# הרשות למשפט, טכנולוגיה ומידע (רמו"ט)

## דו"ח לשנת 2011

**מדינת ישראל**
משרד המשפטים

הרשות למשפט, טכנולוגיה ומידע (רמו"ט)
דו"ח לשנת 2011
משרד המשפטים



# הרשות למשפט, טכנולוגיה ומידע (רמו"ט)

# 2011

**נובמבר 2012**



**מדינת ישראל**
משרד המשפטים







**הרשות למשפט, טכנולוגיה ומידע (רמו"ט)**
**משרד המשפטים**
קרית הממשלה
רח' בגין 125, קומה 9
ת.ד. 7360
תל-אביב 61072

טל' 03-7634050
ilita@justice.gov.il
ilita.justice.gov.il

ISBN 978-965-92053-0-1

ניתן לקבל עותק אלקטרוני של דוח זה בכתובת ilita.justice.gov.il

משרד המשפטים
המנהל הכללי

## דבר המנכ"ל לדו"ח הפעילות לשנת 2011 - רמו"ט

הדו"ח המסכם את שנת העבודה 2011 ברשות למשפט, טכנולוגיה ומידע מציג את הפעילות המגוונת והייחודית שנעשתה ברשות במהלך שנה זו.

בשנה החולפת פעלה הרשות במספר מישורים, תוך הקפדה על השגת היעדים השוטפים לצד תכנון צופה פני עתיד. בזכות שיתוף הפעולה עם גורמים נוספים במשרד המשפטים, פועלת הרשות בתווך שבין החוק להתקדמות הטכנולוגית המהירה, וכך שומרת על יכולת האכיפה וההסדרה של המדינה בתחומי חיים מתפתחים.

השנה הוכיחה הרשות את חשיבות קיומו של גוף המרכז ידע ויכולת בתחומי הגנת המידע והפשיעה הטכנולוגית. דוגמא בולטת לכך היא ההצלחה בפיצוח "פרשת האגרון", והשתלבותה בקידום החקיקה להגברת אכיפה בתחום הגנת הפרטיות.

הרשות למשפט, טכנולוגיה ומידע תמשיך להתמודד עם אתגרים חדשים בנושאים שבתחום אחריותה. על עובדי הרשות להמשיך ולמלא את תפקידם תוך שמירה על ערכי השירות הציבורי ומשרד המשפטים. כגוף הנותן שירות לציבור, על הרשות להמשיך ולחתור לשיפור השירות.

זה המקום להודות לעו"ד יורם הכהן על שש שנות עבודה ממושכת בתפקידו כראש הרשות. תרומתו לרשות החל מהקמתה, דרך שנות פעילותה הראשונות וכלה בשנת העבודה החולפת, ניכרת בכל תחומי העשייה ברשות. בהזדמנות זו, אבקש גם להודות לכלל עובדי הרשות, ובפרט לכותבי הדו"ח השנתי המפורט. משרד המשפטים והנהלתו מחויבים כתמיד להמשיך בשיתוף הפעולה עם הרשות, על מנת להביא יחדיו לצמיחה, התייעלות, חדשנות ושיפור.

בברכה,

ד"ר גיא רוטקופף

# תוכן עניינים


| | |
|---|---|
| פרק א׳<br>**דבר ראש רמו"ט** | **9** |
| פרק ב׳<br>**עיקרי הדו"ח** | **13** |
| פרק ג׳<br>**סטטוס הקמת רמו"ט** | **17** |
| כוח אדם | 17 |
| מערכת מידע מרכזית ברמו"ט | 18 |
| המעבדה הפורנזית | 18 |
| פרק ד׳<br>**חקיקה ומדיניות צבורית בנושאי משפט וטכנולוגיה** | **21** |
| הצעת חוק הגנת הפרטיות (תיקון מס׳ 12)(סמכויות אכיפה), התשע"ב-2011 | 21 |
| טיוטת תזכיר חוק הגנת הפרטיות (תיקון מס׳...) (צמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולעריכת מסמכים) | 21 |
| חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע | 22 |
| הסדר חקיקתי למסלקה הפנסיונית ותקנות לפיו | 22 |
| השימוש בחתימה אלקטרונית מאובטחת במרשמי תרופות | 23 |
| תקנות מרשם רוקח | 24 |
| הסרת גישה לרשימות לקוחות וחשבונות מוגבלים מאתר בנק ישראל | 25 |
| היבטי פרטיות במנגנון הטעינה של רכב חשמלי - smart grid | 25 |
| ועדת אנגלרד - בחינת פרסום מידע פרטי מזוהה בפסקי דין המפורסמים אלקטרונית | 26 |
| ועדת לבחינה מיסוי רכב על פי שימוש | 26 |
| ועדת רשומות אלקטרוניות | 27 |
| הסדרי שיתוף פעולה עם רגולטורים אחרים | 27 |

