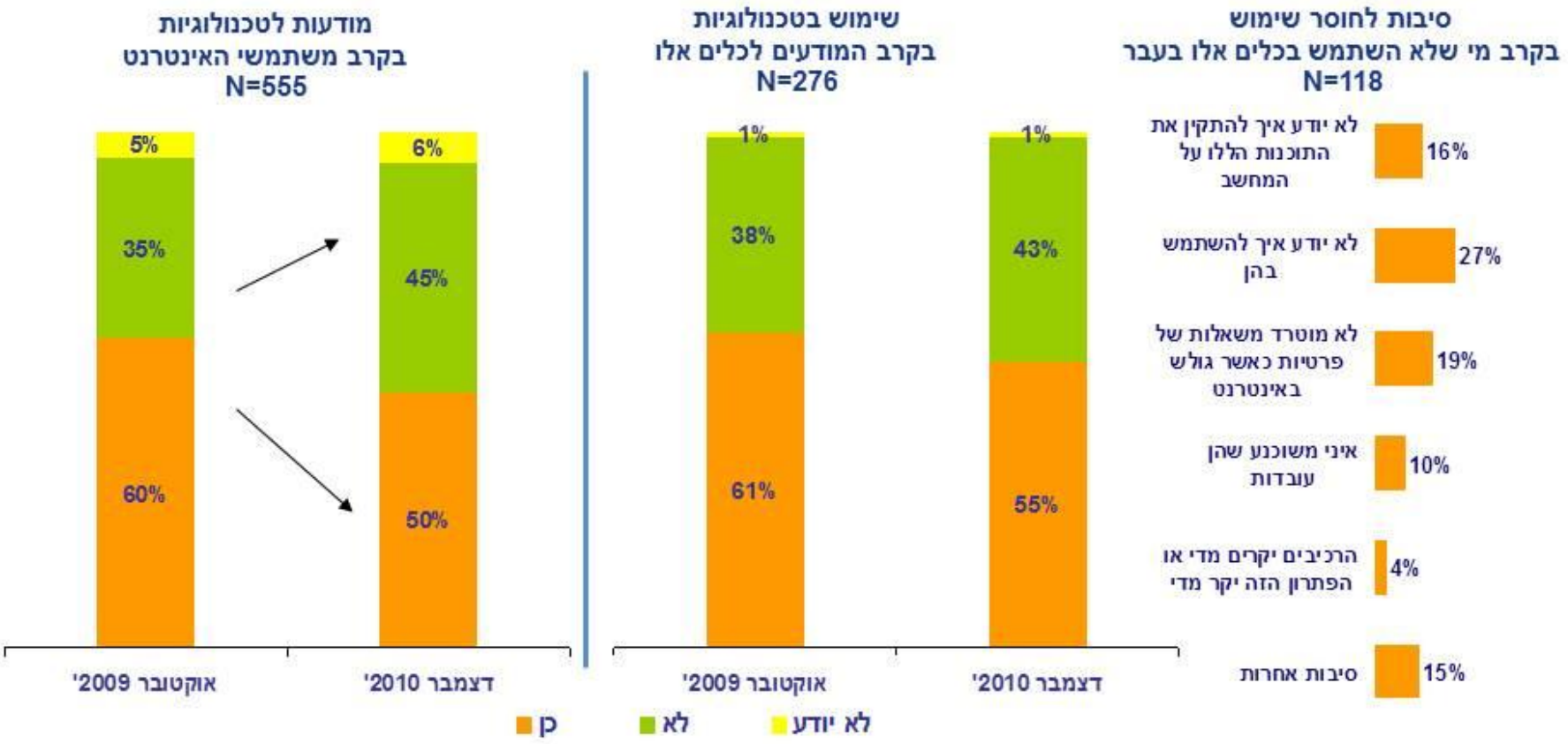


- 61% מהגולשים באינטרנט אינם נוהגים לבדוק את מדיניות שמירת הפרטיות של האתרים אליהם הם גולשים: 44% אינם בודקים כלל ו-17% בודקים לעתים רחוקות. יחד עם זאת, 13% מגולשי האינטרנט בודקים תמיד מהי מדיניות שמירת הפרטיות של האתר אליו גלשו. 16% בודקים בדרך כלל.
- בקרב הבודקים תמיד ייצוג גבוה לתושבי הדרום והצפון ושכירים. בקרב הבודקים בדרך כלל ייצוג גבוה לגברים, לתושבי הדרום ואיזור השרון.

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



- חסמים טכניים מהווים סיבה עיקרית לחוסר שימוש באמצעים טכנולוגיים המגבילים את איסוף המידע מהמחשב האישי בקרב המודעים לאמצעים אלו.

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:

נספח א' – הגנת הפרטיות בישראל – סקר תפיסות בקרב כלל האוכלוסייה

ShiluvMillwardBrown



נספח

ShiluvMillwardBrown

המידה בה מוטרד הציבור מהאופן בו מגנים גופים ציבוריים ופרטיים על מידע פרטי - בדיקה נעזרת נתונים סוציו דמוגרפיים

	מאוד מוטרד	מוטרד	לא מוטרד	כלל לא מוטרד	לא יודע \ מסרב לענות	Total
אחוז מהמדגם	13	34	35	15	4	581
מין						
גברים	15	32	34	16	3	283
נשים	10	35	36	14	4	298
גיל						
18-24	8	20	44	24	4	111
25-39	9	33	37	16	4	182
40-54	19	40	31	6	4	148
+55	14	38	29	16	3	140
השכלה						
יסודית או תיכונית ללא בגרות	12	31	38	12	6	135
תיכונית עם תעודת בגרות	8	28	40	22	1	136
על תיכונית או אקדמאית	15	38	31	13	4	283
לא השיב	11	35	39	13	3	28
אזור מגורים						
ירושלים	8	27	43	17	6	74
מרכז	14	33	38	10	5	163
צפון	11	36	32	18	2	180
דרום	12	36	31	17	4	109
שרון	18	32	37	12	1	56
משלח יד						
עצמאי	14	29	42	12	3	86
שכיר	13	36	34	13	4	313
ללא מקצוע	11	31	34	21	4	182

Q1. מידע פרטי על אנשים נשמר בידי גופים ציבוריים ופרטיים. האם אתה מוטרד מהאופן בו מַגִנִים ארגונים אלה על המידע אודותיך

ShiluvMillwardBrown

תפיסת הבטחון בהגנת מידע פרטי בגופים ציבוריים ופרטיים – % מצייני בוטח בכל קטגוריה- בדיקה נעזרת נתונים סוציו דמוגרפיים

		רשויות מקומיות	מעבידים	משטרה ורשויות אכיפה	רשויות המס	חברות כרטיסי אשראי	בנקים ומוסדות פיננסיים	חפאים ונותני שרותים רפואיים	סה"כ
	אחוז מהמדגם	39	43	51	45	51	59	77	581
מין									
	גברים	39	42	51	48	49	60	77	283
	נשים	39	44	51	43	53	58	78	298
גיל									
	18-24	53	40	48	43	50	64	76	111
	25-39	40	52	59	52	51	62	78	182
	40-54	32	45	52	44	55	56	76	148
	+55	34	31	43	40	49	53	79	140
השכלה									
	יסודית או תיכונית ללא בגרות	43	39	50	46	44	58	79	135
	תיכונית עם תעודת בגרות	41	44	57	48	54	62	78	136
	על תיכונית או אקדמאית	37	46	50	45	54	58	78	283
	לא השיב	25	29	32	30	41	50	58	28
אזור מגורים									
	ירושלים	38	53	55	51	47	59	75	74
	מרכז	41	44	47	45	54	53	71	163
	צפון	40	37	49	47	47	55	82	180
	דרום	36	47	56	41	58	70	75	109
	שרון	38	39	53	43	50	66	88	56
משלח יד									
	עצמאי	36	46	47	47	50	57	73	86
	שכיר	42	49	56	49	53	60	77	313
	ללא מקצוע	35	31	44	39	48	57	80	182

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

	חברת לשחתי דיוור ישיר	חברות סקרים	עמותות וארגונים שלא למטרת רווח	משרדי נסיעות	חברת ביטוח	משרדי ממשלה	סה"כ
אחוז מהמדגם	35	30	33	34	38	46	581
מין							
גברים	34	28	37	36	40	48	283
נשים	36	31	29	32	36	44	298
גיל							
18-24	48	38	43	33	52	54	111
25-39	40	28	36	35	38	53	182
40-54	32	22	30	31	33	42	148
+55	22	32	25	36	33	36	140
השכלה							
יסודית או תיכונית ללא בגרות	48	40	40	44	46	46	135
תיכונית עם תעודת בגרות	40	30	39	30	45	50	136
על תיכונית או אקדמאית	28	26	27	31	32	46	283
לא השיב	19	9	28	30	28	33	28
אזור מגורים							
יחשלים	42	28	38	38	41	52	74
מרכז	27	34	32	32	33	38	163
צפון	44	33	32	37	46	54	180
דרום	33	18	34	29	32	46	109
שרון	25	29	32	31	32	38	56
משלח יד							
עצמאי	35	28	37	43	47	39	86
שכיר	34	26	33	27	34	50	313
ללא מקצוע	37	36	32	41	41	43	182

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	Total
אחוז מהמדגם	30	64	6	581
מין				
גברים	32	64	4	283
נשים	28	65	7	298
גיל				
18-24	41	54	4	111
25-39	29	64	8	182
40-54	27	69	3	148
+55	25	68	6	140
השכלה				
יסודית או תיכונית ללא בגרות	40	52	8	135
תיכונית עם תעודת בגרות	31	65	5	136
על תיכונית או אקדמאית	26	70	5	283
לא השיב	20	72	8	28
אזור מגורים				
ירושלים	41	55	4	74
מרכז	22	73	5	163
צפון	36	59	5	180
דרום	28	63	9	109
שרון	21	74	5	56
משלח יד				
עצמאי	25	69	6	86
שכיר	31	65	5	313
ללא מקצוע	30	62	8	182







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	Total
אחוז מהמדגם	82	15	3	581
מין				
גברים	84	13	3	283
נשים	80	18	2	298
גיל				
18-24	73	21	5	111
25-39	83	16	1	182
40-54	88	11	0	148
+55	81	14	4	140
השכלה				
יסודית או תיכונית ללא בגרות	75	21	3	135
תיכונית עם תעודת בגרות	78	18	4	136
על תיכונית או אקדמאית	87	12	1	283
לא השיב	86	8	6	28
אזור מגורים				
ירושלים	84	15	1	74
מרכז	84	13	3	163
צפון	82	15	3	180
דרום	79	19	2	109
שרון	79	17	4	56
משלח יד				
עצמאי	76	21	3	86
שכיר	85	14	1	313
ללא מקצוע	80	15	4	182







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	Total
אחוז מהמדגם	67	30	2	581
מין				
גברים	63	35	1	283
נשים	71	25	3	298
גיל				
18-24	66	34	1	111
25-39	67	31	2	182
40-54	70	28	3	148
+55	67	28	5	140
השכלה				
יסודית או תיכונית ללא בגרות	61	36	3	135
תיכונית עם תעודת בגרות	70	28	3	136
על תיכונית או אקדמאית	69	29	2	283
לא השיב	67	30	3	28
אזור מגורים				
ירושלים	70	29	1	74
מרכז	68	27	5	163
צפון	65	33	2	180
דרום	64	35	1	109
שרון	77	23	0	56
משלח יד				
עצמאי	67	32	1	86
שכיר	71	27	2	313
ללא מקצוע	61	35	4	182







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	Total
אחוז מהמדגם	40	51	9	581
מין				
גברים	43	49	8	283
נשים	37	54	10	298
גיל				
18-24	39	46	15	111
25-39	46	49	5	182
40-54	38	57	5	148
+55	35	52	13	140
השכלה				
יסודית או תיכונית ללא בגרות	41	44	15	135
תיכונית עם תעודת בגרות	41	52	7	136
על תיכונית או אקדמאית	38	54	7	283
לא השיב	45	52	3	28
אזור מגורים				
ירושלים	45	44	11	74
מרכז	32	62	6	163
צפון	46	44	10	180
דרום	34	56	9	109
שרון	47	43	10	56
משלח יד				
עצמאי	39	55	6	86
שכיר	43	50	7	313
ללא מקצוע	35	51	14	182





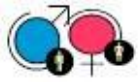


Q18. אקריא בפניך דעות שציינו אנשים שונים, עבור כל אחד מהמשפטים אנא ציין אם אתה מסכים או לא מסכים: החקיקה בישראל מסוגלת להתמודד עם התגברות העברת המידע האישי בין גופים שונים

ShiluvMillwardBrown

מודעות לרשם מאגרי המידע – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	מסכים	לא מסכים	מסרב לענות \ לא יודע	Total
אחוז מהמדגם	23	76	2	581
מין				
גברים	25	75	0	283
נשים	21	76	3	298
גיל				
18-24	20	77	3	111
25-39	19	80	1	182
40-54	29	70	1	148
+55	22	75	3	140
השכלה				
יסודית או תיכונית ללא בגרות	23	74	3	135
תיכונית עם תעודת בגרות	18	81	2	136
על תיכונית או אקדמאית	24	75	1	283
לא השיב	27	70	3	28
אזור מגורים				
ירושלים	18	82	0	74
מרכז	27	71	2	163
צפון	21	78	1	180
דרום	24	73	3	109
שרון	19	79	2	56
משלח יד				
עצמאי	24	74	2	86
שכיר	24	75	1	313
ללא מקצוע	20	77	2	182







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	לא יודע \ מסרב לענות	Total
אחוז מהמדגם	57	20	23	131
מין				
גברים	56	18	26	69
נשים	58	23	20	62
גיל				
18-24	53	18	29	22
25-39	54	21	25	35
40-54	51	24	25	42
+55	70	16	14	31
השכלה				
יסודית או תיכונית ללא בגרות	63	19	19	31
תיכונית עם תעודת בגרות	58	28	14	24
על תיכונית או אקדמאית	55	20	25	69
לא השיב	39	10	51	7
אזור מגורים				
יחשלים	41	18	40	13
מרכז	69	17	14	43
צפון	50	36	14	38
דרום	60	8	33	26
שרון	44	21	35	10
משלח יד				
עצמאי	59	22	19	21
שכיר	54	19	27	74
ללא מקצוע	62	21	17	37





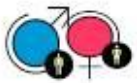


Q20. האם למיטב ידיעתך רשם מאגרי מידע מוסמך לברר ולטפל בתלונות של אנשים בנושא זה?

ShiluvMillwardBrown

יצירת קשר עם יחידת רשם מאגרי מידע - בדיקה נעזרת בקרב המודעים ליחידת רשם מאגרי מידע
נתונים סוציו דמוגרפיים

	כן - בשאלת רישום מאגרים	כן - להגשת תלונה	כן - לשאלה משפטית	כן - עניין אחר	לא	לא יודע \ מסרב לענות	Total
אחוז מהמדגם	3	4	2	6	80	7	131
מין							
גברים	3	3	0	7	76	10	69
נשים	2	4	4	4	85	3	62
גיל							
18-24	0	10	0	9	68	13	22
25-39	0	3	0	3	88	6	35
40-54	3	4	2	10	80	5	42
+55	7	0	5	0	82	6	31
השכלה							
יסודית או תיכונית ללא בגרות	2	9	7	12	68	6	31
תיכונית עם תעודת בגרות	0	4	0	11	80	4	24
על תיכונית או אקדמאית	4	1	0	1	84	9	69
לא השיב	0	0	0	0	100	0	7
אזור מגורים							
יחשלים	0	6	17	22	66	0	13
מרכז	3	0	0	0	97	0	43
צפון	2	11	0	5	61	21	38
דרום	0	0	0	6	94	0	26
שרון	14	0	0	10	66	10	10
משלח יד							
עצמאי	7	5	0	0	68	19	21
שכיר	2	3	2	5	85	3	74
ללא מקצוע	2	5	2	10	77	8	37







Q21 האם יצרת קשר בעבר עם הרשם או עם הרשות? ואם כן באיזה עניין

ShiluvMillwardBrown

שביעות רצון מהשירות שניתן ביחידת רשם מאגרי מידע - בקרב יוצרי הקשר עם הרשם או הרשות
נתונים סוציו דמוגרפיים*

	מאוד שבע רצון	שבע רצון	לא כל כך שבע רצון	לא שבע רצון	כלל לא שבע רצון	לא יודע \ מסרב לענות	Total
אחוז מהמדגם	21	13	13	4	24	24	17
מין							
גברים	16	23	8	0	20	32	9
נשים	27	0	20	10	29	13	7
גיל							
18-24	24	0	0	0	28	48	4
25-39	0	100	0	0	0	0	2
40-54	15	0	11	11	33	30	7
+55	40	0	40	0	19	0	4
השכלה							
יסודית או תיכונית ללא בגרות	0	27	19	9	33	12	8
תיכונית עם תעודת בגרות	27	0	0	0	20	54	4
על תיכונית או אקדמאית	51	0	15	0	15	20	5
לא השיב	0	0	0	0	0	0	0
אזור מגורים							
יחשלים	0	27	34	17	0	23	4
מרכז	0	0	50	0	50	0	1
צפון	29	14	0	0	28	29	7
דרום	0	0	0	0	100	0	1
שרון	60	0	0	0	0	40	3
משלח יד							
עצמאי	60	40	0	0	0	0	3
שכיר	11	0	25	0	30	34	9
ללא מקצוע	19	22	0	14	27	19	5

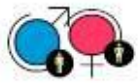
Q22 עד כמה אתה שבע רצון מהשירות שניתן לך ע"י הרשם/הרשות?

* תא סטטיסטי קטן

ShiluvMillwardBrown

מודעות לסמכויות רשם מאגרי המידע – בדיקה נעזרת
נתונים סוציו דמוגרפיים בקרב המודעים ליחידת רשם מאגרי מידע במשרד המשפטים

	כן	לא	לא יודע/מסרב לענות	Total
אחוז מהמדגם	84	13	3	132
מין				
גברים	85	12	4	78
נשים	83	15	2	54
גיל				
18-24	86	6	9	35
25-39	83	17	0	36
40-54	81	19	0	32
+55	86	10	3	29
השכלה				
יסודית או תיכונית ללא בגרות	83	17	0	18
תיכונית עם תעודת בגרות	87	10	3	31
על תיכונית או אקדמאית	81	15	4	75
לא השיב	100	0	0	8
אזור מגורים				
ירושלים	91	9	0	11
מרכז	87	13	0	46
צפון	85	10	5	40
דרום	83	13	4	24
שרון	64	27	9	11
משלח יד				
עצמאי	80	20	0	20
שכיר	85	12	3	67
ללא מקצוע	84	11	4	45







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	Total
אחוז מהמדגם	78	18	4	581
מין				
גברים	77	18	5	283
נשים	79	17	4	298
גיל				
18-24	79	18	3	111
25-39	79	15	6	182
40-54	82	15	3	148
+55	72	24	5	140
השכלה				
יסודית או תיכונית ללא בגרות	70	26	4	135
תיכונית עם תעודת בגרות	83	16	2	136
על תיכונית או אקדמאית	80	16	5	283
לא השיב	77	11	12	28
אזור מגורים				
יחשלים	83	15	2	74
מרכז	74	20	6	163
צפון	79	19	2	180
דרום	75	17	7	109
שרון	87	11	2	56
משלח יד				
עצמאי	77	17	6	86
שכיר	83	16	1	313
ללא מקצוע	71	21	8	182







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	Total
אחוז מהמדגם	45	36	19	581
מין				
גברים	48	36	16	283
נשים	42	35	23	298
גיל				
18-24	49	40	11	111
25-39	46	40	15	182
40-54	48	28	24	148
+55	37	37	26	140
השכלה				
יסודית או תיכונית ללא בגרות	46	39	15	135
תיכונית עם תעודת בגרות	50	35	15	136
על תיכונית או אקדמאית	43	34	23	283
לא השיב	28	47	26	28
אזור מגורים				
יחשלים	47	37	17	74
מרכז	43	35	22	163
צפון	43	40	17	180
דרום	48	32	20	109
שרון	47	33	20	56
משלח יד				
עצמאי	49	31	20	86
שכיר	48	35	17	313
ללא מקצוע	38	40	22	182





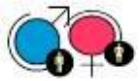


Q25. אקריא לך מספר משפטים הקשורים להגנת מידע אישי, לגבי כל אחד מהם אנא ציין האם למיטב ידיעתך הוא נכון או לא נכון: ישנה הוראה חוקית המאפשרת לך לעיין במידע אודותיך שנמצא בידי אחר

ShiluvMillwardBrown

תפיסות לגבי חוק הגנת הפרטיות – בדיקה נעזרת
נתונים סוציו דמוגרפיים

	נכון	לא נכון	מסרב לענות \ לא יודע	Total
אחוז מהמדגם	77	9	14	581
מין				
גברים	77	11	12	283
נשים	77	8	15	298
גיל				
18-24	85	7	8	111
25-39	80	11	9	182
40-54	75	8	17	148
+55	70	9	21	140
השכלה				
יסודית או תיכונית ללא בגרות	73	9	18	135
תיכונית עם תעודת בגרות	81	11	7	136
על תיכונית או אקדמאית	77	9	14	283
לא השיב	77	5	18	28
אזור מגורים				
יחשלים	82	8	10	74
מרכז	75	11	14	163
צפון	80	12	8	180
דרום	75	5	20	109
שרון	73	6	21	56
משלח יד				
עצמאי	76	14	11	86
שכיר	82	7	12	313
ללא מקצוע	71	11	18	182







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	Total
אחוז מהמדגם	20	72	4	4	581
מין					
גברים	28	66	3	3	283
נשים	12	77	6	5	298
גיל					
18-24	19	77	1	4	111
25-39	24	71	3	2	182
40-54	21	70	3	5	148
+55	14	71	11	5	140
השכלה					
יסודית או תיכונית ללא בגרות	10	76	11	3	135
תיכונית עם תעודת בגרות	17	78	3	3	136
על תיכונית או אקדמאית	25	68	2	5	283
לא השיב	31	60	3	7	28
אזור מגורים					
ירושלים	16	79	1	4	74
מרכז	21	67	7	5	163
צפון	16	75	5	4	180
דרום	25	68	3	3	109
שרון	22	73	2	3	56
משלח יד					
עצמאי	18	76	1	5	86
שכיר	23	70	4	4	313
ללא מקצוע	15	74	8	3	182

Q27. האם לדעתך העברת מידע על ידך באמצעות האינטרנט היא בטוחה יחסית?

ShiluvMillwardBrown

שימוש באינטרנט והגנה על מידע אישי – בדיקה נעזרת בקרב גולשי האינטרנט
נתונים סוציו דמוגרפיים

	כן	לא	לא יודע/מסרב לענות	Total
אחוז מהמדגם	50	45	6	555
מין				
גברים	57	38	5	274
נשים	42	51	6	281
גיל				
18-24	55	40	5	110
25-39	57	39	4	177
40-54	49	47	4	143
+55	36	54	10	125
השכלה				
יסודית או תיכונית ללא בגרות	35	53	12	120
תיכונית עם תעודת בגרות	41	55	4	132
על תיכונית או אקדמאית	61	36	3	276
לא השיב	43	51	5	27
אזור מגורים				
יחשלים	48	47	5	74
מרכז	48	46	6	152
צפון	47	47	7	170
דרום	50	44	6	105
שרון	65	34	2	55
משלח יד				
עצמאי	60	37	3	85
שכיר	52	43	5	302
ללא מקצוע	40	52	8	168







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 אלו שהשתמשו בכלים המגבילים או מונעים, איסוף מידע מהמחשב שלך ,נתונים סוציו דמוגרפיים

	כן	לא	לא עושה שימוש באינטרנט	לא יודע/מסרב לענות	Total
אחוז מהמדגם	55	43	0	1	276
מין					
גברים	65	34	1	0	157
נשים	43	54	0	3	119
גיל					
18-24	68	28	1	2	60
25-39	62	36	0	3	100
40-54	51	49	0	0	70
55+	31	69	0	0	45
השכלה					
יסודית או תיכונית ללא בגרות	45	55	0	0	41
תיכונית עם תעודת בגרות	61	39	0	0	54
על תיכונית או אקדמאית	56	41	1	2	168
לא השיב	62	38	0	0	12
אזור מגורים					
יחשלים	55	45	0	0	35
מרכז	52	44	0	4	73
צפון	47	52	0	1	79
דרום	72	28	0	0	53
שרון	57	41	2	0	35
משלח יד					
עצמאי	54	43	0	3	51
שכיר	58	41	0	1	158
ללא מקצוע	51	46	1	2	67







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

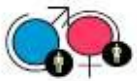
	אני לא יודע איך להתקין את התוכנות הללו על המחשב	לא יודע איך להשתמש בהן	איני משוכנע שהן עובדות	אני לא מוטרד משאלות של פרטיות כאשר אני גולש באינטרנט	הרכיבים יקרים מדי או הפתחן הזה יקר מדי	אחר	לא יודע \ מסרב לענות	Total
אחוז מהמדגם	16	27	10	19	4	15	9	118
מין								
גברים	18	29	9	8	3	23	11	54
נשים	14	25	12	28	6	8	7	64
גיל								
18-24	17	17	6	22	6	23	10	17
25-39	6	29	3	31	10	7	14	36
40-54	23	21	19	11	2	15	9	34
+55	19	36	12	12	0	19	2	31
השכלה								
יסודית או תיכונית ללא בגרות	28	19	4	14	3	23	9	23
תיכונית עם תעודת בגרות	9	30	8	24	5	11	14	21
על תיכונית או אקדמאית	14	29	11	20	5	13	7	69
לא השיב	17	16	34	0	0	16	16	4
אזור מגורים								
יחשלים	5	16	13	45	0	21	0	16
מרכז	7	33	9	22	0	17	11	32
צפון	27	33	6	9	6	7	12	41
דרום	10	24	10	29	13	10	5	15
שרון	22	8	23	0	7	30	10	14
משלח יד								
עצמאי	27	20	7	7	0	24	16	22
שכיר	10	27	10	26	6	13	8	65
ללא מקצוע	20	32	14	13	4	12	6	31

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	Total
אחוז מהמדגם	13	16	17	44	10	555
מין						
גברים	11	19	17	47	6	274
נשים	14	13	16	42	15	281
גיל						
18-24	13	16	18	49	4	110
25-39	12	19	20	39	10	177
40-54	16	15	15	48	7	143
+55	9	14	13	43	20	125
השכלה						
יסודית או תיכונית ללא בגרות	9	15	10	46	20	120
תיכונית עם תעודת בגרות	15	15	17	48	4	132
על תיכונית או אקדמאית	12	17	19	42	9	276
לא השיב	19	19	14	40	8	27
אזור מגורים						
יחשלים	6	13	16	45	20	74
מרכז	10	14	19	44	13	152
צפון	16	10	14	52	7	170
דרום	18	27	20	28	6	105
שרון	7	23	12	50	7	55
משלח יד						
עצמאי	8	18	18	48	8	85
שכיר	16	17	17	41	8	302
ללא מקצוע	8	13	15	47	16	168





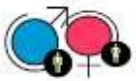


Q31 האם כאשר אתה גולש באינטרנט אתה בודק מהי מדיניות שמירת הפרטיות של האתר/החברה אליה גלשת?

ShiluvMillwardBrown

מתן פרטים אישיים ושמירה על הפרטיות
נתונים סוציו דמוגרפיים

	תמיד	בדרך כלל	לעיתים רחוקות	כלל לא	לא יודע \ מסרב לענות	Total
אחוז מהמדגם	55	22	9	11	3	581
מין						
גברים	50	21	10	16	3	283
נשים	59	23	7	6	4	298
גיל						
18-24	52	23	8	16	1	111
25-39	42	29	12	13	4	182
40-54	68	18	8	5	3	148
+55	60	19	5	10	6	140
השכלה						
יסודית או תיכונית ללא בגרות	59	15	10	12	4	135
תיכונית עם תעודת בגרות	53	19	8	16	3	136
על תיכונית או אקדמאית	54	28	9	7	3	283
לא השיב	44	21	3	22	11	28
אזור מגורים						
יחשלים	67	20	5	5	3	74
מרכז	54	20	11	12	3	163
צפון	59	20	6	11	3	180
דרום	43	30	10	13	4	109
שרון	49	24	10	12	5	56
משלח יד						
עצמאי	52	23	9	12	3	86
שכיר	55	26	9	7	3	313
ללא מקצוע	56	16	8	16	4	182







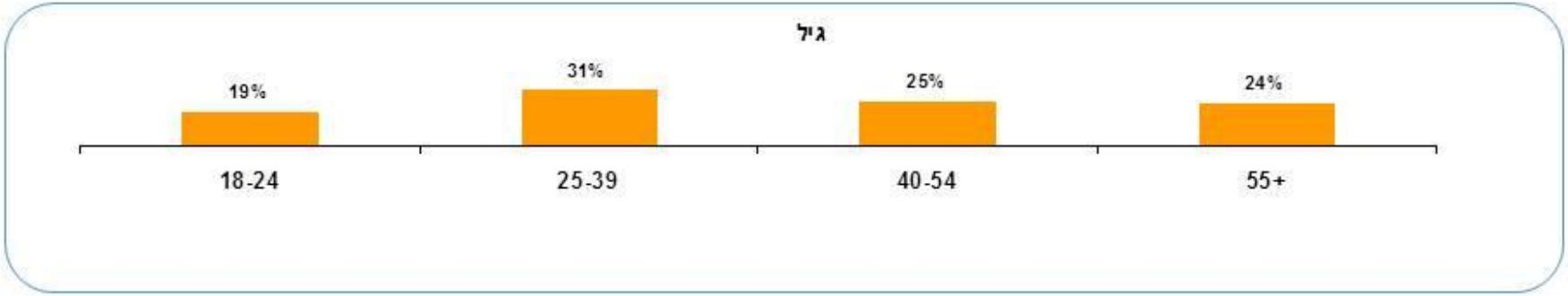
Q32 כאשר אתה מוסר פרטים לגוף כלשהו, האם אתה שואל לשם מה הם נדרשים?

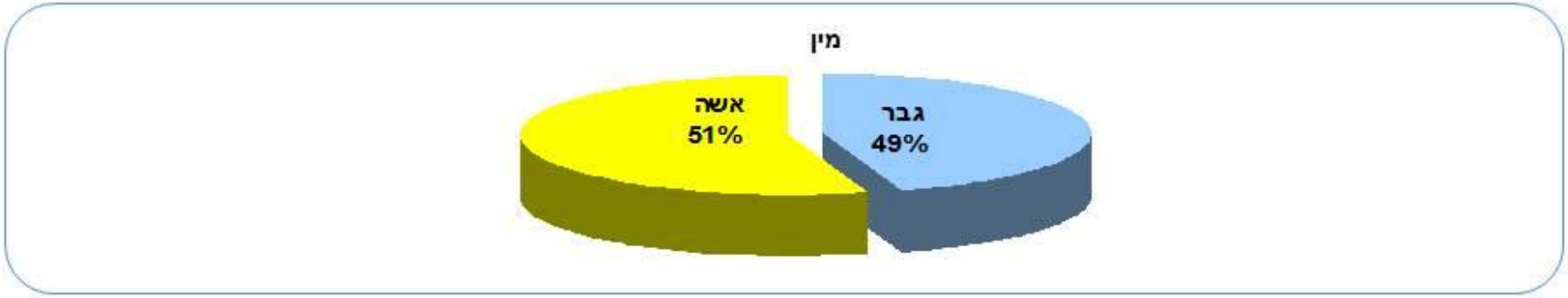
ShiluvMillwardBrown

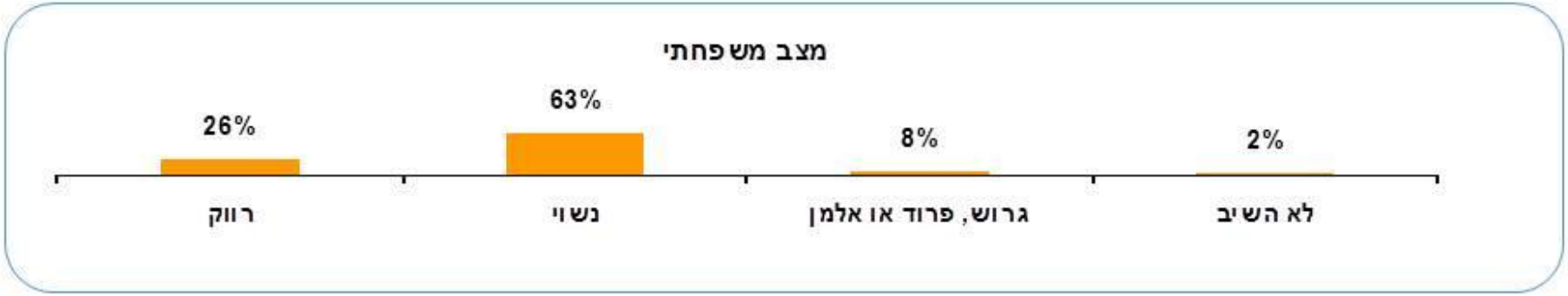


נתונים דמוגרפיים על המדגם

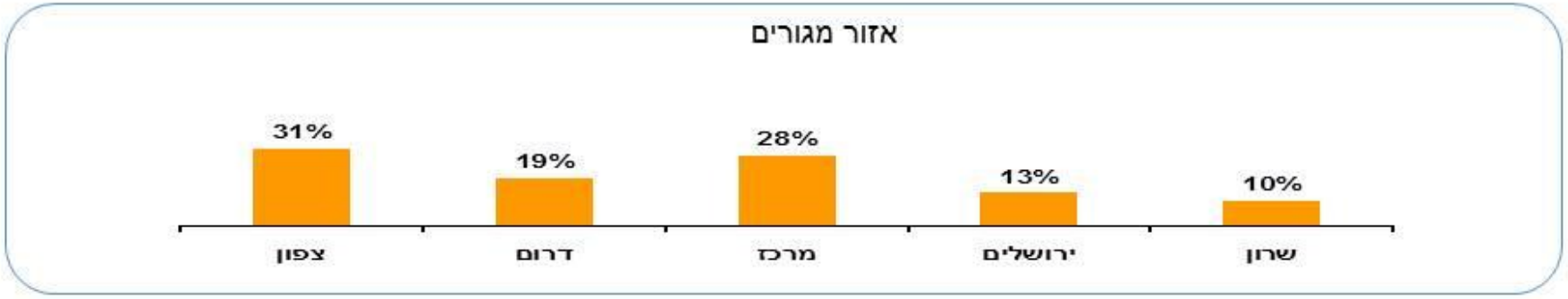
ShiluvMillwardBrown

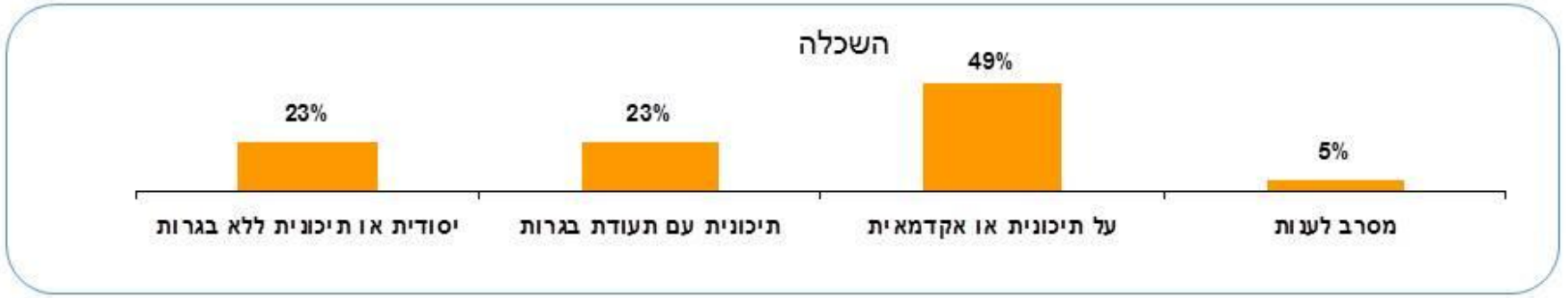


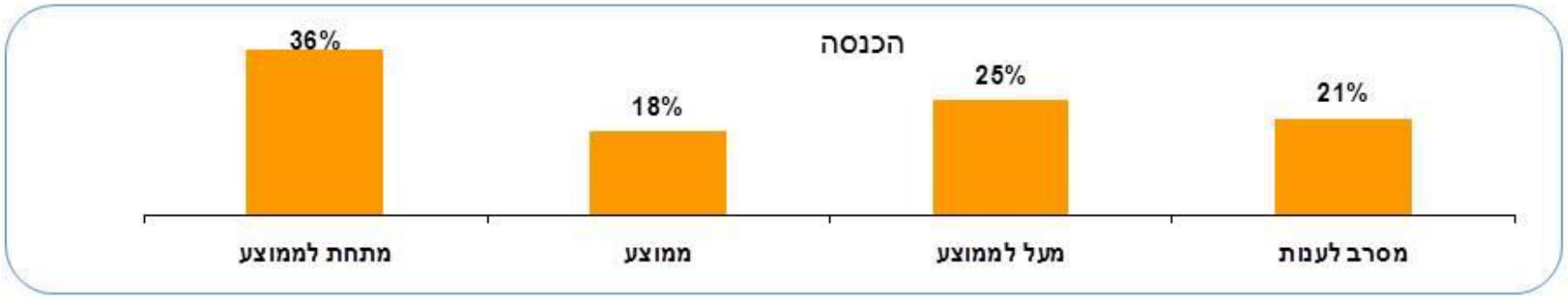




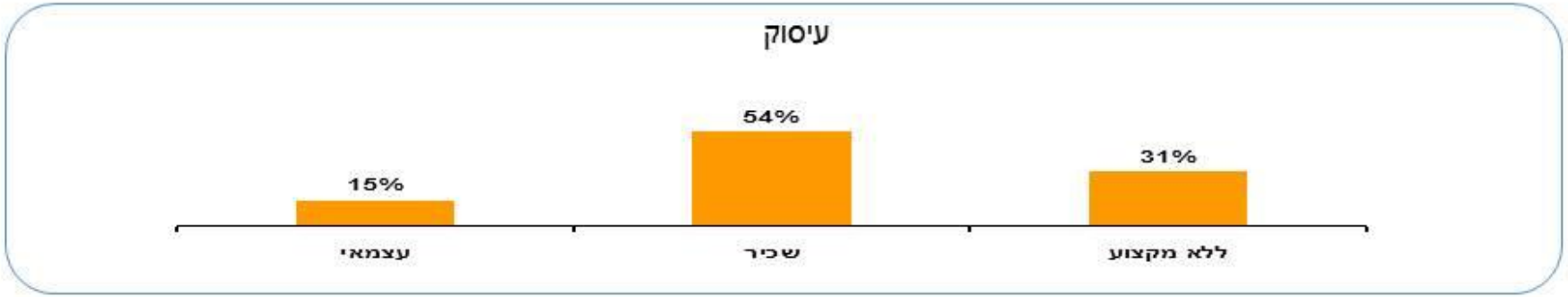
ShiluvMillwardBrown

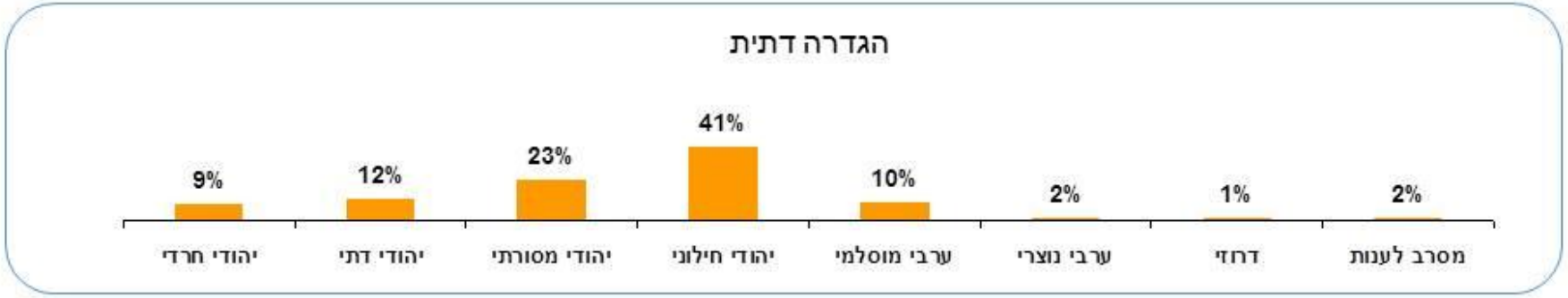






ShiluvMillwardBrown





2) נספח ב' – החלטת הנציבות האירופית על רמת הגנת המידע האישי בישראל

COMMISSION DECISION

of 31 January 2011

pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data

(notified under document C(2011) 332)

(Text with EEA relevance)

(2011/61/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

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, [1] and in particular Article 25(6) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Pursuant to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.