פרק ה'

**פעילות בינלאומית של רמו"ט** 29

הכנס הבינלאומי ה-33 של נציבי הגנת מידע ופרטיות 29

קבוצת העבודה WPISP של הארגון לשיתוף פעולה כלכלי (OECD) 29

רשת שיתוף פעולה באכיפה הגנת הפרטיות במידע (GPEN) 30

סיום תוכנית ה-twinning עם רשות הגנת המידע הספרדית (AEPD) 30

תכנית המסגרת האירופית השביעית למחקר FP7 30

פעילות במסגרת FESA 31

פרק ו'

**דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2011** 33

הערות המועצה להגנת הפרטיות לפי סעיף 10א לחוק הגנת הפרטיות 33

מבוא 39

פיקוח 39

מבוא 39

נתונים 39

שיעורי תיקי הפיקוח לפי חתך מגזרי 40

נושאים שנבדקו בתיקי פיקוח 41

תיקי פיקוח נבחרים במגזר הציבורי 42

משרד הביטחון | רשות האכיפה והגבייה | משרד התחבורה - רשות הרישוי | רשות ניירות ערך | עיריית אשקלון

תיקי פיקוח נבחרים במגזר הפרטי והשלישי 46

אתר MAKO.co.il - איסוף מידע מקטינים | חברה קדישא גחש"א תל אביב - יפו והמחוז | סמארט קלאב בע"מ | אדם מילוא בע"מ | גפן מדיקל בע"מ | הראל חברה לביטוח בע"מ | www.nextmodel.co.il - גרטלר דוידוב תקשורת ש"מ | www.informer.co.il | סלקום ישראל בע"מ

הטלת קנסות מנהליים 53

| | |
|---|---|
| **חקירות פליליות** | **54** |
| מבוא | 54 |
| תיק ה"אֶגרוֹן" - גניבת מרשם האוכלוסין והפצתו באינטרנט | 55 |
| תיק מ.נ.ר | 65 |
| **הנחיות רשם מאגרי מידע** | **67** |
| כרטיס חכם בתחבורה ציבורית | 67 |
| מיקור חוץ (outsourcing) | 68 |
| טיוטה: פרטיות והגנת מידע בחוזה הלקוח של חברות הטלפון הסלולארי (רט"ן) | 68 |
| טיוטה: תחולת חוק הגנת הפרטיות על פעולות מכוני מיון לקבלה לעבודה | 69 |
| איסור שימוש במידע בדבר הטלת עיקול אצל צד שלישי | 69 |
| טיוטה: השימוש במצלמות מעקב | 70 |
| טיוטה: הגנה על מידע אישי במקום העבודה - מדריך למעבידים ולעובדים | 70 |
| **רישום מאגרי מידע** | **71** |
| נתונים | 71 |
| גביית אגרות | 71 |
| רישום מאגר מידע לשירות Google Street View | 72 |

פרק ז'

| | |
|---|---|
| **דין וחשבון של רשם גורמים מאשרים לפי תקנה 16 לתקנות חתימה אלקטרונית (ניהול גורם מאשר וניהולו), התשס"ב-2002** | **73** |
| **כללי** | **73** |
| **נתונים** | **74** |
| **גורמים מאשרים רשומים** | **74** |
| **בקשות רישום חדשות של גורמים מאשרים** | **75** |
| חברת פרסונל איי.די בע"מ | 75 |
| הגורם המאשר הממשלתי | 75 |
| **פעולות פיקוח** | **76** |
| הגורם המאשר קומסיין בע"מ | 76 |

| | |
|---|---|
| **הנחיות** | **78** |
| הנחייה 2-2010 | 78 |
| מעקב - מימוש הנחייה 4-2010 - עדכון אלגוריתמים | 79 |
| **אישור חומרה לפי תקנה 2(9)** | **80** |

פרק ח'

**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.** **81**

| | |
|---|---|
| **כללי** | **81** |
| **בעלי רישיונות** | **81** |
| בעלי רישיונות תקפים | 81 |
| ביטול רישיון שירות מידע על עוסקים | 82 |
| שינוי בבעלות, דירקטורים ומנהל שירות | 82 |
| דיווחים על פגם לפי תקנה 80 | 82 |
| **פיקוח על בעלי רשיונות** | **82** |
| נתונים | 83 |
| תיקי פיקוח נבחרים | 83 |