(2) The Commission may find that a third country ensures an adequate level of protection. In that case, personal data may be transferred from the Member States without additional guarantees being necessary.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations and giving particular consideration to a number of elements relevant for the transfer and listed in Article 25 thereof.

(4) Given the different approaches to data protection in third countries, the adequacy assessment should be carried out, and any decision based on Article 25(6) of Directive 95/46/EC should be made and enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail, nor constitute a disguised barrier to trade, regard being had to the European Union's present international commitments.

(5) The State of Israel's legal system has no written constitution but constitutional status has been conferred on certain 'Basic Laws' by the Supreme Court of the State of Israel. Those 'Basic Laws' are complemented by a large body of case law, as the Israeli legal system adheres to a great extent to common law principles. The right to privacy is included in the 'Basic Law: Human Dignity and Liberty' under section 7.

(6) The legal standards for the protection of personal data in the State of Israel are largely based on the standards set out in Directive 95/46/EC and are laid down in the Privacy Protection Act 5741-1981, lastly amended in 2007 in order to establish new processing requirements for personal data and the detailed organization of the supervisory authority.

(7) That data protection legislation is further complemented by governmental decisions on the implementation of the Privacy Protection Act 5741-1981 and on the organisation and functioning of the supervisory authority, largely based upon recommendations formulated in the Report to the Ministry of Justice by the Committee for the Examination of Legislation relating to Databases (Schoffman Report).

(8) Data protection provisions are also contained in a number of legal instruments regulating different sectors, such as financial sector legislation, health regulations and public registries.

(9) The legal data protection standards applicable in the State of Israel cover all the basic principles necessary for an adequate level of protection for natural persons in relation to the processing of personal data in automated databases. Chapter 2 of Privacy Protection Act 5741-1981, which lays down the principles for the processing of personal data, does not apply to the processing of personal data in non-automated databases (manual databases).

(10) The application of the legal data protection standards is guaranteed by administrative and judicial remedies and by independent supervision carried out by the supervisory authority, the Israeli Law, Information and Technology Authority (ILITA), which is invested with powers of investigation and intervention, and which acts completely independently.

[1] OJ L 281, 23.11.1995, p. 31.

(b) where there is a substantial likelihood that the standards of protection are being infringed, there are reasonable grounds for believing that the competent Israeli authority is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the party responsible for processing established in the State of Israel with notice and an opportunity to respond.

2. The suspension shall cease as soon as the standards of protection are assured and the competent authority of the Member States concerned is notified thereof.

Article 4

1. Member States shall inform the Commission without delay when measures are adopted on the basis of Article 3.

2. The Member States and the Commission shall inform each other of cases where the action of bodies responsible for ensuring compliance with the standards of protection in the State of Israel fails to secure such compliance.

3. If the information collected under Article 3 and under paragraphs 1 and 2 of this Article provides evidence that any body responsible for ensuring compliance with the standards of protection in the State of Israel is not effectively fulfilling its role, the Commission shall inform the competent Israeli authority and, if necessary, present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC with a view to repealing or suspending this Decision or limiting its scope.

Article 5

The Commission shall monitor the functioning of this Decision and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the finding in Article 1 of this Decision, that protection in the State of Israel is adequate within the meaning of Article 25 of Directive 95/46/EC and any evidence that this Decision is being implemented in a discriminatory way. In particular, it shall monitor the processing of personal data in manual databases.

Article 6

Member States shall take all the measures necessary to comply with the Decision within three months of the date of its notification.

Article 7

This Decision is addressed to the Member States.

Done at Brussels, 31 January 2011.

For the Commission
Viviane REDING
Vice-President

(11) Israeli data protection authorities have provided explanations and assurances as to how the Israeli law is to be interpreted, and have given assurances that the Israeli data protection legislation is implemented in accordance with such interpretation. This Decision takes account of these explanations and assurances, and is therefore conditional upon them.

(12) The State of Israel should therefore be regarded as providing an adequate level of protection for personal data as referred to in Directive 95/46/EC with regard to automated international transfers of personal data from the European Union to the State of Israel or, where those transfers are not automated, they are subject to further automated processing in the State of Israel. Conversely, international transfers of personal data from the EU to the State of Israel whereby the transfer itself as well as the subsequent data processing is carried out exclusively through non-automated means should not be covered by this Decision.

(13) In the interest of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify the exceptional circumstances in which the suspension of specific data flows may be justified, notwithstanding the finding of adequate protection.

(14) The adequacy findings pertaining to this Decision refer to the State of Israel, as defined in accordance with international law. Further onward transfers to a recipient outside the State of Israel, as defined in accordance with international law, should be considered as transfers of personal data to a third country.

(15) The Working Party on the protection of individuals with regard to the processing of personal data established under Article 29 of Directive 95/46/EC has delivered a favourable opinion on the level of adequacy as regards protection of personal data in relation to automated international transfers of personal data from the European Union or, whether they are non-automated they are subject to further automated processing in the State of Israel. In its favourable opinion, the Working Party has encouraged the Israeli authorities to adopt further provisions which extend the application of Israeli legislation to manual databases, which expressly recognise the application of the proportionality principle to personal data processing in the private sector and which interpret the exemptions in international data transfers as in accordance with the criteria set out in its 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC' [1]. This opinion has been taken into account in the preparation of this Decision [2].

(16) The Committee established under Article 31(1) of Directive 95/46/EC did not deliver an opinion within the time limit laid down by its Chairman,

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, the State of Israel is considered as providing an adequate level of protection for personal data transferred from the European Union in relation to automated international transfers of personal data from the European Union or, where they are not automated, they are subject to further automated processing in the State of Israel.

2. The competent supervisory authority of the State of Israel for the application of the legal data protection standards in the State of Israel is the 'Israeli Law, Information and Technology Authority (ILITA)', referred to in the Annex to this Decision.

Article 2

1. This Decision concerns only the adequacy of protection provided in the State of Israel, as defined in accordance with international law, with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States.

2. This Decision shall be applied in accordance with international law. It is without prejudice to the status of the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem, under the terms of international law.

Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to a recipient in the State of Israel in order to protect individuals with regard to the processing of their personal data in the following cases:

(a) where a competent Israeli authority has determined that the recipient is in breach of the applicable standards of protection; or

[1] Document WP114 of 25 November 2005. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

[2] Opinion 6/2009/EC on the level of protection of personal data in Israel. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp165_en.pdf

ANNEX

Competent supervisory authority referred to in Article 1(2) of this Decision:

The Israeli Law, Information and Technology Authority
The Government Campus
9th floor
125 Begin Rd
Tel Aviv
Israel
Mailing address:
PO Box 7360
Tel Aviv, 61072
Tel. + 972-3-7634050
Fax + 972-2-6467064
E-mail: ILITA@justice.gov.il
Website: http://www.justice.gov.il/MOJEng/RashutTech/default.htm

נספחים לפרק 8 – דו"ח רשם גורמים מאשרים

1) נספח א' – הנחיית רשם גורמים מאשרים 1-2010

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע
רשם גורמים מאשרים

מדינת ישראל
State of Israel

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

הנחית רשם גורמים מאשרים מס׳ 1/2010
דרישות חלופיות לת״י 1495 להפעלת אמצעי חתימה אלקטרונית

1. **כללי**

1.1. אמצעי חתימה, המשמש לחתימה אלקטרונית[15] לפי חוק חתימה אלקטרונית, התשס״א-2001 (להלן - **החוק**), מצוי בדרך כלל על גבי התקן קריפטוגרפי, שמטרתו שמירה על השליטה הבלעדית של החותם באמצעי זה, בדומה לשליטתו בחתימה שלו.

1.2. בתקנה 8(ג) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס״ב- 2001 נקבע כי:

״היתה הפעלת אמצעי החתימה כרוכה בשימוש בסיסמה, תעמוד הסיסמה בדרישות אבטחה ברמה גבוהה לפי ת״י 1495 חלק 3, או בדרישות חלופיות שקבע הרשם, אם נוכח כי ניתן לפטור מהדרישה האמורה״.

1.3. מטרת הדרישה לוודא כי הפעלת אמצעי החתימה והגישה אליו תיעשה רק בידי מי שיש לו ההרשאה לשימוש באמצעי החתימה.

1.4. כאשר מדובר על סיסמת גישה לכרטיס חכם או לאמצעי פיזי אחר, דרישות האבטחה לפי ת״י 1495 חלק 3 ברמה הגבוהה עשויות להיות חמורות מדי, ואף לא רלבנטיות, בין השאר משום שהן מתעלמות מכך שהמידע מוגן **על גבי אמצעי פיזי המצוי בשליטת בעליו**, ולא במערכת מידע רגילה. התוצאה של דרישות חמורות מדי עלולה לפגוע ברמת האבטחה, משום שמשתמשים עלולים לציין לצד האמצעי את ססמת הגישה, או שעלולה להיגרם פגיעה אחרת בשימושיות.

2. **רקע**

2.1. באופן כללי, סיסמאות מורכבות הנאכפות ברמה מערכתית מהוות כלי אפקטיבי למניעת שימוש לא מורשה והתקפות על מידע.

[15] בהתייחסות ל- "אמצעי חתימה" החוק מכוון למה שמכונה בתשתית מפתח ציבורי "מפתח פרטי", כלומר הסוד השמור על גבי ההתקן הפיזי המשמש לחתימה.

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

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

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

2.2. קיימים ארבעה פרמטרים מקובלים אשר משפיעים על יעילות הסיסמה:

2.2.1. אורך הסיסמה (**Length**) - משפיע בצורה ישירה על היכולת של פורץ ללא מידע מוקדם, לפצח את הסיסמה;

2.2.2. מורכבות הסיסמה (**Complexity**) - כגון: שימוש באותיות קטנות או גדולות (באנגלית), או שימוש בסימנים ומספרים בנוסף לאותיות - עשויה להקשות על פריצתה;

2.2.3. הגדרת נעילת הגישה אחרי מספר מוגדר של ניסיונות גישה (**Lock-out**) - כיום קיימים כלים המאפשרים לנחש סיסמאות תוך פרק זמן קצר. לכן, נעילת הגישה הופכת סיסמאות לבטוחות יותר. שימוש בנעילת גישה גם עשויה לפצות במידת מה על מדיניות סיסמאות חלשה;

2.2.4. תפוגת סיסמה (**Retention**) - רצוי להחליף סיסמאות בתדירות גבוהה. תדירות ההחלפה צריכה להיקבע תוך התייחסות ליכולת של משתמשים לזכור את הסיסמאות. תדירות ההחלפה צריכה לכלול מנגנון האוסר על שימוש בסיסמאות קודמות או רצף הגיוני של סיסמאות (סיסמה1,סיסמה2 וכו').

2.3. ככלל, שימוש בסיסמאות חזקות ומורכבות אשר אינן ניתנות לפיצוח בזמן סביר, מחזק בצורה משמעותית את ההגנה על המידע. אולם, יש לתת את הדעת לסיכונים הנובעים מכך שסיסמאות חזקות ומורכבות מדי עלולות להביא לרישום גלוי של הסיסמא לצד ההתקן או תקלות אבטחה אחרות, ובנוסף לפגוע בשימושיות של אמצעי החתימה. בהתאם לכך, יש למצוא איזון בין מורכבות וחוזק הסיסמה בפרמטרים אלה מפני תקיפה, למול היבטי שימושיות.

2.4. <u>הוראות מקבילות בעניין גישה לאמצעי חתימה</u>

2.4.1. תקן FIPS 140-2 של מכון התקנים האמריקני (NIST) מגדיר דרישות אבטחה ממודול קריפטולוגיה, מהסוג המשמש גם לאפסון מפתחות פרטיים המשמשים לחתימה אלקטרונית[16].

2.4.2. ביחס לאורך הסיסמה[17], קובע מכון התקנים האמריקני, כי יש להקטין את הסיכוי לפריצת הסיסמה או ניחוש רנדומאלי לפחות מניסיון אחד מוצלח למיליון ניסיונות (1-1,000,000), וכן שאם נעשה מספר רב של ניסיונות

---

[16] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[17] שם, בעמ' 18:

The strength of the authentication mechanism shall conform to the following specifications:

- For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods).
- For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur .
- Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password) .
- Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.

להזדהות בפרק זמן של דקה, הסיכוי להצליח באקראי או בשל טעות של המנגנון (False acceptance) לא יעלה על 1 ל - 100,000 ניסיונות.

2.4.3. במסגרת פרויקט התקינה בתחום החתימה האלקטרונית באירופה (EESSI)[18], נכתב תקן CWA-14890-1 (2004)[19]. בהתאם לתקן זה, נדרש אורך סיסמה מינימאלי של 6 תווים ומנגנון נעילה המופעל לאחר 3 ניסיונות. כמו כן, נקבע בתקן כי איפוס סיסמה יעשה באמצעות סיסמת ADMIN באורך של 6 תווים לפחות.

3. הנחיה

3.1. על רקע האמור לעיל, הנחיית הרשם לעניין הדרישות החלופיות לת"י 1495 על פי תקנה 8(ג) הינה:

3.1.1. **אורך סיסמה** - סיסמת הגישה לאמצעי חתימה תהיה באורך של 6 תווים לפחות;

3.1.2. **נעילת סיסמה** - האפשרות להקיש סיסמה תיחסם לאחר 7 ניסיונות כושלים;

3.1.3. **שחרור מנעילה** - ניתן יהיה ליישם שחרור מנעילה באמצעות בדרך של איפוס הסיסמה באחת החלופות הבאות:

3.1.3.1. על ידי סיסמת שחרור [PUK] שתעמוד בדרישות הבאות לפחות:

3.1.3.1.1. הסיסמה ייעודית לאמצעי חתימה זה;

3.1.3.1.2. היא תיוצר או תוגדר במעמד הנפקת אמצעי החתימה ותועבר בצורה שתשמור על סודיותה לבעל אמצעי החתימה;

3.1.3.1.3. הסיסמה לא תהיה בשום מקרה סיסמת ברירת מחדל של ההתקן;

3.1.3.1.4. הסיסמה תהיה באורך 8 תווים לפחות.

3.1.3.2. על ידי מנגנון ייעודי אחר שיאשר הרשם, המבוסס על זיהוי המבקש ותוך מניעת אפשרות גישה לאמצעי החתימה שלו בהליך זה;

3.2. לעניין **מורכבות סיסמה**, מומלץ לבחון יישום דרישות אלה ביחס להתקן:

3.2.1. לאפשר הרכבת הסיסמה משילוב תווים מתוך שתים מקרב הקבוצות הבאות: אותיות גדולות (Capital Letters) באלף בית הלטיני, אותיות קטנות באלף בית הלטיני, סימנים מיוחדים (למשל %) וספרות;

3.2.2. לאפשר שימוש בסיסמאות ארוכות המאפשרות רישום פראזות-משפטים.

---

[18] http://www.ictsb.org/Working_Groups/EESSI/Index.htm.

[19] ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf.

מידע לגבי ההנחיה

1. **מס' ההנחיה:** 1/2010
2. **נושא ההנחיה:** דרישות חלופיות לת"י 1495 להפעלת אמצעי חתימה אלקטרונית
3. **תאריך פרסום:** 9.3.2010
4. **בתוקף מתאריך:** 9.3.2010
5. **חוקים שאוזכרו**:
   א. חוק חתימה אלקטרונית, התשס"ב-2002.
6. **חקיקת משנה שאוזכרה**:
   א. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב- 2001.
7. **פסקי דין שאוזכרו**: אין.
8. **מאמרים שאוזכרו**: אין.
9. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.
10. **הנחיות רשם גורמים מאשרים שאוזכרו**: אין.
11. **מילות מפתח:** Complexity ; CWA-14890-1 ; EESSI ; False Acceptance ; FIPS 140-2 ; Length ; Lock-out ; NIST ; Retention ; אורך סיסמה ; אמצעי חתימה ; התקן קריפטוגרפי ; חתימה אלקטרונית ; מורכבות סיסמה ; נעילת סיסמה ; סיסמה ; ת"י 1495 ; תפוגת סיסמה.
12. **עדכונים**

גרסה	פרטים	ת ריך

2) נספח ב' – הנחיית רשם גורמים מאשרים 2-2010

הנחית רשם גורמים מאשרים מס' 2-2010

תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר

מטרת הנחיה זו היא לקבוע הוראות לעניין תקן מקובל לצורך עמידה בהוראות חוק חתימה אלקטרונית, התשס"א-2001 (להלן - **החוק**) והתקנות מכוחו, לעניין סטנדרט אבטחת המידע והמהימנות הנדרשים ממערכת המשמשת לפעולות חיוניות בגורם מאשר והתקנתה, ולעניין אופן בדיקת העמידה בתקן.

4. **רקע**

1.5. הדרישות לעניין מערכת ניהול תעודות בגורם מאשר קבועות בסעיף 18(ד) לחוק, ולפיהן לצורך ביצוע תפקידי הגורם המאשר המנויים בסעיף 18, ישתמש הגורם המאשר "רק במערכות חומרה ותוכנה מהימנות".

1.6. סעיף 24(9) לחוק מסמיך את שר המשפטים לקבוע הוראות לעניין סוגי מערכות המקיימות, בין היתר, את דרישות סעיף 18 לחוק.

1.7. תקנה 4 לתקנות (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן - **התקנות**) קובעת לעניין אמצעי החתימה של הגורם המאשר, כי עליו להיות "מגובה באמצעים מוגנים ומאובטחים, להנחת דעתו של הרשם", וכן כי עליו לעמוד ב"דרישות נוספות שהעמיד הרשם לשם קיום אבטחה ברמה סבירה מפני חדירה, שיבוש או שימוש לרעה".

1.8. בתקנה 5(א) לתקנות נקבע, כי "מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה יעמדו ברמת ביטחון של תקן Common Criteria EAL4 או לפי תקן מקובל אחר, המבטיח רמת אבטחה מקבילה, להנחת דעתו של הרשם". לפי תקנה 1 לתקנות, מערכת היא "מערכת החומרה והתוכנה של הגורם המאשר המשמשת לפעילותו כגורם מאשר".

1.9. בתקנה 2(8) לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001, נקבעה דרישה לעריכת חוות דעת של מבקר לפי כללי ביקורת מקובלים להנחת דעת הרשם, ולפי תקנה 4(4) לתקנות אלה על גורם מאשר להגיש חוות דעת כאמור אחת לשנה.

1.10. מכאן שהתקנות מקנות שיקול דעת לרשם להרחיב את בסיס התקינה הקבוע בתקנות ולקבוע את אופן מימושו.

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

1.11. החוק והתקנות לפיו מיישמים עקרונות דומים להוראות הדירקטיבה האירופית בנושא חתימה אלקטרונית משנת 1999[20] (להלן - **הדירקטיבה**), הן בעקרונות המהותיים, והן בשיטת ההפניה לתקינה טכנולוגית. בשל כך נבחנו הוראות התקינה החלות על מערכות לניהול גורם מאשר באירופה.

1.12. לצורך מימוש הוראות הדירקטיבה, תואם באמצעות ICT Standards Board (ICTSB), שהוא מיזם של שלושת מכוני התקינה המוכרים האירופאים[21], פרויקט European Electronic Signature Standardization Initiative[22].

1.13. ה-European ICT Standards Board, בתמיכת נציבות האיחוד האירופי, שיתף בעבודת התקינה גורמים ממשלתיים פרטים ומסחריים בעלי ידע בנושא זה. במסגרת זו הוסמכו "ועדת התקינה האירופאית" [CEN - "European Committee for Standardization"], ומכון תקינת הטלקומוניקציה האירופאי ["European Telecommunications Standards Institute"], לבצע את העבודה ולפתח את התקנים המקובלים. לצורך עריכת תקנים אלה נערכו "הסכמי תקינה" ["CEN Workshop Agreements (CWA)"], שמטרתם לקדם סטנדרטים אלה. קבוצת העבודה העבירה את תחזוקת התקנים והמשך עבודת התקינה בפרויקט זה ל - CEN ו- ETSI.

1.14. ועדת התקינה האירופית[23] פרסמה את תקן CWA 14167-1[24] (להלן - **התקן** או **תקן CWA 14167-1**) ואת תקן CWA 14172-3[25] (להלן - **תקן העזר**).

1.10.1 התקן מחלק את המערכת למספר חלקים חיוניים שיש לבחון את תפקודם באופן מנדטורי:

1. שירותי רישום נתונים של מבקש תעודה;
2. שירותי ייצור וחתימה על תעודה בהתאם לנתונים שנרשמו;
3. שירותי הפצת תעודה לבעל התעודה ולצדדים מסתמכים;
4. שירותי ביטול תעודה;
5. שירותי מסירת מידע על ביטול תעודה.

1.10.2 בנוסף, כולל התקן שני פרקים וולונטריים החלים לעניין שירותים נוספים שגורם מאשר יכול לספק, וקובע הוראות ביחס אליהם - שירותי אתחול

---

[20] Directive 1999/93/EC of the European Parliament and of the Council of 13 September 1999, on a Community framework for electronic signatures. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en

[21] ראה: http://www.ictsb.org

[22] ראה באופן כללי על הדירקטיבה ועבודות ועדת התקינה למימושה: http://www.ictsb.org/Working_Groups/EESSI/Index.htm

[23] European Committee for Standardization. כתובת אתר האינטרנט: www.cen.eu.

[24] CEN Workshop Agreement, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, June 2003.

[25] CEN Workshop Agreement, EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures, March 2004.

והפעלה של התקן המשמש לאמצעי חתימה של משתמש קצה, ושירותי Time-stamp.

1.10.3 התקן נקבע כמסמך בעל תוקף מנחה, בהתאם להוראות סעיף 3(5) לדירקטיבה[26] ורשמים מקבילים מאירופה רואים בו מקור מקצועי לעניין הסטנדרט הנדרש ממערכת המנהלת את התעודות, לענין התקנתה בגורם מאשר.

1.10.4 תקן העזר קובע את הדרישות מגורם שמבצע בדיקות אבטחה לפי התקן. דרישות אלה כוללות הוראות בעניין דרישות מקצועיות, אי תלות והתנהלות אתית[27]. בנוסף, קובע תקן העזר את השיטה לפיה המבקר צריך לפעול, תוך הסתמכות על מידע נתונים ומסמכים אודות הרכיבים הרלוונטיים, ואופן תיעוד הבדיקות לצורך בקרה על ידי צדדים שלישים, ובכלל זה הרשם.

1.15. התקן ותקן העזר לבדיקתו מהווים סטנדרט ברור ליישום מעטפת האבטחה בארגון המסוים בו מוטמעת המערכת. התקן מבהיר לגורם המאשר את אופן העמידה בהוראות החוק, תוך הותרת גמישות תפעולית לגורם המאשר.

1.16. ככלי רגולטורי התקן והכללים הקבועים בתקן העזר מאפשרים הרחבת היצע המערכות שניתן להשתמש בהן לגורם מאשר מבלי לפגוע ברמת האבטחה של המערכת. התקן מאפשר למקד את פיקוח הרשם בהיבטים המהותיים של המערכת. על רקע האמור יש צורך בהרחבת בסיס התקינה בהתאם לדגם האירופאי.

5. הנחייה זו פורסמה כטיוטה להערות הציבור ביום 22.02.2010, הועברה לגורם המאשר ולגורמים נוספים, ולא התקבלו ביחס אליה כל הערות.

6. **הנחיה**

6.1. בהתאם לאמור לעיל, הנחיית רשם גורמים מאשרים הינה כדלקמן:

6.1.1. תקן CWA 14167-1 יחול לצורך הוכחת עמידת גורם מאשר בדרישות החוק והתקנות לפיו, ולעניין סטנדרט אבטחת המידע והמהימנות הנדרשים לניהולה ולהפעלתה של מערכת המשמשת לפעולות חיוניות בגורם מאשר, בהתאם לתקנות 4 ו-5.

6.1.2. תקן העזר יחול לעניין אופן הוכחת עמידה בתקן, בין היתר בשים לב לתקנה 2(8) לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001, ועל פי הוראותיה. על עורך חוות הדעת לפי התקן לפרט, בהתאם לתקן

---

[26] ראה: Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognized standard for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (notified under document number C(2003) 2439).

להשלמה יצוין, כי באותה החלטה נקבע גם תקן CWA 14167-2, המסדיר את פרופיל ההגנה (protection profile), של הסטנדרט שנקבע במסמך זה הוא פרופיל הגנה לפי תקן common criteria. עם זאת תקן זה עבר שינויים ולאחר מכן שונה לשני תקנים נפרדים: CWA 14167-2 ו- CWA 14167-4.

[27] ראה שם, סעיף 3.5, עמ' 11-12.

העזר, נתונים מזהים אודות המערכת ורכיביה, הבדיקות שבוצעו על ידו ונתונים נוספים ככל שנדרש לצורך הבנה והערכה של חוות הדעת.

6.2. יישום התקן בישראל ייעשה בשינויים המחויבים הנובעים מהוראות דין מקומיות, ובמרכזן הוראות החוק, התקנות מכוחו, תקנים ישראלים, הוראות אחרות של הרשם והוראות מקבילות הרלבנטיות למימוש החתימה האלקטרונית בדברי חקיקה מקבילים. רשימה של הסתייגויות מופיעה בנספח להנחיה זו.

6.3. לצורך הוכחת עמידה בתקן על הבודק או צוות הבדיקה לעמוד בהוראות תקן העזר, בדגשים הבאים:

6.3.1. ניסיון מעשי בתחום ה- PKI להנחת דעת הרשם.

6.3.2. התחייבות להעדר ניגוד עניינים, עבודה על פי כללי ביקורת מקובלים, ויישום הנחיות התקן.

6.4. מאחר שהבדיקה היא פונקציונאלית, מקום בו נבחנו רכיבים של המערכת לפי תקן Common Criteria, ניתן יהיה להסתפק בבדיקה מפורטת פחות, לעניין בחינת היבטים תפעוליים של רכיבים אלה, תוך וידוא כי נעשה שימוש ברכיבים בהתאם לדרישות והתנאים המקדמים המוגדרים בתקינה.

6.5. במקום שבו מדובר ברכיבים או חלקים פונקציונאליים שפותחו באופן עצמאי על ידי הגורם המאשר או מטעמו או באינטגרציה של רכיבים מוכרים יש צורך בבדיקה טכנית מעמיקה יותר, בהיקף הנגזר מהחשיבות הפונקציונאלית, ותוך תיעוד מפורט של הממשקים בין הרכיבים בגורם המאשר.

6.6. למען הסר ספק, זהות הבודק ואופן עמידתו בהוראות אלה, יובאו לאישור הרשם מראש.

6.7. הנחייה זו תכנס לתוקף עם פרסומה הסופי לאחר הערות. לעניין הגורם המאשר הרשום במועד פרסום הנחייה זו, הנחייה זו תכנס לתוקף תוך 45 יום.

נספח - סייגים לתחולת התקן

1. הסימוכין הנורמטיביים שבסעיף 2.1 לתקן CWA 14167-1, לא יחולו בישראל.
2. מבלי לגרוע מהאמור, להלן סייגים ספציפיים לתחולת התקן:

סעיף בתקן	נושא	במקום	סייג/תחולה חליפית
5.1.5.2 [KM1.2]	דרישות אבטחה מהמודול הקריפטוגרפי	הפנייה ל- [CEN CMCSO-pp]	הפנייה לתקנה 4(2) לתקנות
5.1.5.2 [KM1.7] [KM2.6] [KM6.2]	הוראות בנושא אלגוריתמים	הפנייה ל- "מסמך ALGO"[28]	לפי הנחית הרשם 4-2010 בנושא אלגוריתמים
5.1.5.2 [KM3.4]	מגבלות על שימוש במפתחות ומבנה תעודה	האמור בסעיף	על פי האמור בתקינה ישראלית, ולא יחול על תעודות המונפקות לפי חוק ניירות ערך, התשכ"ח-1968
5.1.8 [BK2.2]	הצפנה של מידע קריטי	הפנייה ל- "מסמך ALGO"	שימוש בתקן מקובל
5.2.2 [R 1.3]	איסוף מידע הנדרש בדירקטיבה האירופית להנפקת תעודה	הפנייה לדירקטיקבה האירופית	בהתאם לדין הישראלי [החוק, תקנות והוראות דין ספיציפיות כגון חוק ניירות ערך, התשכ"ח-1968].
5.2.3.2 [CG1.6], 1	תוכן שדה "שם" בתעודה	"or pseudonym"	ימחק
5.2.3.2 [CG1.6], 6	הוראות בעניין אלגוריתמים לחתימה	הפנייה ל- "מסמך ALGO"	לפי הנחיית הרשם 4-2010 בנושא אלגוריתמים
5.2.3.2 [CG1.6]	מבנה תעודה	האמור בסעיף	לפי תקן ישראלי
5.2.5.2	עדכון רשימת תעודות בטלות	האמור בסעיף	לפי תקנה 15 והנחיות הרשם לפיה או לפי הוראות או הנחיות לפי חוק ניירות ערך, התשכ"ח-1968 (במידת הרלבנטיות) או לפי הוראות לפי דין אחרות
5.2.6.2	הוראות בנושא אלגוריתמים	הפנייה ל- "מסמך ALGO"	לפי הנחייה 4-2010 בנושא אלגוריתמים

[28] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

מידע לגבי ההנחיה

13. **מס' ההנחיה:** 2/2010
14. **נושא ההנחיה:** תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר
15. **תאריך פרסום:** 12.10.2010
16. **בתוקף מתאריך:** 24.11.2010
17. **חוקים שאוזכרו:**
    א. חוק חתימה אלקטרונית, התשס"ב-2002.
18. **חקיקת משנה שאוזכרה:**
    א. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב- 2001.
    ב. תקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001.
19. **פסקי דין שאוזכרו:** אין.
20. **מאמרים שאוזכרו:** אין.
21. **הנחיות היועץ המשפטי לממשלה שאוזכרו:** אין.
22. **הנחיות רשם גורמים מאשרים שאוזכרו:** 2010-4.
23. **מילות מפתח:** EAL4 common criteria, CWA 14167-1, CWA 14172-3 , אבטחת מידע, אמצעי חתימה, גורם מאשר, גיבוי, הנפקת תעודה אלקטרונית, זיהוי, חתימה אלקטרונית, מבקר מערכות, מהימנות, מערכת ניהול תעודות, תקן.
24. **עדכונים**

גרסה	פרטים	תאריך

3) נספח ג' – הנחית רשם גורמים מאשרים 4/2010

הנחית רשם גורמים מאשרים מס' 4/2010
עדכון אלגוריתמים ואורכי מפתחות לשימוש לפי חוק חתימה אלקטרונית, התשס"א-2001

7. כללי

1.17. חוק חתימה אלקטרונית, התשס"א-2001 (להלן - **החוק**) מגדיר מהי "חתימה" בעולם האלקטרוני ומסדיר את התוצאות המשפטיות של השימוש בה. בתקנות לפי החוק נקבעו הוראות מפורטות יותר.

1.18. המימוש המקובל כיום של חתימה אלקטרונית, הינו על בסיס "הצפנה אסימטרית", הידועה גם בשם הצפנת מפתח ציבורי.

1.19. חוזק החתימה תלוי בחוזק ההצפנה, ובהתאם לכך נקבעו הוראות לפי החוק בנושא זה.

1.20. במסגרת הצורך לבדוק מעת לעת את תנאי הסף הנדרשים להצפנה זו, על מנת למנוע זיוף או שבירת חתימה, רשם גורמים מאשרים ביקש את חוות דעתו של ד"ר בני פנקס, מומחה ישראלי להצפנה (להלן - **חוות הדעת**), בהתבסס על תקנים מקובלים.

1.21. חוות הדעת הצביעה על הצורך בקביעת פרמטרים לפונקציות הצפנה, לפונקציות גיבוב, ולשיטות ריפוד של החתימה, הכל כפי שפורט בחוות הדעת. חוות הדעת פורסמה להערות הציבור, ונערך דיון בנושא זה במשרד המשפטים בספטמבר 2009.

1.22. בעקבות הערות הציבור שהתקבלו לגבי חוות הדעת, הדיון בנושא שנערך במשרדי הרשות למשפט טכנולוגיה ומידע, וכן עדכונים נוספים בתחום זה, גובש הנוסח הסופי לחוות הדעת המצורף כנספח להנחיה 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

8. **הנחיה**

בהתאם לנוסח הסופי של חוות הדעת, הנחיית הרשם לעניין עדכון אלגוריתמים ואורכי מפתחות לשימוש לפי החוק הינה כמפורט להלן:

8.1. שיטות גיבוב (HASH)

תוקף	אורך פלט	שיטה
עד 1.4.2011	160	SHA-1
עד סוף שנת 2012	160	RIPEMD-160
עד סוף שנת 2012	160	SHA-224 עם פלט מקוצר ל-160 סיביות
ללא הגבלה	224	SHA-224
ללא הגבלה	256	SHA-256
ללא הגבלה	384	SHA-384
ללא הגבלה	512	SHA-512
ללא הגבלה	512	Whirlpool

8.2. שיטות ריפוד (Padding) מקובלות

מקור	שיטה
FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)	RSASSA-PKCS1-v1.5
FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)	RSASSA-PSS

8.3. שיטות חתימה ואורכי מפתחות

תוקף	אורך מפתחות	שיטה
עד 1.4.2011 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016	1024	RSA
ללא הגבלה	2048 סיביות או יותר	RSA
יש להתכונן למעבר לאורכי מפתחות אלו	4096 סיביות או יותר	RSA
עד 1.4.2011 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016	(L=1024,N=160)	DSA
ללא הגבלה	(L=2048,N=224) (L=2048,N=256) (L=3072,N=256).	DSA
עד 1.4.2011 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016	160	ECDSA מעל $E(F_p)$
ללא הגבלה	224 או יותר	ECDSA מעל $E(F_{2^m})$

נספח
בחינת אלגוריתמים לפי חוק חתימה אלקטרונית

ד"ר בני פנקס
חבר סגל, המחלקה למדעי המחשב, אוניברסיטת חיפה

תל אביב, יוני 2010

נתבקשתי על ידי רשם גורמים מאשרים במשרד המשפטים, לחוות דעתי המקצועית בשאלות המקצועיות המפורטות מטה. אני מצהיר בזאת כי ידוע לי היטב, שלעניין הוראות החוק הפלילי בדבר עדות שקר בשבועה בבית המשפט, דין חוות דעתי זו כשהיא חתומה על ידי כדין עדות בשבועה שנתתי בבית המשפט. אין לי עניין אישי כלשהו בהמלצות הנדונות בחוות הדעת, פרט לכך שאני חוקר בתחום ההצפנה.
ואלה פרטי השכלתי:

- דוקטורט (PhD) במדעי המחשב, מכון וייצמן, שנת 2000.
- תואר שני (MSc) במדעי המחשב, הטכניון, שנת 1991.
- תואר ראשון (BA) במדעי המחשב, הטכניון, שנת 1987.

ואלה פרטי ניסיוני:

- הנני חבר סגל, בדרגת מרצה בכיר, במחלקה למדעי המחשב באוניברסיטת חיפה, החל מחודש אוקטובר 2005. בתפקיד זה אני מלמד בצורה קבועה קורסים בנושאי הצפנה ואבטחת מחשבים.
- פרסמתי יותר מ-45 מאמרים אקדמיים בתחום הקריפטוגרפיה, בכנסים ועיתונים מדעיים אשר מקבלים לפרסום רק אחוז קטן מהמאמרים הנשלחים אליהם. מאמרי הראשון בתחום פורסם בשנת 1990.
- אני משתתף באופן פעיל בוועדות שיפוט של מאמרים הנשלחים לכנסים ועיתונים מדעיים בנושאי קריפטוגרפיה.
- הנני רשום כממציא של 7 פטנטים, ו-13 בקשות פטנט, בנושאי הצפנה.

חוות דעתי מפורטת בהמשך מסמך זה.

חתימה אלקטרונית - מבוא

הבסיס המתמטי

הבסיס המתמטי לביצוע חתימה אלקטרונית מתבסס על שימוש בפונקציה הנקראת "פונקצית חתימה אסימטרית", בעלת התכונות הבאות:

- הפונקציה מוגדרת על ידי פרמטר סודי, אשר יכונה *"מפתח חתימה"*, או *"מפתח פרטי"*. אם נסמן את מפתח החתימה בסימן SK, נסמן את פלט הפונקציה על הקלט כלשהו X בצורה F(SK,X).[29]
- קיים פרמטר פומבי, אשר יכונה *"מפתח וידוא חתימה"* או *"מפתח ציבורי", או "מפתח פומבי"*. אין צורך לשמור ערך זה בסוד. נסמן את מפתח וידוא החתימה בסימן PK. אף אם ידוע ערך מפתח וידוא החתימה, לא ניתן לחשב בצורה יעילה את מפתח החתימה הסודי.
- בהינתן הערך X וערך Y האמור להיות שווה ל- F(SK,X) (חתימה על X), ובהינתן מפתח וידוא החתימה PK, קל לבדוק האם Y=F(SK,X). (כלומר, לוודא שהחתימה על X נכונה.)
- ללא ידיעת SK קשה לחשב את F(SK,X) לכל ערך X שהוא וזאת אף אם ידוע ערך המפתח הפומבי PK.

בהינתן פונקציה F המקיימת תכונות אלו, נרצה לבנות מערכת חתימה אשר מבטיחה כי ללא ידיעת מפתח החתימה הסודי SK, לא ניתן לייצר חתימה חדשה. ביתר דיוק, מתקיימת התכונה הבאה:

- יתכן והתוקף יודע את מפתח וידוא החתימה PK.
- יתכן והתוקף יודע גם מספר חתימות על ערכים כלשהם, אשר אולי אף נבחרו בידי התוקף.
- למרות מידע זה אין התוקף יכול לחשב חתימה על אף ערך נוסף.