נספח א'

**הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב-2011** **85**

נספח ב'

**מסכים של תוכנת אגרון** **113**

נספח ג'

**הנחית 2/2011 של רשם מאגרי מידע - שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי** **121**

| | |
|---|---|
| **Introductory remarks by head of ILITA** | **i** |
| **Summary of the report** | **v** |

# פרק א' **דבר ראש רמו"ט**

את דברי המצורפים לדו"ח השנתי על אודות פעילות רמו"ט בשנת 2011, אני מבקש להקדיש לחשיבות שרמו"ט מייחסת לאכיפה של עקרונות הפרטיות במידע במסגרת פעילותה הרגולטורית וקידום המדיניות הציבורית לגבי הגנת הפרטיות, נוכח אירועים משמעותיים שקרו במהלך שנה זו.

דיני הגנת הפרטיות במידע (data protection) מיועדים להסדיר את אופן השימוש במידע אישי על אודות אנשים האגור ומעובד במערכות מידע, ולמנוע מראש שימוש לרעה במידע אישי על אודות אדם, אם בידי מי שהורשה כדין לעשות שימוש במידע, ואם בידי מי שכלל אין לו הרשאה כזו. מחד גיסא נקבע עקרון צמידות המטרה והגבלת השימוש במידע למטרה לשמה נאסף המידע ועל בסיס ההרשאה שניתנה לו, ומאידך גיסא נקבעה חובת אבטחת המידע על מי שמנהל את המידע האישי. דיני הגנת הפרטיות במידע מקנים זכויות נוספות לנושאי המידע (data subjects), בעיקר לעניין שקיפות בדבר הליכי איסוף המידע על אודותם. תוכנו של המידע האגור, עדכניותו ונכונותו, והשימוש בו בפועל.

במהלך שנת 2011 עשתה רמו"ט שימוש במגוון כלים רגולטוריים להשגת יעדיה, ובפרט בתחום הגנת הפרטיות במידע, ובהם: פיקוחים לאיתור הפרות של החוק, ייזום וליווי הליכי חקיקה, פעילות בתחום המדיניות הציבורית, חינוך הציבור, פרסום הנחיות, שיתוף פעולה עם רגולטורים אחרים בישראל ושיתוף פעולה עם רגולטורים עמיתים ובעלי עניין אחרים בזירה הבינלאומית.

אכיפה – מנהלית, פלילית או אזרחית–פרטית – היא נדבך מרכזי והכרחי בכל מארג כלים רגולטורי ובכל תחום הדורש הסדרה של רשות מפקחת. בהגנת הפרטיות במאגרי מידע ממוחשבים, מהווה האכיפה אמצעי רגולציה חיוני במיוחד, בשל חשיבותו של הערך המוגן, פרטיות בני אדם, המהווה זכות יסוד חוקתית במדינת ישראל.

אכיפה מנהלית הינה לחם חוקה של רמו"ט מיום הווסדה, והיא נעשית תוך הפעלת סמכויות הפיקוח ונקיטת הסנקציות הקיימות בחוקים השונים שרמו"ט אחראית להפעלתם – חוק הגנת הפרטיות, חוק שירות נתוני אשראי וחוק חתימה אלקטרונית. במהלך שנים אלה שופרה ללא היכר דרך הפעלת סמכויות אלה, בפרט לעניין פיקוח, וכן נרכש הנסיון והידע הנדרשים להטלת עיצומים כספיים לפי חוק חתימה אלקטרונית וחוק שירות נתוני אשראי, וקנסות מנהליים על הפרתן של הוראות פליליות בסעיף 31א לחוק הגנת הפרטיות. ציבור בעלי מאגרי המידע נחשף יותר ויותר לפעולות אכיפה מנהלית של רמו"ט, אל מול עושר איסוף ועיבוד המידע המתרחש בישראל.

למיקומה של פעילות האכיפה הפלילית במסגרת רשות הסדרה ייעודית המתמחה במשמעויות המשפטיות של טכנולוגיות מידע חשיבות מיוחדת, נוכח המורכבות של החקירה הפלילית בנושאים אלה, המחייבים ידע מעמיק בטכנולוגיות מידע, ראיות אלקטרוניות והגנת פרטיות. בשים לב לרמת המודעות הנמוכה של מקבלי החלטות ונושאי תפקידים, כמו גם של כלל הציבור בישראל (אשר הולכת ומשתפרת עם פעילותה של רמו"ט), לאכיפה פלילית משנה תוקף.