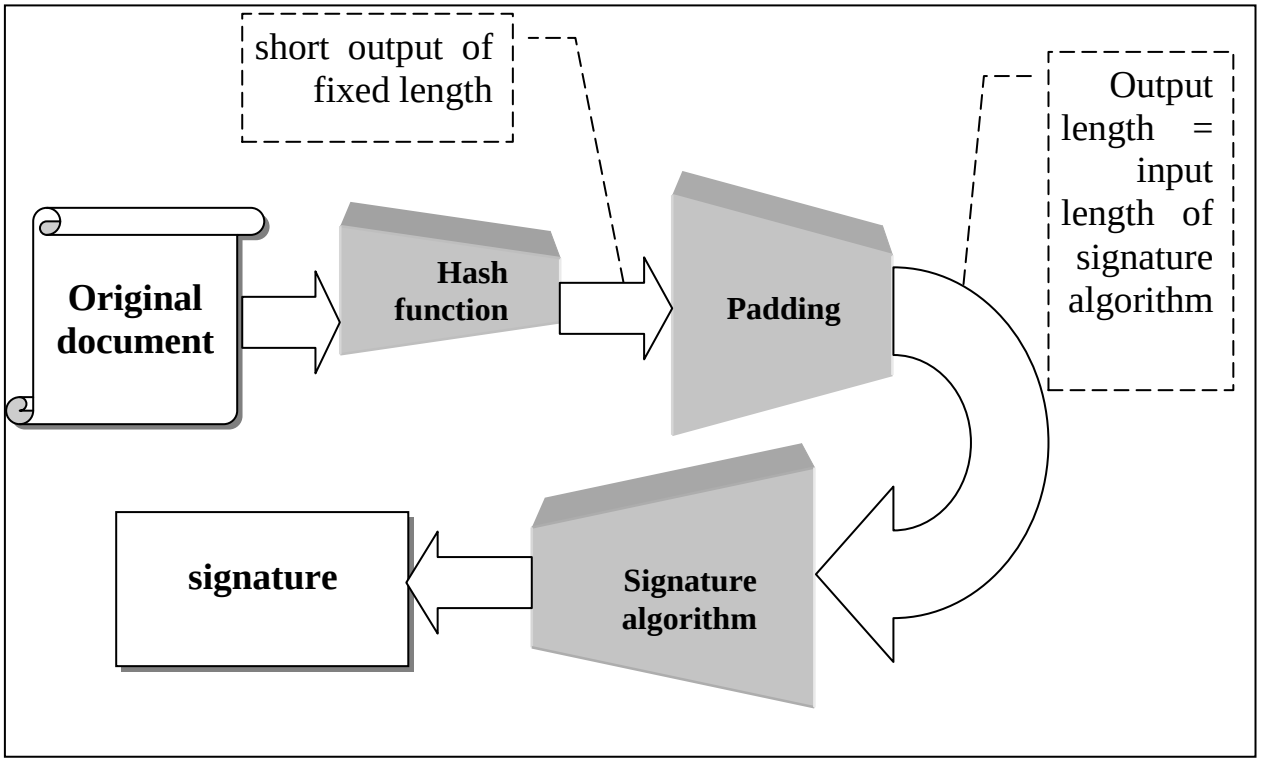
[29] יתכן והפונקציה F תהיה רנדומית, כלומר, חישוב F יהיה תלוי בערכים אקראיים שנבחרים בזמן חישוב הפונקציה. משמעות הדבר שבפעמים שונות בהן יחושב ערך זה, נקבל פלטים שונים של הפונקציה. (תכונה זו מתקיימת במספר סוגי חתימות, לדוגמא DSA). לענייננו אין הדבר עקרוני.

<u>מרכיבי מערכת לחתימה אלקטרונית</u>

מערכת לחתימה אלקטרונית מורכבת משלושה מרכיבים:

- שיטת גיבוב (hash), אשר מטרתה לתרגם קלט באורך כלשהו לפלט באורך קבוע (לדוגמא, פלט באורך 256 סיביות). שיטות גיבוב ידועות הן, לדוגמא, הפונקציות ממשפחת SHA.
- שיטת ריפוד (padding), אשר מקבלת קלט באורך כלשהו, קצר מפרמטר מסוים (לדוגמא, קצר מ-2048 סיביות), ומטרתה לרפד את הקלט במידע נוסף כך שאורכם הכולל יהיה זהה לערך הפרמטר. שיטות ריפוד ידועות מוגדרות, לדוגמא, בתקן PKCS V2.1.
- שיטת חתימה (signature), אשר מחשבת חתימה אלקטרונית[30]. לשיטה זו פרמטרים המגדירים לרוב את אורך ההודעה הנחתמת, ואת אורך וצורת יצור מפתח החתימה ומפתח וידוא החתימה. שיטת חתימה ידועה היא, לדוגמא, שיטת RSA עם מפתח וידוא חתימה באורך 2048 סיביות.

השימוש המקובל במערכות לחתימה אלקטרונית משתמש בשלושת מרכיבי המערכת: ראשית, מופעלת שיטת הגיבוב על ההודעה עליה יש לחתום, ומתקבל פלט באורך קבוע. לאחר מכן, מרופד ערך זה על ידי שיטת הריפוד, כך שאורכו יהיה זהה לאורך הקלט הדרוש לשיטת החתימה. לבסוף, מחושבת חתימה על הערך המרופד. תהליך זה מתואר בתרשים 1.



תרשים 1: מרכיבי מערכת חתימה, והשימוש בהם.

<u>משמעות חולשות של מרכיבי המערכת</u>

חולשה בכל אחד ממרכיבי מערכת החתימה פוגעת בבטיחות החתימה:

- חולשה בשיטת הגיבוב יכולה לפגוע בבטיחות החתימה בצורות הבאות:

[30] זוהי הפונקציה F אשר תוארה בסעיף 2.1 למעלה, אש משתמשת במפתח חתימה פרטי ובמפתח וידוא חתימה ציבורי.

- על שיטת הגיבוב לקיים את תכונת **2nd preimage resistance**: כלומר, עבור שיטת גיבוב הממומשת בפונקציה H(), צריך להתקיים שבהינתן קלט **m** והערך H(**m**), אזי אין דרך יעילה לחישוב קלט **m'** שונה מ-**m**, כך שמתקיים H(**m**)=H(**m'**). אם תכונה זו אינה מתקיימת אזי בהינתן חתימה על ערך **m** שחושבה בשיטה שתוארה למעלה (כלומר, הפעלת שיטת הגיבוב H על **m** ואח"כ המשך חישוב החתימה), קל למצוא ערך **m'** אשר החתימה תקיפה גם לגביו.
- על שיטת הגיבוב לקיים את תכונת **collision resistance**: כלומר, צריך להתקיים שאין דרך יעילה לחישוב שני ערכים **m,m'** השונים זה מזה ואשר מקיימים H(**m**)=H(**m'**). אם תכונה זו אינה מתקיימת אזי ניתן למצוא שני ערכים כאלו **m,m'**, ולבקש חתימה על הערך **m**, כאשר חתימה זו תהווה גם חתימה על הערך **m'**.[31]
- בנוסף, על שיטת הגיבוב להיות עמידה גם ל-near collision resistance. כלומר, דרוש שיהיה בלתי אפשרי למצוא שתי הודעות כך שרוב הסיביות של פלט פונקצית הגיבוב זהות עבורן. (שבירת תכונה זו תהיה שימושית ליריב אם האפליקציה המשתמשת בפונקצית הגיבוב מקצצת חלק מסיביות הפלט של הפונקציה. במקרה זה ה-"כמעט התנגשות" עלולה להפוך להתנגשות ממש.)

- חולשה בשיטת הריפוד יכולה לאפשר התקפות בהן ניתן ללמוד את מפתח החתימה הסודי או לזייף חתימות על הודעות אשר לא נחתמו על ידי החותם המאושר.
- חולשה בשיטת החתימה יכולה לחשוף את מפתח החתימה הסודי, או לאפשר זיוף חתימה על הודעות שעליהן לא חתם בעל מפתח החתימה.

<u>שיטות גיבוב (hash)</u>

<u>חולשות של שיטות גיבוב ומשמעותן לגבי חתימות אלקטרוניות.</u>

כאמור, שיטת גיבוב H חייבת לקיים את תכונת ה- 2nd preimage resistance (כך שבהינתן קלט m והערך H(m), אזי אין דרך יעילה לחישוב קלט m' שונה מ-m, כך שמתקיים H(m)=H(m')), ואת תכונת ה-collision resistance (כלומר, שאין דרך יעילה לחישוב שני ערכים m,m' השונים זה מזה ואשר מקיימים H(m)=H(m')).

[31] במסמך ETSI ובספרות מתוארת דרישת בטיחות נוספת בשם preimage resistance, אשר דורשת שבהינתן הערך H(m) יהיה בלתי אפשרי למצוא בצורה יעילה כל ערך m' שהוא, אפילו m=m', המקיים את התכונה H(m')=H(m) את הערך m. ההבדל בין תכונה זו ובין 2nd preimage resistance הוא שהתקפה אשר בהינתן H(m) מוצאת את m, תיחשב כפגיעה בתכונת ה-preimage resistance אך לא בתכונת ה-2nd preimage resistance. לענייננו תכונת ה-preimage resistance אינה רלוונטית, משום שאין צורך לשמור את ההודעה הנחתמת בסוד.

ידוע שקל יותר לתקוף את תכונת ה-collision resistance מאשר את תכונת ה- 2nd preimage resistance.

- בפרט, קל לראות שאם תוקף מצליח להביס את תכונת ה- **2nd preimage resistance** אזי ביכולתו לשבור את תכונת ה-**collision resistance**.
- אכן, התקיפות הידועות כנגד שיטת MD5, והרעיונות הקיימים לתקיפת SHA-1, משפיעים רק על ה-**collision resistance** ולא על תכונת ה- **2nd preimage resistance**ידוע שהתקפות גנריות, אשר ניתן להפעיל על כל פונקצית גיבוב שהיא, ופועלות על ידי חישוב H פעמים רבות עד לשבירת התכונה, יעילות יותר כנגד **collision resistance**. ביתר פרוט, אם אורך הפלט של H הינו **n** סיביות, אזי התקפה גנרית על תכונת ה-**collision resistance** תדרוש כ-$2^{n/2}$ חישובים של H, בעוד שהתקפה על תכונת ה- **2nd preimage resistance** תדרוש כ-2^{n} חישובים של H.[32] (אם יש יותר ממטרה אחת להתקפה אזי ההתקפה תהיה יעילה יותר[33] .)

<u>התקפות ידועות על שיטות גיבוב</u>

- ידועה התקפה יעילה המוצאת התנגשויות בפלט של פונקצית הגיבוב MD5. כמו כן, מתבצע מאמץ רב למצוא התנגשויות בפלט של שיטת הגיבוב SHA-1 וההערכה היא כי התנגשויות כאלו ימצאו בקרוב. **עקב כך, אין להניח כי פונקציות אלו מקיימות את תכונת ה-collision resistance.**
- לא ידועות התקפות יעילות על תכונת ה-**2nd preimage resistance** של MD5 או SHA-1, או של כל פונקציה אחרת אשר נמצאת היום בשימוש נרחב. . יחד עם זאת, ידועות תקיפות **2nd preimage** כנגד MD4 (שהינו וריאנט קדום של MD5) וכנגד הודעות חלשות ב-MD5.
- בנוסף להתקפות ספציפיות כנגד פונקציות גיבוב מסוימות, יש לקחת בחשבון גם התקפות <u>גנריות</u> אשר פועלות על ידי חישוב הפונקציה פעמים רבות עד אשר נמצאת התנגשות הפלטים הדרושה. היעילות של התקפות אלו תלויה אך ורק באורך הפלט של פונקצית הגיבוב, ולא בפעולות המתמטיות המתבצעות לשם חישוב הפונקציה. ההערכה המקובלת היא שבהשקעה של עשרות מיליוני דולרים ניתן יהיה בשנים הקרובות, בשיטות גנריות, למצוא התנגשויות של פונקציות שאורך הפלט שלהן הוא כ-160 סיביות, ולתקוף את תכונת ה-**2nd preimage resistance** של פונקציות שאורך הפלט שלהן הוא כ-100 סיביות.[34] ראו דיון בסעיף 3.4 למטה.

---

[32] ראו "Design principles for hash functions revisited", Bart Preneel, October 2005. http://csrc.nist.gov/groups/ST/hash/documents/preneel_nist_v2.pdf

[33] ראו תיאור ב- Parallel collision search with cryptanalytic applications, P .C. ***VAN OORSCHOT***, M.J. ***WIENER, 1996***, ובמסמך Design principles for hash functions revisited המצוטט למעלה.

[34] ראו תיאור במסמך Design principles for hash functions revisited המצוטט למעלה.

- התקפות על תכונת ה-collision resistance מוצאות שתי הודעות כלשהן, לאו דווקא הודעות בעלות משמעות, אשר פלט פונקצית הגיבוב עבורן שווה. לכאורה אין בכך סכנה משום שסביר שהתוקף לא יפיק תועלת ממציאת התנגשות של ערכי הודעות מסוג זה. אולם, הודגם בעבר שהמצב אינו כזה:
  - לגבי MD5 הודגם שהתנגשות של כל זוג הודעות ניתנת לתרגום להתנגשות של כל זוג מסמכי postscript, לפי בחירת התוקף[35]. התקפה זו ניתנת לשימוש מיידי עם כל פונקצית גיבוב אשר ידועה לגביה התנגשות של זוג הודעות כלשהו.
  - בצורה דומה, במקום לייצר מסמכי postscript ניתן, בהינתן התנגשות של ערכים כלשהם, ליצור זוג תכניות מחשב, אשר לכל אחת מהן פונקציונאליות כלשהי לפי בחירת התוקף, ואשר פלט פונקצית הגיבוב המופעלת עליהן זהה. כלומר, זוג תכניות מחשב P1 ו-P2, המבצעות חישובים שונים הניתנים לבחירה על ידי התוקף, ואשר מקיימות H(P1)=H(P2).
  - הודגם (כמתואר למטה) שניתן לשפר את שיטת מציאת ההתנגשויות של פונקצית MD5 כך שאפשר יהיה למצוא התנגשויות של הודעות המתאימות לפורמט של certificates. בצורה דומה, יתכן ושיטה שתימצא למציאת התנגשויות כלשהן בפונקצית גיבוב מסוימת, תהיה ניתנת לשיפור כך שאפשר יהיה למצוא התנגשויות בפורמט המתאים להודעות בעלות ערך לתוקף
- כאמור, לאחרונה תוארה התקפה כנגד CA אשר השתמש בפונקצית הגיבוב MD5. התקפה זו מאפשרת ליצור תעודות אלקטרוניות (certificates) לכל אתר אינטרנט שהוא, כולל אתרים שלא השתמשו בשירותיו של CA זה. התקפה זו מתוארת בנספח. המסקנה מהתקפה זו היא שניתן לעיתים להפוך חולשות מזעריות בשיטות הקריפטוגרפיות להתקפות של ממש על אפליקציות. לכן יש להימנע שכל שימוש בשיטות חתימה או גיבוב אשר קיים חשש כלשהו לגבי בטיחותן.

<u>משמעות ההתקפות עבור מערכות חתימה</u>

זמן וצורת ההתקפה

קיים הבדל בשימוש שתוקף של מערכת חתימה המשתמשת בשיטת גיבוב H יכול לעשות בכל אחד מסוגי החולשות:

- אם ביכולת התוקף לתקוף את תכונת ה- 2nd preimage resistance אזי בהינתן חתימה על מסמך מסוים הוא יכול לייצר חתימה על מסמך אחר. בפרט, התוקף יכול לבחון חתימה S על מסמך m שנבחר על ידי גוף אחר (שונה מהתוקף), ואשר נחתמה בעבר. כעת, אם התוקף מוצא מסמך שונה m' המקיים H(m)=H(m'), הרי שהחתימה S היא גם חתימה על m'.

[35] http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/

- אם ביכולת התוקף לתקוף רק את תכונת ה-**collision resistance** אזי עליו למצוא *<u>מראש</u>* שני מסמכים **m,m'**, כך שמתקיים **H(m)=H(m')**, על התוקף להשיג חתימה על המסמך **m** (כלומר, התוקף חייב לשכנע את החותם לחתום על מסמך שנבחר על ידי התוקף), ואילו התוכן של **m'** צריך להיות בעל ערך רב לתוקף. כעת יכול החותם להציג את החתימה על **m** כאילו היא חתימה על המסמך **m'**.

- ההבדלים העיקריים בין שני סוגי התקיפות הוא שההתקפה מהסוג השני דורשת מהתוקף לדעת מראש, לפני שהחותם מחשב את החתימה, את השיטה למציאת התנגשויות ב-**H()**, ואת זוג ההודעות **m,m'**, וכן על התוקף לשכנע את החותם לחתום על המסמך **m**. דרישה זו מקשה מאד על התקפות. כמו כן יש לה משמעות לגבי הגבלת התקופה בה מותר יהיה להשתמש בשיטות הגיבוב. ראה דיון למטה.

- יש שים לב כי לשם ניצול התקפה על תכונת ה-**collision resistance** על התוקף להיות מסוגל לבחור את ההודעה עליה תתבצע החתימה, או לפחות להיות מסוגל לבחור חלקים משמעותיים ממנה. במימוש המקובל בישראל של תעודה לחתימה אלקטרונית מאושרת (**certificates**), המפתח הפומבי נוצר על גבי אמצעי חומרה, כרטיס חכם, שבידי הגורם שמבקש לקבל את החתימה, אולם הגורם מבקש החתימה אינו יכול להשפיע על ערך המפתח, ואינו יודע את המפתח הסודי. לכן, בצורת שימוש זו אין ביכולת התוקף לנצל התקפת **collision resistance** (לשם יצירת תעודה מאושרת, **certificate**, אשר הינה תקפה לשני מפתחות שונים) כל עוד התוקף אינו יכול לפרוץ את הגנות הכרטיס החכם.

- כאמור, לשם התקפה על תכונת ה-**collision resistance** על התוקף להיות מסוגל לבחור את ההודעה עליה תתבצע החתימה, או לפחות להיות מסוגל לבחור חלקים משמעותיים ממנה. מומלץ לכן שגורם מאשר (**CA**) יכניס מחרוזת אקראית אשר איננה ניתנת לחיזוי על ידי אף גורם אחר, לתוך ההודעה עליה הוא מחשב את פונקצית הגיבוב וחותם. יש להכניס מחרוזת זו לפני השדות אשר תוכנם נקבע על ידי הגורם המבקש את החתימה. (המלצה זו נמצאת במסמך **ETSI** סעיף 5.2.1 הערה 2.)

- מכון התקנים האמריקאי (**NIST**) מקיים תהליך של בחירת פונקציות גיבוב, אשר יקראו **SHA-3**, אשר יחליפו את שיטות הגיבוב הקיימות. ההחלטה בעניין צפויה להתקבל בשנת 2012. יש לעקוב אחר תהליך זה ולעדכן את ההמלצות בהתאם.

אורך פלט שיטת הגיבוב

כאמור למעלה, ניתן להתקיף, בעלות כספית ניכרת, את תכונת ה-collision resistance של כל שיטת גיבוב שאורך הפלט שלה הוא עד 160 סיביות. לכן לא רצוי להשתמש בשיטות מסוג זה. מאידך, ישנן שיטות חתימה אשר מקבלות קלט שאורכו עד 160 סיביות (לדוגמא, שיטת DSA עם פרמטר q באורך 160 סיביות). לכן, לא רצוי יהיה להשתמש בשיטות חתימה מסוג זה.

2.4 המלצות לגבי שימוש בשיטות גיבוב

ההמלצות הן ברוח ההמלצות באיחוד האירופי[36] ובארה"ב[37].

ההמלצות:

1. מומלץ לאפשר להשתמש בשיטות הגיבוב הבאות: SHA-224, SHA-256, SHA-384, SHA-512, Whirlpool (אורכי הפלט של שיטות אלו הינם 224, 256, 384, 512 ו-512 סיביות, בהתאמה).[38]

2. מומלץ שלא לאפשר להשתמש בשיטת הגיבוב MD5.

3. ניתן, אך לא מומלץ, להמשיך את השימוש בשיטת הגיבוב SHA-1, אך זאת רק עד לסוף שנת 2010.

4. אם יש צורך בשיטת גיבוב אשר אורך הפלט שלה הוא 160 סיביות בתאריך מאוחר יותר, אזי ניתן להשתמש בשיטות הבאות וזאת רק עד סוף שנת 2012:

   א. להשתמש בשיטת RIPEMD-160, או

   ב. להשתמש בשיטת SHA-224 כאשר מקצרים את הפלט המקורי של הפונקציה לפלט באורך 160 סיביות (למשל, על ידי התעלמות מ-64 הסיביות הראשונות (most significant bits) של הפלט של SHA-224.[39]

5. עקב החולשות האחרונות שהתגלו לגבי SHA-1, מתקיים כיום מחקר ענף בבטיחות של שיטות גיבוב. בפרט, מכון התקנים האמריקאי (NIST) מקיים תהליך אל בחירת פונקצית גיבוב חדשה, SHA-3. יש לעקוב אחר תוצאות מחקר זה ולבחון מחדש את ההמלצות לאחר פרסום המלצות מכון התקנים האמריקאי (NIST) לגבי SHA-3, אשר יחליפו את שיטות הגיבוב הקיימות. ההחלטה בעניין צפויה להתקבל בשנת 2012.

---

[36] ETSI TS 102 176-1 V2.0.0 Electronic signatures and infrastructures (ESI); Algorithms and parameters for secure electronic signatures; Part 1: Hash functions and asymmetric algorithms, November 2007.

[37] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revised), March 2007.

[38] לגבי SHA-224, פונקציה זו מחושבת בצורה דומה ל-SHA-256 אך תוך שימוש בערך אתחול (IV) שונה, ובהוספת קיצוץ של הפלט לאורך של 224 סיביות. לכן, אם ניתן להשתמש ב-SHA-256 לא כדאי להשתמש ב-SHA-224. (המלצה זו נמצאת גם במסמך ETSI, סעיף 5.2.3.)

[39] לאורה היה ניתן כאן להשתמש בפלט של SHA-256 ולקצצו לאורך של 160 סיביות. הסיבה להמלצה על חישוב וקיצוץ SHA-224 היא מכיוון ששימוש בערכי אתחול זהים בפונקציות שונות יכול לגרום לבעיות בטיחות. ערך האתחול של SHA-224 שונה מזה של SHA-256. כמו כן, צפוי שלא יהיה שימוש נרחב ב-SHA-224 (לעומת השימוש ב-SHA-256). אנו מעדיפים לכן שהפונקציה שאורך הפלט שלה יהיה 160 סיביות, תהיה מבוססת על ערך ה-IV של SHA-224, שלא צפוי לו שימוש אחר נרחב.

<u>נימוקים להמלצות:</u>

1. שיטות הגיבוב הנ"ל אושרו לשימוש במסמך ETSI, סעיף 5.2. לא ידועות התקפות על תכונת ה-preimage resistance 2nd, או תכונה אחרת, של שיטות גיבוב שלו.

2. שיטת MD5 אינה מקיימת את תכונת ה-collision resistance. היא אינה מותרת בשימוש לפי מסמכים עדכניים (ובפרט, מסמך ETSI ומסמך NIST 800-57.)

3. ההערכה כיום היא כי התקפות מעשיות על תכונת ה-collision resistance של SHA1 ימצאו בקרוב.[40] ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לסיים את השימוש בשיטת SHA1 עד סוף שנת 2010.[41] מסמך NIST 800-57 ממליץ לא להשתמש בפונקציה במערכות חדשות.

4. לא ידועות התקפות יעילות כנגד השיטות אשר מוצעות בסעיף זה, פרט לשיטות התקפה גנריות אשר טובות כנגד כל פונקצית גיבוב אשר הפלט שלה באורך 160 סיביות. התקפות אלו דורשות השקעה רבה ולכן אינן מהוות סיכון מיידי, אולם כדאי לעבור לשימוש בפונקציות אשר אורך הפלט שלהן ארוך מ-160 סיביות בכדי להתגונן מהתקפות אלו.

   א. ביתר פרוט, העלות של מציאת התנגשות עבור פונקצית גיבוב שאורך הפלט שלה הוא 160 סיביות, היא כ-2^{80} הפעלות של הפונקציה, תוך שימוש בכ-2^{80} מילות זיכרון. הודגם גם על ידי Von Oorschot ו-Wiener כיצד ניתן להפעיל אלגוריתם לחיפוש התנגשויות על הרבה מחשבים במקביל, כך שניתן למקבל את זמן החיפוש.[42] עלינו לבדוק, לכן, מהי ההשקעה הדרושה בכדי לבצע חישוב כזה. התוקף האפשרי הוא גוף אשר ביכולתו להשקיע כסף רב (עשרות מיליוני דולרים) בבניית חומרה ייעודית להתקפה, או אשר ברשותו מחשבים רבים אשר יכולים לעבוד למען ההתקפה (לדוגמא, תוקף אשר שולט ב-bot net המכיל מאות אלפי מחשבים).

   ב. Preneel טוען, על סמך מאמרם של Von Oorschot ו-Wiener, כי בעלות של 10 מיליוני דולרים היה ניתן ב-2006 למצוא התנגשויות בפלט של שיטת גיבוב שאורך הפלט שלה הוא 160 סיביות.

---

[40] http://eurocrypt2009rump.cr.yp.to/837a0a8086fa6ca714249409ddfae43d.pdf, http://eprint.iacr.org/2009/259

[41] http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html

[42] Parallel collision search with cryptanalytic applications, P .C. ***VAN OORSCHOT***, M.J. ***WIENER, 1996***.

ג. ניראה שעלות החישוב גבוהה יותר. לדוגמא, ניטען[43] ב-2005 שניתן בעלות של 10 מיליוני דולרים לבנות מערכת המכילה 303 מחשבים,כ"א מהם עם 16 לוחות המכילים כ"א 32 LSIs, המכילים כ"א 64 ליבות לחישוב SHA-1. כל ליבה מבצעת 2^{25} חישובי SHA-1 בשנייה. כלומר, המערכת מבצעת כ-2^{48} חישובי SHA-1 בשנייה. לפי חוק מור, ניתן יהיה בסוף 2009 לבנות בעלות זו מערכת אשר תבצע 2^{51} חישובי SHA-1 בשנייה, כלומר כ-2^{76} חישובים בשנה. לכן העלות (התיאורטית, יש לציין) של ביצוע 2^{80} חישובי SHA-1 תוך שנה היא כ-160 מיליוני דולר. יש לציין שעלות חישוב פונקציה אחרת (שונה מ-SHA-1 אך בעלת פלט באורך דומה) יכולה להיות שונה.

ד. בצורה דומה, תוקף המשתמש במאות אלפי מחשבים (לדוגמא, על ידי הפעלת bot net), יכול גם כן לבצע חישוב בסדר גודל דומה בזמן סביר.

ה. במאמר משנת 2000 של Lenstra ו-Verheul [44] מחושבים אורכי המפתחות אשר יספקו בטיחות שקולה לזו שסיפקה מערכת DES בשנת 1982, וזאת לכל שנה ושנה. חישוב זה מתבסס על ההתקדמות בקצב החישוב והעלות לבניית מערכות חמרה ותכנה. להערכתם, מפתח סימטרי באורך 80 סיביות (אשר שבירתו שקולה לעלות מציאת התנגשויות בפונקצית גיבוב עם פלט באורך 160 סיביות) יהיה שקול בשנת 2012 לבטיחות שנתן DES בשנת 1982. אם אנו מאמינים ש-DES היה בטוח לשימוש מסחרי עד שנת 1997, אזי לשיטתם נוכל להשתמש עד שנת 2027 בפונקצית גיבוב עם פלט באורך 160 סיביות.

ו. מסמך SP 800-57 של NIST משנת 2006 קובע שאורך מפתח סימטרי של 80 סיביות יהיה בטוח לשימוש עד שנת 2010.

ז. מסמך של ECRYPT [45] משנת 2009 מתאר את העלויות הבאות להתקפות מסוגים שונים על מפתחות סימטריים (אורך הפלט של פונקצית הגיבוב צריך להיות לפחות כפול). ניתוח מפורט של האנליזה שהביאה למסקנות אלו נמצא בפרק 5 של המסמך.

[43] Hardware Architecture and Cost Estimates for Breaking SHA-1, Satoh, A., 2005.

[44] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, PKC2000: p. 446-465, 01/2000.

[45] Yearly Report on Algorithms and Keysizes (2007-2008), D.SPA.7, IST-2007-216676 ECRYPT, 07/2009. http://www.ecrypt.eu.org/documents/D.SPA.7.pdf

ח.

תוקף	תקציב	חמרה	אורך מפתח מינימאלי אשר בטוח כנגד ההתקפה
האקר	$400	PC/FPGA	כ-60
ארגון קטן	$10K	PC/FPGA	64
ארגון בינוני	$300K	FPGA/ASIC	68
ארגון גדול	$10M	FPGA/ASIC	78
ממשלה	$300M	ASIC	84

ט. <u>לסיכום, לא ברורה העלות המדויקת של התקפה גנרית כנגד פונקציות שאורך הפלט שלהן הוא 160 סיביות, אולם ניראה שהתקפה כזו היא בגדר הסביר בעתיד הנראה לעין ולכן יש לעבור לפונקציות עם פלט באורך גדול יותר.</u>

5. מתקיים כיום מחקר ענף בבטיחות של שיטות גיבוב. יש לעקוב אחר תוצאות מחקר זה.

<u>שיטות ריפוד (padding)</u>

מטרת השימוש בשיטות ריפוד היא לגשר בין אורך הפלט של שיטת הגיבוב ואורך הקלט של שיטת החתימה, במצב בו האורך של פלט שיטת הגיבוב קצר מאורך הקלט של שיטת החתימה. מסיבה זו אין צורך להשתמש בשיטות ריפוד יחד עם חתימות לפי אלגוריתם DSA או עם חתימות בשיטת המבוססות על עקומים אליפטיים (elliptic curves), כי בשיטות אלה החתימה מתבצעת על קלט שאורכו כאורך הפלט של שיטות גיבוב ידועות (כלומר, 160, 224, 256 או 512 סיביות).יש צורך להשתמש בשיטות ריפוד בחתימות לפי שיטת RSA, כי במקרה זה אורך הקלט לאלגוריתם החתימה הוא כאורך המפתח הפומבי (כלומר, 1024 סיביות או יותר) והינו ארוך יותר מהפלט של שיטת הגיבוב. שיטות ידועות לריפוד קלט לחתימות RSA מתוארות במסמך PKCS #1 v2.1[46] ובתקן ISO 9796. (קיים גם מסמך קודם, PKCS #1 v1.5, אך לא מומלץ לעבוד לפיו כי הוא הוחלף על ידי PKCS #1 v2.1.)

<u>המלצה: יש לבצע את הריפוד לפי אחת השיטות המתוארות במסמך FIPS 186-3, סעיף 5.5.</u>

- שיטות אלו הינן שיטת RSASSA-PKCS1-v1.5 ושיטת RSASSA-PSS, לפי מסמך PKCS #1 v2.1, בשינויים קלים המתוארים למטה.[47]
- שיטות אלו מתוארות גם במסמך ETSI, סעיף 7.2. מסמך ETSI מאפשר גם שימוש בשיטות לפי תקן ISO 9796.
- מסמך FIPS 186-3 דורש את השינויים הקלים הבאים בשיטות:
  - בשימוש בשיטת RSASSA-PSS (מתקן PKCS #1 v2.1), אורך ה-salt, המסומן כ-eLen, חייב להיות קטן או שווה מאורך פלט פונקצית הגיבוב (hash) בה משתמשים.
  - בשימוש בשיטת RSASSA-PKCS-v1.5 (מתקן PKCS #1 v2.1), בזמן וידוא החתימה, יש לחלץ את ערך ה-hash מההודעה החתומה תוך וידוא שמדובר בסיביות הנכונות המכילות ערך זה, כמתואר בסעיף 5.5(f) במסמך FIPS 186-3.

<u>נימוקים להמלצה:</u>

- ההמלצות הן לפי התקנים הבינלאומיים האחרונים. מסמך PKCS #1 v2.1, המלצות ETSI, FIPS 186-3.
- התיקונים במסמך FIPS 186-3 מתקנים נקודות בהן מסמך PKCS #1 v2.1 לא היה חד משמעי, ואשר היו עלולות לגרום לבעיות בטיחות.

---

[46] ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[47] יש לשים לב כי ישנו דמיון בין המספור של שמות המסמכים ושל שמות שיטות הריפוד המתוארות בהם. המסמך העדכני הוא מסמך PKCS #1 v2.1, משנת 2002, אשר מחליף את מסמך PKCS #1 v1.5. מסמך PKCS #1 v2.1 מתאר את שיטות הריפוד RSASSA-PKCS1-v1.5 ו- RSASSA-PSS

שיטות חתימה (signing)

הגבלה על מועד שימוש בשיטות חתימה שיש חשש לגבי בטיחותן בעתיד

ישנו הבדל משמעותי באפשרות לביצוע התקפה עקב חולשה בשיטת החתימה, לעומת ביצוע התקפות עקב חולשה בתכונת ה-collision resistance של שיטות גיבוב[48].

חולשה בתכונת ה-collision resistance של שיטת גיבוב מאפשרת לתוקף לבקש חתימה על מסמך אחד, ולהשתמש בה כחתימה על מסמך אחר. לכן על התוקף להיות מסוגל לבקש ולקבל חתימה על מסמך לאחר שהתגלתה (או לאחר שהתוקף גילה) חולשה בשיטת הגיבוב.

חולשה בשיטת חתימה (לדוגמא, מציאת אלגוריתם פירוק מספרים אשר מסוגל לפרק מפתח פומבי של שיטת RSA), מאפשרת לתוקף לזייף חתימות כל עוד ישנה משמעות לחתימות אשר נוצרו בעזרת שיטת החתימה האמורה. זאת אף אם החתימה המקורית נעשתה לפני שהתגלתה חולשה בשיטת החתימה.

נניח לדוגמא שמערכת חתימה משתמשת בשיטת גיבוב מסוימת (לדוגמא SHA-1) ובשיטת חתימה מסוימת (לדוגמא, RSA עם מפתח פומבי באורך 1024 סיביות). הוגדר שניתן לבצע חתימות חדשות במערכת זו עד תאריך X, אך ניתן להציג ולהשתמש בחתימות מסוג זה עד תאריך Y שהינו מאוחר יותר. משמעות הדבר היא שגילוי אפשרות למציאת התנגשויות ב-SHA-1 יועיל לתוקף אם שיטה זו תתגלה לפני תאריך X. לעומת זאת, אם תתגלה לפני תאריך Y שיטה יעילה לפרוק מספרים בני 1024 סיביות, היא תאפשר זיוף חתימות שנעשו בעזרת המערכת (כיוון שהתוקף יכול לבצע את זיוף החתימה עד תאריך Y).

בניסוח אחר, נניח כי אנו מאמינים כי עד תאריך Z לא יתאפשר למצוא התנגשויות ב-SHA-1 או לפרק מספרים בני 1024 סיביות, אך אנו חוששים שלאחר תאריך זה יתכן ותימצא דרך לבצע אחת מהתקפות אלו. כמו כן, אנו מאמינים שבעתיד הנראה לעין לא יהיו התקפות של ממש כנגד אלגוריתם הגיבוב SHA-256 או חתימות RSA עם מפתח באורך 2048 סיביות. ברשותנו מערכת חתימה א' המשתמשת בשיטת הגיבוב SHA-1 ובמפתח RSA באורך 2048 סיביות. ברשותנו גם מערכת חתימה ב' המשתמשת בשיטת הגיבוב SHA-256 ובמפתח RSA באורך 1024 סיביות.

בהתאם להנחות נוכל לאפשר ביצוע חתימות במערכת א' עד תאריך Z, ולאסור ביצוע חתימות כאלו אח"כ. השימוש בחתימות ובדיקתן יכולים להתבצע גם בתאריך מאוחר יותר. לעומת זאת, עלינו לאסור כל שימוש במערכת ב' לאחר תאריך Z, כולל איסור האפשרות להשתמש בחתימות שנחתמו בתאריך מוקדם יותר. זאת משום שהחל מתאריך זה יתכן וקיימת האפשרות לזייף חתימות מסוג זה.

חתימה לפי אלגוריתם RSA

שיטת החתימה לפי אלגוריתם RSA היא השיטה הנפוצה ביותר בשימוש כיום. היא מבוססת על שימוש במפתח חתימה פרטי המורכב משני מספרים ראשוניים p, q, בעלי אורך דומה זה לזה, ומפתח פומבי (הנקרא גם "מפתח ציבורי") n המקיים $n=p\cdot q$. כמו כן מכיל המפתח הפומבי מספר נוסף (אקספוננט) המכונה e, והמפתח הפרטי מכיל מספר (אקספוננט) המכונה d.

המלצות לגבי חישוב חתימות לפי שיטת RSA:

חישוב חתימות לפי שיטת RSA חייב להתבצע בצורה הבאה, המקבילה לדרישות במסמך ETSI סעיף 6.1.2.1:

חישוב חתימות חייב להתבצע לפי מסמך RFC 3447 [49] (אליו מפנה מסמך ETSI), המתאר את תקן PKCS#1 V2.1, בתוספת הדרישות הבאות המפורטות גם הן במסמך ETSI:

- אורכם של המספרים p ו-q צריך להיות דומה, עד להפרש של 30 סיביות (כלומר, מתקיימת התכונה $|\log_2 p - \log_2 q|<30$).

[48] כל ההתקפות הידועות כיום כנגד שיטות גיבוב אשר הינן בשימוש נרחב, הינן נגד תכונה זו.

[49] RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, J. Jonsson, B. Kaliski. February 2003.

- המספרים p ו-q צריכים להיבחר באקראי מקבוצת מספרים ראשוניים גדולה (ההסתברות לבחירת ערך מסוים לאחד ממספרים אלו צריכה להיות לכל היותר 2^{-128}).
- אורך האקספוננט d שבמפתח הפרטי חייב להיות קצר מאורך המפתח הפומבי n, אך קרוב מאד אליו, עד להפרש של 30 סיביות (כלומר, מתקיימת התכונה $\log_2 n - \log_2 d$ <30).

<u>נימוקים להמלצות:</u>

- ההמלצות מקבילות לדרישות במסמך ETSI סעיף 6.1.2.1.
- ההפניה לתקן PKCS #1 V2.1 קיימת גם במסמך FIPS 186-3, סעיף 5.5.
- הדרישות מעבר לתקן PKCS#1 V2.1, המפורטות במפורש כאן (ובמסמך ETSI), ידועות כחיוניות לשם אבטחת החתימה.

<u>אורכי המפתחות</u>

בטיחות מערכת RSA תלויה בכך שלא ניתן לפרק את המפתח הפומבי n ולמצוא את גורמיו הראשוניים p,q המהווים את המפתח הפרטי. ככל שהמפתח הפומבי n הינו ארוך יותר, קשה יותר לבצע את הפירוק. ידוע שניתן לפרק מפתחות RSA באורך של כ-663 סיביות. שיפורים ביכולת הפירוק יכולים להתבצע באחת מהדרכים הבאות:

- שיפורים ביכולת החישוב: חוק מור טוען שכוח החישוב מוכפל כל שנה וחצי. כמו כן, ישנם שיפורים מתמידים ביכולת לרתום מספר גדול מאד של מחשבים לעבודה במקביל לפתרון בעיה. שיפורים אלו מביאים לשיפור מתמיד וניתן לחיזוי, אך איטי, ביכולת לפרק מספרים.

- שיפורים אלגוריתמיים: מידי פעם (אחת למספר ניכר של שנים) מוצאים חוקרים שיפורים משמעותיים באלגוריתמים לפרוק מספרים. שיפורים אלו מביאים לקפיצה ביכולת לפרוק מספרים. לא ניתן לחזות מראש את המועד בו ימצא השיפור הבא, ואת איכות השיפור.

- קיימות הצעות לבניית חמרה מיוחדת לפרוק מספרים. העלות של בניית חמרה זו היא גבוהה, אולם ביכולתה יהיה לפרק מספרים ביעילות רבה יותר מאשר בידי חמרה סטנדרטית.

מסמך ECRYPT [50] משווה בין אורכי מפתחות RSA (וכן מפתחות של מערכות חתימה מבוססות לוגריתם דיסקרטי, כדוגמת DSA המתוארת בהמשך) לבין אורכי מפתחות סימטריים המספקים בטיחות מקבילה. הטבלה היא כדלהלן:

אורך מפתח RSA או DSA	בטיחות (סיביות של מפתח סימטרי שקול)
768	62
1024	73
1536	89
2048	103

אותו מסמך מביא בפרק 6 סקירה של הערכות שונות המשוות בין הקושי של פרוק מספרים לבין הקושי של שבירת מפתח סימטרי באורך 80 סיביות, כלומר לגבי אורך המפתח הפומבי של RSA השקול בבטיחות למפתח סימטרי באורך 80 סיביות. ההערכות הללו נעות בין אורך מפתח פומבי של 1024 סיביות ל-1536 סיביות (ההערכה השנייה היא המחמירה יותר).
ציינו למעלה כי מקובל היום להניח שמפתחת סימטרי באורך 80 סיביות נותן בטיחות גבולית כנגד ממשלות, ובטיחות לטווח בינוני כנגד ארגונים בגודל בינוני[51]. לכן מפתחות פומביים באורך 1024 סיביות טובים לשימוש רק לזמן הקרוב ביותר. מפתחות באורך 2048 צפויים לתת בטיחות סבירה לשנים הקרובות. (יחד עם זאת, הבטיחות של מפתחות באורך 2048 סיביות קטנה משמעותית מזו של מפתחות סימטריים באורך 128 סיביות, אשר נחשבים כמפתחות באורך מינימאלי להצפנה סימטרית. לכן יש להתכונן למעבר לשימוש במפתחות ארוכים יותר.)
הערה: כל ההערכות הללו מתבססות על שיפורים בכוח החישוב ואינן לוקחות בחשבון פריצת דרך מחקרית בשיטות לפירוק מספרים. פריצת דרך כזו, אם תהיה, או אם התגלתה כבר אך לא פורסמה בספרות הגלויה, תאפשר פרוק מספרים ארוכים יותר מאלו המצוינים בהערכות.