הקלות יוצאת הדופן של ביצוע הפרות בתחום הגנת מידע אישי מחייבת קיומה של אכיפה יעילה, אשר תשפיע על כלל השחקנים. עליה להבטיח כי מי שמנהל מידע אישי או מחזיק בו, יפנים במידה מיטבית את התוצאות השליליות הנובעות מהפרה, בין אם על ידו ובין אם על ידי מי שינצל את רשלנותו בשמירה על המידע. היא נדרשת לייצר הרתעה מספקת של עברייני המידע האישי, אשר לאור כשלים באכיפה בעבר לא חששו ממערכת אכיפת החוק, ועליה לגרום להעלאת רמת המודעות של הציבור כולו בישראל לזכויותיו על פי חוק הגנת הפרטיות ולחשיבות קיומן.

בהשוואה לענפי רגולציה אחרים בישראל בהם הגברת האכיפה העלתה את המודעות ואת מידת הציות לחוק (כגון הגבלים עסקיים, ניירות ערך ואיכות סביבה) – קיימת הצדקה מיוחדת להגברת האכיפה של דיני הגנת המידע דווקא, משום שבמקרים רבים הנזק שנגרם כתוצאה מהפרתם, אינו ניתן לתיקון ולעומת זאת הפגיעה בפרטיות קשה, אך לא בלתי אפשרית, לכימות כספי ולפיצוי בגין הנזק.

התשתית הטכנולוגית של עיבוד מידע אישי ממוחשב הופכת מורכבת משנה לשנה, וכך גם התהליכים הכלכליים והעסקיים המניעים את עולם המידע. אלה דורשים תחכום והבנה מעמיקה בטכנולוגיה, מידע וכלכלה. בנוסף להבנה של נפש העבריין וכלי חקירה ותשאול מסורתיים, נדרשת רשות אכיפה מודרנית בהגנת פרטיות ליכולות משלימות שיאפשרו חשיפה של העבריינים המסתתרים מאחורי מיסוך טכנולוגי ואמצעים המשתנים תדיר. חוקר מערכות המידע נדרש להכרות עם הארכיטקטורה של הטכנולוגיה והיכולות שהיא מאפשרת, לצד הבנה מעמיקה של מערכות תפעוליות ומידול תהליכי הליבה בארגונים.

שימוש לרעה במידע אישי ניתן לביצוע בנקל: עלות העתקת מידע דיגיטלי ושמירתו היא אפסית; ניתן להפיצו במהירות ובקלות לציבור בלתי מוגבל; העבריינים מתוחכמים, בעלי הבנה טכנולוגית, ומסוגלים לבצע את פעולות ההעתקה וההפצה המפרות מאחורי מנגנוני הסתתרות דיגיטליים; קשה לאתר עבריינים כאלה, שכן במקרים רבים הם אינם נדרשים לשותפים לעבירה; הרווח הכספי מסחר ושימוש במידע אישי גנוב עשוי להיות עצום; מידע אישי משמש כתשתית מרכזית לביצוע עבירות נוספות, כגון עבירות זיוף והונאה, גניבת קנין רוחני, טרור קיברנטי, פריצות למערכות מידע וכד'.

לא רק שהתועלת משימוש לרעה במידע אישי עשויה להיות גבוהה – קשה במקרים רבים לאתר שימוש כזה, שכן אין מדובר בחפץ ממשי שנגנב. מעת שנפגמה השליטה הבלעדית במידע של בעל הזכות החוקית לשימוש במידע, הנזק שנגרם אינו ניתן לתיקון. פעמים רבות הנפגעים, בעלי המאגרים או נושאי המידע (data subjects) כלל אינם מודעים לדבר השימוש האסור, אף כי הוא עשוי להשפיע על חייהם.

כדי להתמודד עם מורכבות האכיפה הפלילית בתחום המורכב של עבירות מידע אישי, נדרשת רשות האכיפה הייעודית למגוון כלים משפטיים, טכנולוגיים ואנושיים. עליה להחזיק בסמכויות התואמות את אופי העבירות, אשר ברוב המקרים כרוכות גם בעבירות מחשב, כפי הגדרתן בחוק המחשבים, התשנ"ה–1995. היא חייבת לפתח מיומנות בנושא המורכב של ראיות אלקטרוניות, ובפרט כאלה שבבסיסן עומדים מאגרי מידע, לרבות היכולת להפיק ראיות כאלה ברמה הנדרשת במשפט פלילי. עליה להתמחות בסביבה הטכנולוגית בהן מתנהלות עבירות מידע אישי, קרי בסיסי נתונים, יישומי מידע, אינטרנט ואבטחת מידע, ועליה להעסיק חוקרים בעלי מיומנות טכנולוגית והבנה משפטית בנושא הליבה של הגנת הפרטיות, המסוגלים להתמודד עם האתגר האינטלקטואלי אשר מציבים עברייני המידע.