<u>המלצות לגבי אורך מפתחות RSA:</u>

- מומלץ להשתמש במפתח פומבי שאורכו 2048 סיביות לפחות.

- ניתן להשתמש במפתח פומבי שאורכו 1024 סיביות, <u>אך זאת רק עד לסוף שנת 2010</u>. יחד עם זאת שימוש זה יהיה אפשרי רק לחתימות שהן בעלות ערך <u>עד סוף שנת 2016</u> וחסרות

[50] <u>Yearly Report on Algorithms and Keysizes (2008-2009)</u>, D.SPA.7, IST-2007-216676 <u>ECRYPT</u>, http://www.ecrypt.eu.org/documents/D.SPA.7.pdf 07/2009.
[51] מסמך ECRYPT, טבלה 7.4.

ערך לאחר תאריך זה. (כלומר, אם יתכן ויהיה צורך לבדוק חתימה לאחר סוף שנת 2016, אין לבצע חתימה זו בעזרת מפתח באורך 1024 סיביות.) [52]

- גורם מאשר חייב להשתמש, החל מסוף שנת 2011, במפתח פומבי שאורכו 4096 סיביות לכל הפחות.
- בשימושים אחרים בעלי חשיבות קריטית (כגון חתימות על ידי גופים במעמד מקביל לגורם מאשר, או חתימות אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים אסור השימוש במפתחות בני 1024 סיביות, ויש לשקול מעבר למפתח פומבי שאורכו 4096 סיביות לכל הפחות.
- יש להתכונן למעבר עתידי של כל הגורמים החותמים לשימוש במפתחות באורך 4096 סיביות.

<u>נימוקים להמלצות לגבי אורך מפתחות RSA:</u>

- מסמכי ETSI או FIPS 186-3 מרשים שימוש במפתח פומבי שאורכו 1024 סיביות, אך לא במפתחות קצרים יותר. לאחרונה הודגם פירוק של מפתח RSA באורך 768 סיביות (משמעות הדבר שבירה של מערכת החתימה התואמת).[53]
- ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לעבור למפתחות RSA באורך 2048 סיביות החל מסוף שנת 2010.[54] .
- מסמך ECRYPT מאפשר שימוש במפתח באורך 1024 סיביות (סעיף 14.2) אך, כאמור לעיל, טוען שבכדי להשיג בטיחות כנגד ארגונים בסדר גודל רציני יש להשתמש במפתחות ארוכים יותר.
- הבטיחות של מפתחות באורך 2048 סיביות קטנה משמעותית מזו של מפתחות סימטריים באורך 128 סיביות, אשר נחשבים כמפתחות באורך מינימאלי להצפנה סימטרית. לכן יש להתכונן למעבר לשימוש במפתחות ארוכים יותר.

לגבי ההמלצה לגבי הגבלת מועד <u>השימוש</u> בחתימה (לעומת הגבלת מועד יצור החתימה), ראו הסבר להגבלה זו בסעיף 4.1.

<u>חתימה לפי שיטת DSA</u>

שיטת החתימה לפי אלגוריתם DSA פותחה על ידי ממשלת ארה"ב. השיטה מבוססת על הקושי בחישוב לוגריתם דיסקרטי. השיטה משתמשת בפרמטרים פומביים p,q,g אשר יכולים להיות משותפים לחותמים רבים, כאשר p הוא מספר ראשוני ו-q הוא מספר ראשוני קטן מ-p. הפרמטר g הוא יוצר של תת-חבורה מסדר q מודולו p. המפתח הפרטי מכיל גם מספר x בתחום $0<x<q$, ואילו המפתח הציבורי מכיל את הערך g^x מודולו p.

<u>המלצה:</u>

<u>חישוב חתימות לפי שיטת DSA חייב להתבצע בצורה המתוארת במסמך FIPS 186-3.</u>[55] יש לשים לב לדגשים הבאים:

[52] כיום ברירת המחדל של תוקף מסמכים חתומים היא שבע שנים. מטרתנו היא להגביל את התוקף של מסמכים הנחתמים על ידי מפתחות קצרים לעד שבע שנים מסוף שנת 2009. כמו כן, במידה ובמהלך תקופה זו תתגלה התקפה על חתימות עם מפתחות באורכים אלו, יהיה צורך לבטל תוקף של חתימות קיימות ולבצע תהליך של חתימה מחדש על מסמכים רלוונטיים.

[53] http://eprint.iacr.org/2010/006.pdf

[54] http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html

- **אורכי מפתחות.** נסמן באות L את האורך בסיביות של הפרמטר p, ובאות N את האורך בסיביות של הפרמטר q. ישנם רק ארבעה צרופים מאושרים של אורכי מפתחות: (L=1024,N=160), (L=2048,N=224), (L=2048,N=256), (L=3072,N=256).

  - **המלצה:** ניתן להשתמש במפתח פומבי עם אורכים (L=1024,N=160), אך זאת רק עד לסוף שנת 2010. יחד עם זאת שימוש זה יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחסרות ערך לאחר תאריך זה. לגבי חתימות בעלות חשיבות קריטית, אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים, יש לעבור בהקדם האפשרי למפתח פומבי לפי צירופי האורכים האחרים המאושרים במסמך FIPS 186-3 (כלומר, (L=3072,N=256), (L=2048,N=256), (L=2048,N=224)). גורם מאשר המשתמש בחתימות מסוג זה יהיה חייב לעבור עד סוף שנת 2011 לשימוש במפתח פומבי באורכים המתאימים לצרופים אלה.מבחינת בטיחות עדיף כמובן להשתמש בצרוף עם המפתחות הארוכים ביותר האפשריים באילוצי המערכת.[56]

- נשים לב כי N (אורך הפרמטר q) חייב להיות שווה לאורך הפלט של שיטת הגיבוב בה נשתמש. אין צורך בביצוע ריפוד לערך זה, אולם יש לשנותו לייצוג של מספר שלם (integer) בצורה המתוארת במסמך FIPS 186-3.

- אלגוריתם ה-DSA מגדיר כי בכל ביצוע חתימה יש לבחור ולהשתמש בערך אקראי k בתחום 0<k<q. יש חובה לבחור ערך זה באקראי עבור כל ביצוע חתימה. ידועות התקפות על בטיחות המערכת אם ערך זה או חלקים ממנו חזרה אינם נבחרים באקראי.

נימוקים להמלצה:

- DSA הינו תקן חתימה אמריקאי, אשר פותח על ידי ממשלת ארה"ב, ויש לעקוב אחר ההמלצות העדכניות של מכון התקנים האמריקאי לגביו.

- אורכי המפתחות תואמים להמלצות של מסמך ECRYPT.

חתימה לפי שיטות המבוססות על עקומים אליפטיים (elliptic curves)

חתימות המבוססות על עקומים אליפטיים מתבצעות בשיטה דומה לשיטת DSA, אולם בחבורה שונה – כלומר, במקום לבצע חישובים בחבורה מסדר q מודולו p, החישובים מתבצעים בחבורה המוגדרת על ידי עקום אליפטי.
היתרון הגדול של ביצוע חתימות על ידי עקומים אליפטיים הוא שאורכי המפתחות והחתימה קצרים יותר, וזמן החישוב יעיל יותר.

המלצה:

שיטות חתימה המתבססות על עקומים אליפטיים יתבצעו לפי מסמך ETSI, סעיפים 6.1.2.3-6.1.2.6, בשינוי הבא: במקומות בהם מסמך ETSI מסתמך על מסמך FIPS 186-2 יש להסתמך על מסמך FIPS 186-3.

ביתר פרוט

- אלגוריתם ECDSAאליפטי מעל שדה מסדר ראשוני $E(F_p)$. זהו אלגוריתם DSA בהתבסס על עקום אליפטי מעל שדה מסדר ראשוני $E(F_p)$. (סעיף 6.1.2.3 במסמך ETSI): הסעיף מאפשר שימוש בעקומים אליפטיים סטנדרטיים המתוארים במסמכי FIPS 186-

---

[55] מסמך FIPS 186-3 מתאריך יוני 2009 מחליף את מסמך FIPS 186-2, ונכתב בהתאם להתפתחויות אחרונות בתחום. מסמך ETSI, סעיף 6.1.2.2, אשר נכתב בשנת 2007 (לפני פרסום מסמך FIPS 186-3), מפנה למסמך FIPS 186-2.

[56] ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לעבור למפתחות DSAבאורך L=2048 סיביות החל מסוף שנת 2010. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html

2 ובמסמך brainpool.[57] מסמכים אלו אפשרו שימוש בעקום אליפטי באורך 160 סיביות. מסמך FIPS 186-3 אינו מאפשר יותר שימוש בעקום בגודל זה, והעקום המינימאלי הוא באורך 224 סיביות.

המלצה: ניתן להשתמש בעקומים אליפטיים באורך 160 סיביות רק עד סוף שנת 2010.[58] לאחר תאריך זה יש לעבור לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך ETSI) באורך גדול מ-160 סיביות. יחד עם זאת שימוש בעקומים אליפטיים באורך 160 סיביות יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחסרות ערך לאחר תאריך זה. לגבי חתימות בעלות חשיבות קריטית, אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים, יש לעבור בהקדם האפשרי לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך ETSI) באורך גדול מ-160 סיביות.

- אלגוריתם ECDSAאליפטי מעל שדה מסדר ראשוני $E(F_{2^m})$. זהו אלגוריתם DSA בהתבסס על עקום אליפטי מעל שדה בינארי $E(F_{2^m})$. (סעיף 6.1.2.4 במסמך ETSI): הסעיף מאפשר שימוש בעקומים אליפטיים סטנדרטיים המתוארים במסמכי FIPS 186-2. המלצה: יש לעבוד עם העקומים האליפטיים המוגדרים במסמך FIPS 186-3. ניתן להשתמש בעקומים אליפטיים באורך 160 סיביות רק עד סוף שנת 2010. לאחר תאריך זה יש לעבור לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך FISP 186-3) באורך גדול מ-160 סיביות. יחד עם זאת שימוש בעקומים אליפטיים באורך 160 סיביות יהיה אפשרי רק לחתימות שהן בעלות ערך עד סוף שנת 2016 וחסרות ערך לאחר תאריך זה. לגבי חתימות בעלות חשיבות קריטית, אשר יש חשש שיותקפו על ידי מדינה או ארגון בעל משאבים גדולים, יש לעבור בהקדם האפשרי לשימוש בעקומים אליפטיים סטנדרטיים (לפי מסמך FIPS 186-3) באורך גדול מ-160 סיביות.) גורם מאשר המשתמש בעקומים אליפטיים יהיה חייב לעבור עד סוף שנת 2011 לשימוש במפתח פומבי באורכים המתאימים לצרופים אלה.

- הערה: מסמך ETSI מאפשר להשתמש גם באלגוריתם EC-GDSA מעל חבורה מסדר ראשוני $E(F_p)$, או מעל חבורה בינארית $E(F_{2^m})$. אלגוריתם זה הוא הגרסא הגרמנית לאלגוריתם ECDSA. בכדי לא להרחיב ללא צורך את מסמר האפשרויות לאלגוריתמי חתימה, לא נאפשר חתימות בשיטה זו.

<u>נימוקים להמלצה:</u>

יש לעקוב אחר ההמלצות העדכניות בעולם לגבי חתימות מסוג זה.

יש לעבור לשימוש בעקומים גדולים יותר מאורך של 160 סיביות מהסיבות הבאות:

- עקומים אלו דורשים שימוש בפונקציות גיבוב עם פלט באורך 160 סיביות.

- כמו כן, שימוש בעקומים באורך 160 סיביות ניתן להתקפה על ידי שיטת baby step giant step, בעלות של 2^{80} פעולות ו-2^{80} זיכרון,

[57] http://www.ecc-brainpool.org/ecc-standard.htm

[58] ההמלצה של הרשות לביטחון תקשורת בקנדה, Communications Security Establishment Canada, היא לעקומים באליפטיים באורך 256 סיביות החל מסוף שנת 2010. http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11d-eng.html

<u>אורכי מפתחות בשימוש גורם מאשר (CA)</u>
<u>המלצות:</u>

- גורם מאשר חייב יהיה להשתמש בשיטת גיבוב עם פלט של 256 סיביות לפחות.

- לגבי שיטת החתימה, גורם מאשר חייב יהיה להשתמש באורכי מפתחות שלא יפלו מאלה המאושרים לשימוש כללי. כמו כן, מסוף שנת 2011 יהיה חובה על גורם מאשר להשתמש באחת השיטות הבאות

  - שיטת **RSA** עם מפתח באורך 4096 סיביות לפחות, יש להדגיש שמדובר הן בחתימות על מפתחות של הגורם המאשר (**self signed root**) והן בחתימות על תעודות של משתמשים.

    באפליקציות מסוימות, בהן יש מגבלה על אורך המפתחות בהם ניתן להשתמש, ניתן יהיה להשתמש בתעודות חתומות על ידי מפתח CAבאורך 2048 סיביות, אך זאת רק באישור הרשם.
  - או שיטת **DSA** עם פרמטר **q** באורך 256 סיביות לפחות,

  - או שיטות חתימה מבוססות עקומים אליפטיים באורך 256 סיביות לפחות.

<u>נימוק ההמלצה:</u> שבירה של חתימות המבוצעות על ידי גורם מאשר מאפשרת לזייף חתימה מאושרת של כל גורם אחר. עקב כך יש חשיבות להבטיח ביתר וודאות את בטיחות החתימות של גורם מאשר.

<u>יצור מספרים אקראיים</u>

יצור המפתחות של מערכת החתימה חייב להתבצע בצורה בטוחה. יש לעקוב אחר ההנחיות במסמך FIPS 186-3 לגבי יצור המפתחות ולגבי בחירת מספרים אקראיים המשמשים בתהליך החתימה.

טבלאות מסכמות

שיטות גיבוב

הערות	תוקף	אורך פלט	שיטה
כנראה ישבר בקרוב	עד סוף שנת 2010	160	SHA-1
כנראה יכול להישבר בהשקעה גדולה	עד סוף שנת 2012	160	RIPEMD-160
כנראה יכול להישבר בהשקעה גדולה	עד סוף שנת 2012	160	SHA-224 עם פלט מקוצר ל-160 סיביות
לא ידועות תקיפות	ללא הגבלה	224	SHA-224
לא ידועות תקיפות	ללא הגבלה	256	SHA-256
לא ידועות תקיפות	ללא הגבלה	384	SHA-384
לא ידועות תקיפות	ללא הגבלה	512	SHA-512
לא ידועות תקיפות	ללא הגבלה	512	Whirlpool

שיטות ריפוד

מקור	שיטה
FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)	RSASSA-PKCS1-v1.5
FIPS 186-3 (דומה למסמך PKCS #1 v2.1 ולמסמך ETSI)	RSASSA-PSS

שיטות חתימה

מקור	תוקף	אורך מפתחות	שיטה
ETSI, ECRYPT, Canada	עד סוף שנת 2010 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016	1024	RSA
ETSI, ECRYPT, Canada	ללא הגבלה	2048 סיביות או יותר	RSA
	יש להתכונן למעבר לאורכי מפתחות אלו	4096 סיביות או יותר	RSA
FIPS 186-3	עד סוף שנת 2010 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016	(L=1024,N=160)	DSA
FIPS 186-3	ללא הגבלה	(L=2048,N=224) (L=2048,N=256) (L=3072,N=256).	DSA
ETSI יש להשתמש בשדות המוגדרות במסמך ETSI	עד סוף שנת 2010 ורק לחתימות שהן בעלות ערך עד סוף שנת 2016	160	ECDSA מעל $E(F_p)$
FIPS 186-3 יש להשתמש בשדות המוגדרים במסמך FIPS 186-3	ללא הגבלה	224 או יותר	ECDSA מעל $E(F_{2^m})$

נספח: החולשה בשיטת הגיבוב MD5 ומשמעותה

שיטת הגיבוב MD5 הוצגה בשנת 1992 ומאז הייתה בשימוש נרחב אע"פ שלאורך זמן התגלה חשש לגבי בטיחותה. בשנת 2004 הוצגה שיטה למציאת התנגשויות ב-MD5, כלומר למציאת זוגות קלטים m,m' כך שמתקיים $MD5(m)=MD5(m')$. לאחר מכן שופרו הטכניקות למציאת התנגשויות כך שאפשר יהיה למצוא זוג certificates (תעודה אלקטרונית שהנפיק גורם מאשר, לצורך חתימה מאושרת) בפורמט סטנדרטי, כך שערכי ה-MD5 שלהם זהים. לאחרונה, בסוף שנת 2008, הודגם שניתן להשתמש בערכים מסוג זה בכדי לקבל תעודה אלקטרונית מאחד מה- root CAs של האינטרנט[59]. הדבר מאפשר התקפה רבת עוצמה, בצורה הבאה:

- רוב ה-root CAs אינם משתמשים יותר ב-MD5, אך מספיק לאתר CA בודד המשתמש בשיטה זו.
- יש למצוא זוג תעודות אלקטרוניות, כך שערך ה-MD5 שלהן זהה. אחת מהן היא עבור אתר תמים, השנייה היא לתעודה המסמיכה את בעליה להיות CA בעצמו.
- יש לבקש חתימה על התעודה הראשונה מ-root CA. התוקפים אכן הצליחו לקבל חתימה כזו.
- חתימה זו מהווה גם חתימה על התעודה השנייה, המסמיכה את התוקפים להיות CA. כעת ניתן באמצעות תעודה זו לחתום על תעודות אלקטרוניות נוספות, חתימות אלו אינן חייבות להתבצע בעזרת MD5, אלא באמצעות כל שיטת גיבוב או חתימה שהיא. ניתן לדוגמא לחתום על תעודה המאשרת שיוך של מפתח פומבי מסוים לבנק, או לכל מוסד פיננסי אחר.
- כעת, באמצעות תעודה זו ניתן להתחזות לבעלי המוסד הפיננסי ולזייף אתר אינטרנט האמור לאפשר גישה לאותו מוסד. משתמש שייגש לאתר המזויף יקבל תעודה אשר תעבור את כל הבדיקות של הדפדפן, ויהיה משוכנע שזהו האתר המקורי. (שימו לב שההתקפה משפיעה על כל אתר, ולא רק על אתרים המשתמשים ב-MD5, או בתעודה מה-CA הבודד אשר משתמש ב-MD5).

המסקנה מהתקפה זו היא שניתן לעיתים להפוך חולשות מזעריות בשיטות הקריפטוגרפיות להתקפות של ממש על אפליקציות. לכן יש להימנע שכל שימוש בשיטות חתימה או גיבוב אשר קיים חשש כלשהו לגבי בטיחותן.

59 ראו MD5 considered harmful today, Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, http://www.win.tue.nl/hashclash/rogue-ca/, Dec. 30, 2008.

מידע לגבי ההנחיה

25. **מס' ההנחיה:** 4/2010

26. **נושא ההנחיה:** עדכון אלגוריתמים ואורכי מפתחות לשימוש לפי חוק חתימה אלקטרונית, התשס"א-2001

27. **תאריך פרסום:** 1.7.2010

28. **בתוקף מתאריך:** 1.4.2011

29. **חוקים שאוזכרו**:

א. חוק חתימה אלקטרונית, התשס"א-2001.

30. **חקיקת משנה שאוזכרה**: אין.

31. **פסקי דין שאוזכרו**: אין.

32. **מאמרים שאוזכרו**: אין.

33. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.

34. **הנחיות רשם גורמים מאשרים שאוזכרו**: אין.

35. **מילות מפתח:** אלגוריתמים, אורכי מפתחות, גיבוב (hash), הצפנה אסימטרית, הצפנת מפתח ציבורי, חתימה אלקטרונית, ריפוד (padding).

36. **עדכונים**

גרסה	פרטים	תאריך
.1.1	דחיית תחילת תוקף עד 25.2.2011	2.1.2011
.1.2	דחיית תחילת תוקף עד 1.4.2011	23.2.2011

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

Registration and Supervision Department

מחלקת רישום ופיקוח

תאריך: 30 דצמבר 2010
כ"ג טבת תשע"א
סימוכין: 015-99-2010-005292
תיק: פק 10-699 קומסיין - עמידה בהנחיה 02.2010
באמצעות: דואר אלקטרוני

לכבוד
[רשימת תפוצה – חתימה אלקטרונית]

א.ג.נ.,

הנדון: **<u>דחיית יישום הנחיה 4-2010</u>**

הריני לעדכנכם, בדבר החלטת רשם גורמים מאשרים (להלן – **הרשם**), לפי חוק חתימה אלקטרונית, התשס"א-2001 (להלן – **החוק**), כדלקמן:

1. בהתאם להנחיה 4-2010, נדרשת קומסיין לעדכן את אמצעי החתימה המשמש אותה עד סוף שנת 2010.

2. בשל אי הערכות חברת קומסיין לעמוד בדרישות הנחיה 4-2010 להנחת דעת הרשם, החליט הרשם לדחות את תחילת ההנחיה, בכל הנוגע לאורך המפתחות לחתימה שבשימוש חברת קומסיין עד ליום 25.02.2011.

3. לידיעתכם.

רות ברנר, עו"ד

מחלקת רישום ופיקוח

העתקים:
מר יורם הכהן, ראש הרשות למשפט טכנולוגיה ומידע
מר עמית אשכנזי, רשם גורמים מאשרים
גבי רבקי דביש, מנהלת מחלקת רישום ופיקוח כאן.

קריית הממשלה, ת.ד. 7360, תל אביב 61072, טל' 03-7634050 פקס: 02-5467064
The Government Campus, P.O.Box 7360, Tel Aviv 61072, Israel. Tel: +972-3-7634050 Fax: +972-2-5467064
Email: ilita@justice.gov.il Web: ilita.justice.gov.il

תאריך: 23 לפברואר, 2011
ייט אדר א', תשעייא
סימוכין: 015-99-2011-000740
פק 10-699
באמצעות: דואר אלקטרוני

לכבוד:
[רשימת תפוצה חתימה אלקטרונית]

א.ג.נ.,

הנדון: **<u>דחיית יישום הנחייה 4-2010 ליום 01.04.2011</u>**

הריני לעדכנכם, בדבר החלטת רשם גורמים מאשרים (להלן – **הרשם**), לפי חוק חתימה אלקטרונית, התשסייא-2001 כדלקמן:

1. תחולת הנחייה 4-2010 (להלן – **ההנחיה**) נדחתה מיום 01.01.2011 עקב אי הערכות הגורם המאשר חברת קומסיין להנחת דעת הרשם.
2. במקביל, פנתה חברת קומסיין לרשם, בבקשה שלא להפסיק להשתמש בפונקציית גיבוב SHA-1 בהתאם להנחיה.
3. בתום בירור של נושא זה מול ספקי טכנולוגיה ומול רשמים מקבילים באירופה, ובשים לב לאופי השימוש הגובר בחותימה אלקטרונית, והאיומים בנושא זה בהקשר הישראלי, החלטתי שלא לסטות מחוות דעתו המקצועית של דייר פנקס אשר צורפה להנחיה ומהמלצותיו לעניין השימוש בפונקציה זו.
4. תחולת הנחייה 4-2010 תדחה ליום 01.04.2011.

בכבוד רב,
עמית אשכנזי
רשם גורמים מאשרים ויועץ משפטי
רמו"ט

העתקים:
מר יורם הכהן, ראש הרשות למשפט טכנולוגיה ומידע
מר עמית אשכנזי, רשם גורמים מאשרים
גבי רבקי דבייש, מנהלת מחלקת רישום ופיקוח כאן.

קריית 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) נספח ד' – הנחיית רשם גורמים מאשרים מס' 5-2010

הנחית רשם גורמים מאשרים מס' 5/2010
בדיקת הזהות בפני הגורם המאשר לפי תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

1. כללי

1.1. ביום 7.7.2010 נכנס לתוקפו התיקון[60] לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן - **התקנות**).

1.2. לאחר התיקון, סעיף 10 לתקנות, קובע חלופות למסמך מזהה, הנוסף על תעודת זהות ומידע ממרשם האוכלוסין, באמצעותו יחיד שהוא תושב ישראל יזדהה בפני גורם מאשר לצורך הנפקת תעודה אלקטרונית.

1.3. בין החלופות, ניתן למסור אישור של עורך דין על זהותו של המבקש.

1.4. כמו כן, הרשם רשאי לאשר, מטעמים שיירשמו, מסמך מזהה אחר אשר ישמש את הגורם המאשר בעת אימות זהות.

1.5. מטרת הנחיה זו היא לקבוע את נוסח אישור עורך דין על זהות, וכן להבהיר את אופן הגשת הבקשה לאישור מסמך מזהה על ידי הרשם לפי התקנות.

2. הנחיה

2.1. בהתאם לסמכויות שניתנו לי בסעיף 10 לתקנות, הריני לקבוע כדלקמן:

2.1.1. אישור עורך דין על זהות לצורך תקנה 10(2)(א)(4)(ג) לתקנות יהיה על פי הנוסח שב**נספח א' - נוסח אישור זהות בידי עורך דין**.

2.1.2. פנייה לאישור מסמך מזהה על ידי הרשם לפי תקנה 10(2)(א)(4)(ב) לתקנות תכלול התייחסות לכל הפרטים המנויים ב**נספח ב' - פרטים נדרשים בפנייה לבקש אישור מסמך מזהה**.

2.1.3. מסמך מזהה שאושר על ידי הרשם יתפרסם באתר האינטרנט של הרשם בכתובת: http://ilita.justice.gov.il וברשומות.

[60] תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות) (תיקון), התש"ע-2010. נוסח התיקון התפרסם באתר משרד המשפטים בכתובת: http://www.justice.gov.il/NR/rdonlyres/F2CBAB4E-B377-4B18-B081-CCE36C91DB97/21216/6907.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

<u>נספח א' - נוסח אישור זהות בידי עורך דין</u>

לפי תקנה 10(2)(א)(4)(ג) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

אני הח"מ, עורך דין _____, מס' רישיון _____ שכתובתי _____ ומס' הטלפון שלי הוא _____,

מאשר בזה כי מר/גב'* _____, נושא תעודת זהות מס' _____, אשר תמונתו/ה* מצורפת בזאת וחתומה בידי, מוכר לי אישית ופרטי הזיהוי שלו הם כפי שפירטתי לעיל.

אני מודע לכך כי אישורי זה נועד לתמוך בבקשה להנפקת תעודה אלקטרונית לפי חוק חתימה אלקטרונית תשס"א-2001.

ולראיה באתי על החתום –

היום _____

עו"ד _____

_____
חתימה וחותמת

כאן תצורף תמונה של המבקש עם חתימה וחותמת של עורך הדין, על גביה

_____

* מחק את המיותר

נספח ב' - פרטים נדרשים בפנייה לבקש אישור מסמך מזהה

לפי תקנה 10(2)(א)(4)(ב) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

1. שם הגוף המבקש;
2. שם המסמך המזהה לגביו מתבקש האישור;
3. מסמך רשמי, החתום על ידי בעל התפקיד הבכיר האחראי על הנפקת המסמך המזהה, הכולל פירוט הפרטים הבאים:
   3.1. האם התעודה המונפקת כוללת תמונה ומספר זהות.
   3.2. מקור הסמכות לפיו מופקת התעודה (חוק, תקנות וכו').
   3.3. מהם תהליכי הזיהוי הננקטים על מנת לוודא את זהות מבקש התעודה, ובפרט את עדכניות התמונה.
   3.4. באיזו תדירות מחודשת התעודה, אם בכלל.
   3.5. מה הכללים לגבי הנפקה מחודשת של תעודה במקרה של אובדן או גניבה. האם מבוצע תהליך ההנפקה מחדש.
   3.6. נתונים לגבי המסמך:
      3.6.1. סוג המסמך (תעודה/כרטיס וכד') ופרטים טכניים אודותיו, כולל נתוני המדיה לשמירת/עיבוד נתונים המשולבת בו, אם קיימת.
      3.6.2. הפרטים המודפסים עליו.
      3.6.3. מנגנוני ההגנה מזיוף המשולבים בו, אם קיימים.
4. צילום ברור של דוגמת המסמך המזהה הנדרש לאישור.

מידע לגבי ההנחיה

37. **מס' ההנחיה:** 5/2010

38. **נושא ההנחיה:** בדיקת הזהות בפני הגורם המאשר לפי תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

39. **תאריך פרסום:** 26.7.2010

40. **בתוקף מתאריך:** 26.7.2010

41. **חוקים שאוזכרו**:

א. חוק חתימה אלקטרונית, התשס"א-2001.

42. **חקיקת משנה שאוזכרה**:

א. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

43. **פסקי דין שאוזכרו**: אין.

44. **מאמרים שאוזכרו**: אין.

45. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.

46. **הנחיות רשם גורמים מאשרים שאוזכרו**: אין.

47. **מילות מפתח:** בדיקת זהות, גורם מאשר, הנפקת תעודה, זיהוי, מבקש תעודה, מסמך מזהה.

48. **עדכונים**

גרסה	פרטים	תאריך

5) נספח ה' – סיכום מפגש תקופתי FESA

הנדון: **<u>סיכום מפגש תקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית [FESA]</u>**

1. ב- 13-14.04.2010 התקיים בורשה, פולין המפגש התקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית (Forum of European Supervisory Authorities – FESA), באירוח משרד הכלכלה הפולני והמכון הפולני לחקר המחשבים.

2. ארגון FESA הוקם באופן וולנטרי על ידי החברים, ואינו בעל מעמד רשמי של ארגון דיפלומטי אלא מהווה פורום להחלפת דעות ותיאום עמדות בין רשויות הפיקוח.

3. החל משנת 2007 רשם גורמים מאשרים הישראלי חבר בפורום זה כחבר משקיף, ובשנת 2008 הרשות למשפט טכנולוגיה ומידע אף אירחה את המפגש בתל אביב.

4. במפגש נכחו נציגים של רשויות הפיקוח מהמדינות הבאות: גרמניה, פולין, איטליה, בלגיה, הולנד, צ'כיה, שוודיה, איסלנד, לטביה, פינלנד, יוון, אוסטריה, שוויץ. כן השתתפו נציג נציבות האיחוד האירופי, ושני חוקרים העוסקים במחקרים מטעם הנציבות לקידום המדיניות האירופית, ונציג הרשות האלבנית (שבסוף המפגש נבחר להיות חבר משקיף). בנוסף הוזמנו נציגים של מספר גורמים פרטיים הפעילים בשוק זה להציג את פעילותם. במפגש הנוכחי נדונו מספר רב של נושאים בעלי רלבנטיות לישראל, ובהם עדכונים מנציבות האיחוד על מגמות ההסדרה והחקיקה, קידום סוגיות של תעודות זהות חכמות, הסדרה של רשימה ממוחשבת אחידה כלל אירופאית של "גורמים מאשרים", הצגה של פתרון חתימה המבוסס על טלפונים סלולרים, שירות וידוא תוקף חתימה אירופי ופולני, עדכונים על פעילות התקינה באירופה ובמיוחד על פורמט אחיד למסמכים חתומים וחתימות לטווח ארוך.

<u>א. מגמות ההסדרה ברמת נציבות האיחוד האירופי</u>

5. הטיפול בנושא החתימה האלקטרונית מטופל ביחידת DG Information Society, העוסקת ברגולציה וחקיקה בתחום האינטרנט והתקשורת. לצד הטיפול של DG Information Society, יחידת DG Internal Market, העוסקת בהסדרת השירותים (services), גרמה למהפכה זוטא בתחום זה, בכך שקידמה חקיקה המונעת יכולת שלא לקבל חתימה אלקטרונית לפי הדירקטיבה שהונפקה במדינה אירופאית אחת, במדינה אחרת.[61]

6. התוצאה הישירה של הטמעת מדיניות זו במדינות האיחוד הינה הסרה גורפת של חסמים לשימוש בחתימה אלקטרונית בין מדינות אירופה. החלטה זו נובעת כפי הנראה מסדרת מחקרים שנערכת על ידי מוסדות האיחוד לאיתור חסמים לשימוש בחתימה אלקטרונית (ראו גם להלן).

7. במסגרת הפעילות המשולבת של שני משרדים אלה, אף התקבלה בתום דיונים מרובים בשנת 2009 החלטה של הנציבות המחייבת כל מדינה לנהל רשימה ממוחשבת של הגורמים

[61] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN: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

המוסמכים להנפיק תעודות אלקטרוניות לפי הדירקטיבה. רשימה כזו נועדה ליצור מאגר בפורמט אחיד ובמקום קבוע, שיאפשר בדיקה מהירה ואמינה של מהימנות תעודה אלקטרונית שהונפקה במדינת האיחוד. לצורך תמיכה ברשימה זו נקבע תקן אירופאי המפרט את אופן עריכתה. ההחלטה נכנסה לתוקף בסוף 2009, ולפי הנתונים שנמסרו במפגש, יושמה על ידי רוב מדינות אירופה. בנוסף, הנציבות מרכזת את "רשימת הרשימות" של גורמי האמון האירופאים.

8. יצויין כי במסגרת מאמצנו בשנים 2003-5 להביא להסכמי הכרה הדדית בין ישראל לאיחוד בתחום החתימות האלקטרוניות, התברר כי על אף קיומו של דין אחיד לכאורה באירופה, דה פקטו אין הכרה הדדית בחתימות אלקטרוניות בין מדינות אירופה לבין עצמן, ובשל כך לא היה בסיס לקידום הכרה הדדית ברמת הנציבות עם ישראל.

9. במסגרת המפגש הוצגו לקחים ונתונים אודות המימוש של נושא זה, וכן שאלות לעניין האפשרות שהנציבות תקח על עצמה לרכז את "רשימת הרשימות." אופן עריכת רשימת הרשימות של גורמי האמון, והכללים החלים, רלבנטים מאוד לישראל משום שאם תתאפשר הכרה הדדית ברמה המהותית, הדרך המעשית לממשה היא בפורמט הטכני של עריכת רשימת רשימות זו.

<u>ב. שירותי בדיקת תוקף חתימה/ תעודה</u>

10. במסגרת הדיון המוזמן הציגו שני גורמים מסחרים, אחד גורם מאשר פולני, והשני שירות אירופאי אחר, שירות שהם מציעים לצורך בדיקה של תוקף חתימה על מסמך או בדיקה של תוקף תעודה.

11. שירות זה מאפשר למסתמך לבדוק את תוקף החתימה מול מקור אחד בלבד ומבלי צורך לפנות לכל אחד מהגורמים המאשרים באירופה, בדרך של שאילתא נקודתית פשוטה מול אתר ספק השירות.[62]

12. השירות הוצג במתכונת של שאילתא רגילה דרך דפדפן אינטרנט, וכן באפשרות של מימוש פרוטוקול המבצע את הבדיקה ומחזיר תשובה באופן אוטומטי על בסיס פרוטוקול SOAP.

<u>ד. הסדרה של חתימה אלקטרונית בפורמט התואם את הדירקטיבה האירופית במסמכי PDF</u>

13. מר Julian STERN, ששימש עורך של תקן של מכון התקינה ETSI, בנושא של פורמט PDF חתום בהתאם לדרישות הדין האירופי.[63]

14. במסגרת עבודת התקינה תוקנן אופן השילוב של חתימה אלקטרונית, ומידע אודות תוקפה, בפורמט הסטנדרטי של pdf.

---

[62] ראה: http://www.certum.eu/certum/cert,offer_DVCS_WebNotarius.xml

[63] ראה הודעה לעתונות של etsi: http://www.etsi.org/website/newsandevents/200909_electronicsignature.aspx

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

15. מר STERN הציג את פרקי התקן, בדגש על פרק 4, קביעת מנגנון להוכחת תוקף החתימה גם לטווח ארוך. בתמצית, אף שניתן לבדוק תוקף חתימה סמוך לזמן עריכתה, ככל שמתרחקים ממועד זה, עלולים להיות קשיים לוידוא תוקף החתימה בזמן עריכתה. בנוסף, בשל התקדמות פריצת הצפנות, עולה חשש שמסמכים ישונו לאחר שמנגנון החתימה שלהם כבר אינו חזק דיו (אף שהיה חזק דיו בעת עריכת המסמך).

16. על מנת להתמודד עם קושי זה, תוקנן פתרון המשמר את בדיקת מהימנות החתימה בעת עריכתה, ומאפשר גם לרענן תוקף בדיקה זו באופן שהיא תהיה תקפה באופן קבוע.

מעבר למידע המועיל שנמסר אודות התקן, והעלאת המודעות שלנו לנושא זה, הרלבנטי גם לפרוייקט ארכביאות אלקטרונית שאנו מקדמים, אציין הערה מעניינת של האחראי על הפיקוח בגרמניה, שהציג שיטה חלופית לשמירת תוקף של חתימה המבוססת על תפיסה המכונה כ- chain model.

ה. <u>חיתום זמן</u>

17. במסגרת הדיון הציגו המדינות השונות את האופן שבו הן מסדירות שירותי חיתום זמן, כלומר שירותים שבהם מוצמדת חותמת מהימנה עם זמן המבוסס על מקור זמן מהימן, למסמך כלשהו, וכך מספקת ראיה לקיומו במועד הנטען.

18. נושא זה מתוקנן בתקינה האירופית, אולם לא מוסדר משפטית בכל מדינות האיחוד.

19. בדיון עלה כי במדינות רבות יש הסדר רלבנטי, ושירותים אלה מפוקחים במסגרת הפיקוח על גורמים מאשרים.

20. יתרה מזו, בחלק ממדינות אירופה (גרמניה ואוסטריה), יש חובה שמקור הזמן יתבסס על מקור הזמן הרשמי במדינה – מכון מטאורולוגי.

<u>ו. פתרון חתימה המבוסס על טלפונים סלולרים</u>

21. סוגייה מרכזית המהווה חסם להפצה רחבה של חתימות אלקטרוניות היא שהן מחייבות חומרה מיוחדת, שמטרתה שמירה על אמצעי החתימה, הוא מפתח החתימה הסודי, המשמש לחתימה. בנוסף, במציאות יש קשיים בהטמעה של חומרה כאמור בשל הצורך בתמיכה בהתקנתה, תחזוקה, וממשקיה אל המערכות הסטנדרטיות.

22. נושא זה מאתגר זמן רב את העוסקים בתחום.

23. במסגרת הדיון הציגה חברה איטלקית [aliasLab][64] פתרון המבוסס על ארכיטקטורה שבה חתימתו של החותם מצויה על גבי התקן מאובטח מרכזי, והפעלתו נעשית מרחוק באמצעות הטלפון הסלולרי של בעל החתימה. [הפתרון מכונה SecureCall Sign]. הפתרון של החברה האיטלקית משמש לפרויקטים רגישים של חתימה אלקטרונית באיטליה, ואושר גם על ידי הרשות המפקחת האיטלקית.

[64] www.aliaslab.net

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

24. נושא זה עורר דיון סוער בין החברים, משום שהוא מאתגר את הדרישה הקיימת בדין האירופי, וגם בישראל ל – "שליטה בלעדית" של החותם באמצעי החתימה שלו.

25. העובדה שהחתימה מצויה על גבי שרת מרכזי, ולא בכיס של החותם, מהווה סמרטוט אדום לחלק מהרשויות.

26. אחרים, ביקשו לדעת מהו ההסדר שנקבע בנושא זה, וכיצד בוקר, וזאת משום שתיאורטית ניתן ליצור מערכת של בטוחות שימנעו חששות מפני שימוש לרעה. ככלל ניתן לומר כי רוב הנוכחים בדיון סברו כי עד לתיקון של הדין האירופי, פתרון כאמור אינו קביל. זו לא היתה כמובן גישתו של הנציג האיטלקי.

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