ייחודה של שנת 2011 הינו הצלחת מאמציה של רמו"ט בקידום האכיפה הפלילית בפרטיות במידע, ובפריצת הדרך שהשיגה רמו"ט בתחום זה. הצלחה זו היא קצירתן של פירות ההשקעה של רמו"ט בבניית מחלקת חקירות ייעודית, שמטרתה הגברת האכיפה הפלילית בנושא של פרטיות במידע, ועונה על האפיונים המתוארים.

דוגמא מוחשית לקלות ביצוע הפרות הקשורות למאגרי מידע, לעוצמת הנזק שנגרם ולחוסר האפשרות לתקנו – באה לידי ביטוי בפרשה המתוארת בהרחבה בדו"ח זה – פרשת גניבת מאגר מרשם האוכלוסין של מדינת ישראל והפצתו ברשת האינטרנט (פרשת הָאֶגְרוֹן). בשנת 2011 סיימה מחלקת החקירות הפלילית ברמו"ט את פיצוח פרשת האגרון לאחר חקירה מאומצת שהחלה בשנת 2009, והעבירה את תיק החקירה לפרקליטות מחוז ת"א עם המלצה להעמיד את החשודים לדין. בחודש מאי 2012 הוגש נגד החשודים כתב אישום הכולל עבירות מחוק הגנת הפרטיות, מחוק המחשבים, ומחוק העונשין. הנזקים שגרמה פרשת הָאֶגְרוֹן למדינת ישראל ולאזרחיה רבים וקשים, ודו"ח זה מפרט אותם אחד לאחד.

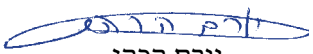
גם בתחום התשתית החקיקתית לסמכויות הפיקוח והאכיפה של רמו"ט, התרחשה בשנת 2011 קפיצת דרך: בשלהי השנה קיבלה הכנסת בקריאה ראשונה את הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2012. הצעת חוק זו שגובשה ביוזמת רמו"ט בשיתוף עם מחלקת ייעוץ וחקיקה במשרד המשפטים, צפויה לקדם את יכולות האכיפה של הנורמות הקבועות בחוק הגנת הפרטיות, התשמ"א–1981 לאתגרים של זמננו.

כפי שעולה מן הדו"ח המצורף, נוקטת רמו"ט בפעילות אכיפה משולבת המתאימה את האמצעים לחומרת ההפרות ולהיקפן: פיקוח מנהלי והטלת סנקציות מנהליות על ההפרות

הקלות והבודדות, לצד שימוש בכלי חקירה פליליים ועניישה מתאימה להרתעה מפני ביצוע עבירות המידע החמורות יותר, וככלי משלים לסמכויות הפיקוח המנהלי.

במהלך השנים הקרובות תמשיך רמו"ט להתמקד באכיפה מנהלית ופלילית של הוראות החוק. מבלי לגרוע מכך, ובשים לב למגבלות המשאבים העומדים לרשותה, מאמינה רמו"ט גם ביעילות ובחשיבותה של אכיפה פרטית, באמצעות המשפט האזרחי, של הוראות החוק. אכיפה פרטית זו מופנית כבר היום אל גופים פרטיים, אך גופים ציבוריים – לרבות מוסדות המדינה – האוספים מידע אישי על אודות האזרחים וחבים בניהול תקין ושמירה על המידע האישי חייבים גם הם להיות נתונים, במקרים הראויים, לסנקציה אזרחית. בהתאם לתפישה זו, תמשיך רמו"ט לנהוג בשקיפות בחשיפתם לציבור של ממצאי הליכי פיקוח שהיא מקיימת ולפרסם הנחיות שיעמידו את הציבור על זכויותיו.

לסיומם של דברים אלה, אבקש להודות לעובדים האיכותיים והמסורים של הרשות למשפט, טכנולוגיה ומידע על העבודה הנפלאה שהם עושים מדי יום, ואשר תוצאותיה מפורטות בדו"ח זה.



יורם הכהן
ראש רמו"ט

# פרק ב' **עיקרי הדו"ח**

דו"ח זה סוקר את פעילותה של רמו"ט במהלך שנת 2011. בשנה זו המשיכה רמו"ט להיבנות, אך טרם הגיעה להיקף כח האדם והמשאבים אשר יועדו לה עם ההחלטה על הקמתה. במהלך השנה הוחל בפיתוח מערכת מידע ייעודית לתמיכה במגוון הפעולות הרגולטוריות של רמו"ט.

לקראת סוף השנה התקבלה בקריאה ראשונה בכנסת הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2012 אשר אמורה להסדיר באופן מודרני והולם את סמכויות האכיפה הנדרשות לפעולתו של רשם מאגרי מידע הפועל במסגרת רמו"ט, או בשמו החדש בהצעת החוק – הממונה על הגנת מידע. נמשכה העבודה על התיקון המשלים לחוק הגנת הפרטיות, והוא שינוי החוק אשר בעקבותיו תצומצם משמעותית חובת רישום מאגרי מידע ויונהג משטר של ניהול תקין של מידע אישי.

בסוגיות שונות של מדיניות ציבורית המשיכה רמו"ט במסגרת שנת 2011 להיות מעורבת ולהשפיע על מהלכים שונים המערבים סוגיות של משפט וטכנולוגיות מידע, כגון: גיבוש הסדר חדש לפרסום מידע אישי על אודות אנשים בפסקי דין במסגרת ועדת אנגלרד; הקמת המאגר הביומטרי במסגרת פרוייקט תעודת הזהות החכמה; המסלקה הפנסיונית להנגשת מידע על אודות חסכון פנסיוני לצורך שיפור מערך הייעוץ הפנסיוני לאזרחי ישראל; שימוש בחתימה אלקטרונית לחתימת מרשמי תרופות, אבטחת המידע במסגרת הנגשת מידע רפואי לרוקחים במסגרת רפורמה לשיפור השירות לחולים כרוניים; סוגיות פרטיות העולות בהקמת רשת חכמה (smart grid) לטעינת רכב חשמלי; יוזמה לבחינת אפשרות שינוי מערך מיסוי הרכב על פי שימוש בפועל; גיבוש מדיניות לאומית לגנז המדינה באשר לשימורן של רשומות אלקטרוניות; פרסום מידע על אודות לקוחות וחשבונות מוגבלים על ידי בנק ישראל.

במהלך שנה זו החלה רמו"ט בבניית הסדרי שיתוף פעולה וקביעת מנגנונים למניעת כפל הסדרה עם רגולטורים אחרים במדינת ישראל להם נגיעה בסוגיות של מידע אישי, כגון הפיקוח על הבנקים בבנק ישראל ואגף שוק ההון באוצר.

במישור הבינלאומי, רמו"ט המשיכה בשנת 2011 להשתתף ולהשפיע על השיח הבינלאומי בסוגיות של פרטיות במידע, וזאת בעקבות המעמד הבינלאומי לו זכתה בשל פעולות רבות בזירה זו, כגון: אירוח הכנס הבינלאומי של נציבי הגנת מידע אישי בירושלים בשנת 2010; קיום תוכנית ה–twinning עם רשות הגנת המידע הספרדית AEPD (אשר הסתיימה בראשית השנה); קבלת ההכרה של האיחוד והפרלמנט האירופיים שרמת הגנת המידע האישי בישראל

תואמת את דרישות הדירקטיבה האירופית להגנת מידע אישי; נציגת ישראל בועדת ICCP (Information, Communication and Computers Policy) של ארגון ה–OECD ובקבוצת העבודה שלה בנושא פרטיות ואבטחת מידע (WPISP – Working Party on Information Security and Privacy); חברה מייסדת ברשת האכיפה הבינלאומית לפרטיות במידע (GPEN – Global Privacy Enforcement Network).

בתחום הפיקוח על פרטיות במאגרי מידע, רמו"ט המשיכה בתהליך שיפור יכולות הפיקוח שלה על בעלי מאגרי מידע ברחבי ישראל. הנושאים המרכזיים אשר עלו בפעולות אלה היו שימוש במידע אישי החורג מהמטרה לשמה נאסף המידע, אי קיום הוראות פרק הדיוור הישיר בחוק הגנת הפרטיות וקיום חובת אבטחת המידע הקבועה בחוק. הדו"ח מפרט תיקי פיקוח של רשם מאגרי מידע במגזר הציבורי (משרד הבטחון, רשות האכיפה והגביה, משרד התחבורה (רשות הרישוי), רשות ניירות ערך, עיריית אשקלון) ובמגזר הפרטי והשלישי, בסקטורים שונים (אינטרנט, שירותי קבורה, דיוור ישיר, מיון והשמת כ"א, רפואה, ביטוח, חוקרים פרטיים, תקשורת). בחלק מהתיקים שהסתיימו בשנת 2011 הוטלו קנסות מנהליים.

האירוע המרכזי של שנת 2011 בפעילות רמו"ט היה פענוחו של תיק הָאֶגְרוֹן, פרשת גניבתו של מרשם האוכלוסין המלא של מדינת ישראל והפצתו באינטרנט. חקירת הפרשה החלה בשנת 2010, עם קבלתן של סמכויות חקירה פליליות למחלקת החקירות של רמו"ט. לאחר חקירה מאומצת, סבוכה ומורכבת, הצליחה מחלקת החקירות של רמו"ט לבסס תשתית ראייתית כנגד ששה אנשים, אשר חברו לגניבתו של מרשם האוכלוסין המלא על אודות 9.2 מליון אזרחי ישראל (חיים ומתים), סחר בו, פיתוח תוכנה לשימוש בו והפצתו ברשת האינטרנט, וזאת בצד עבירות אחרות. פרשת הָאֶגְרוֹן גרמה נזק גדול ביותר, בראש ובראשונה לפרטיות אזרחי מדינת ישראל, אך גם לערכים נוספים, ולפענוחה משמעות רבה לתכלית למענה קמה רמו"ט.

ברמו"ט נוהל בשנת 2011 תיק חקירה פלילי נוסף, שגם עניינו סחר במידע אישי ממקור לא חוקי. תיק זה נוהל בתחילתו כתיק פיקוח מנהלי בגינו הוטלו קנסות מנהליים, אך הנאשם בחר להישפט בגין העבירות שנעשו, ועל כן הפך התיק להליך חקירה פלילי שהועבר לטיפול הפרקליטות.

בשנת 2011 המשיכה רמו"ט לפרסם הנחיות בתחום הגנת הפרטיות, לשם הבהרת הדין בסוגיות קונקרטיות. הופצו הנחיות בנושאים הבאים: פרוייקט הכרטיס החכם בתחבורה ציבורית (כרטיס הרב–קו); מיקור חוץ של עיבוד (processing) של מידע אישי; טיוטה של הנחיה בהקשר של פרטיות והגנת מידע אישי בחוזים של חברות הטלפון הסלולרי; טיוטה של הנחיה באשר לתחולת הוראות חוק הגנת הפרטיות על פעילות מכוני מיון לקבלה לעבודה; איסור שימוש במידע בדבר הטלת עיקול אצל צד שלישי; טיוטת הנחיה לעניין שימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהם.

במהלך שנת 2011 אישר רשם מאגרי מידע לחברת Google להפעיל בישראל את שירות Google Street View, וזאת לאחר שהוסדרו מספר נושאים הקשורים לאופן איסוף הצילומים לשירות, שקיפות ויידוע האזרחים לגבי הצילום, סמכות שיפוט של בתי משפט ישראליים לגבי הפרות של החוק, ככל שיתרחשו ואופן הצגת המידע לציבור משתמשי השירות.

בתחום החתימה האלקטרונית, אושר במהלך שנת 2011 רישומה של חברת פרסונל איי.די. בע"מ כגורם מאשר להנפקת תעודות אלקטרוניות לחתימה אלקטרונית מאושרת בהתאם לחוק חתימה אלקטרונית, התשס"א–2001, לאחר שהחברה עמדה בדרישות החוק ורשם גורמים מאשרים. במהלך השנה נמשך הטיפול בבקשת הרישום של הגורם המאשר הממשלתי המוקם במסגרת פרוייקט "ממשל זמין" במשרד האוצר, ואשר אמור לאפשר ביצוע חתימה אלקטרונית מאושרת לכל אזרח במסגרת פרוייקט תעודת הזהות החכמה. במהלך השנה הוטלו על הגורם המאשר חברת קומסיין בע"מ שני עיצומים כספיים בשיעור של 71,600 ₪ בשל הפרות שונות של החוק והוראות הרשם.

בשנת 2011 הוחל ביישומה בפועל של הנחיה 2–2010, המסדירה את הדרישות הטכנולוגיות, הנוהליות והאבטחתיות של מערך לניהול גורם מאשר לחתימה אלקטרונית. בנוסף, אושר בפעם הראשונה על ידי רשם גורמים מאשרים רכיב חומרה, כרטיס חכם של חברת Athena, כתואם את דרישות החוק באשר להפקתה של חתימה אלקטרונית מאובטחת.

בתחום נתוני האשראי, בוטל, לבקשת חברת לב אמון יזמים, רשיון להפעלת שירות מידע על עוסקים. במסגרת שיתוף פעולה עם בנק ישראל גובש הסדר להפצת קבצים המכילים רשימת מושכי שיקים ללא כיסוי (מושל"כ) לגופים הנדרשים לכך, לצורך סליקת שיקים במסגרת פעילותם העסקית, וזאת לאחר שביוזמת רמו"ט הפסיק בנק ישראל להפיץ מידע זה בקבצים באתר האינטרנט שלו.

# פרק ג' סטטוס הקמת רמו"ט

## כוח אדם

במהלך שנת 2011 נמשכה בניית תשתית כוח האדם ברמו"ט, אך גם בשנה זו לא הושלמה יצירת תקני כוח האדם ואיושם ליעד של 24 עובדי מדינה כפי שאושר על ידי נציבות שירות המדינה ומשרד המשפטים בשלבים הראשוניים של הקמת רמו"ט. בסוף שנת 2011 עמדה מצבת כוח האדם של רמו"ט על 22 איש, מהם ארבעה קבלנים וארבעה מתמחים באופן הבא:

| מחלקה | תקני כ"א (מלאים) | | | | | | הערות |
|---|---|---|---|---|---|---|---|
| | קיימים | | | | מתוכננים | | |
| | סה"כ עובדים | | עובדי מדינה קבועים | | קבלנים ועובדים זמניים | עובדי מדינה | |
| | 2010 | 2011 | 2010 | 2011 | 2010 | 2011 | |
| לשכת ראש רמו"ט | 3 | 3 | 3 | 3 | – | | 4 | בנוסף – בת שירות לאומי |
| מחלקת רישוי ופיקוח | 7 | 10 | 5 | 7 | 2 | 3 | 9 | בנוסף – שני סטודנטים ובת שירות לאומי למוקד אגרות |
| מחלקת חקירות | 6 | 6 | 5 | 5 | 1 | 1 | 8 | |
| מחלקה משפטית | 3 | 3 | 3 | 3 | – | – | 4 | בנוסף – ארבעה תקני מתמחים (עד 2013) |
| סה"כ | 19 | 22 | 16 | 18 | 3 | 4 | 25 | |

במהלך השנה הקצה מנכ"ל משרד המשפטים 8 תקנים להשלמת יתרת התקנים אשר הובטחו לרמו"ט בעת ההחלטה על הקמתה. תקנים אלה אמורים להתממש במהלך השנים 2011–2012.

במהלך שנת 2011 נקלט ברמו"ט מומחה אבטחת מידע ראשון בתקן מלא, בהתקשרות קבלנית דרך מערך ההתקשרויות עם אנשי מחשוב בשירות המדינה. ידע זה, של איש אבטחת מידע מנוסה בטכנולוגיות ובנהלי אבטחת מידע, חשוב מאוד לפעילות רמו"ט כרשות רגולציה שעיקר עיסוקה בסוגיות שונות של אבטחת מידע.

## מערכת מידע מרכזית ברמו"ט

לקראת סוף שנת 2011 הוחל בפיתוח מערכת מידע ייעודית לפעילותה של רמו"ט במגוון פעילויותיה – רישוי ורישום, פיקוח, חקירה פלילית, איסוף מודיעין וניהול מערך הייעוץ המשפטי הפנימי והחיצוני.

מערכת זו נבנית על בסיס תהליך אפיון מקיף של תהליכי העבודה ברמו"ט והצרכים הנוכחים והעתידיים שלה כרשות הסדרה שמרכז עיסוקה הוא הגנת מידע אישי בפורמט אלקטרוני. גרסה ראשונה של המערכת צפויה לעמוד לרשות רמו"ט במהלך חודש אוקטובר 2012.

בגרסאותיה העתידיות, תכיל המערכת ממשק אינטרנטי ישיר בין הציבור לרמו"ט באמצעות פורטל מקוון, אשר יאפשר לציבור לקיים את חובות הרישום, הרישוי והדיווח מכוח החוקים השונים שרמו"ט אמונה על יישומם ואכיפתם על פי מתודת "ממשל זמין".

## המעבדה הפורנזית

במהלך שנת 2011 חלה התקדמות רבה בהקמתה של המעבדה הפורנזית, והיא מילאה תפקיד מרכזי בחקירת פרשת גניבת מרשם האוכלוסין, המפורטת בדו"ח רשם מאגרי מידע להלן. במהלך החקירה נתפסו ונחקרו עשרות רבות של מחשבים ומאות תקליטורים (CD/DVD), כוננים קשיחים (hard disks) ואמצעי אחסון מידע דיגיטלי ניידים אחרים (disk-on-key, טלפונים וכד') בהיקף של כ– 70 טרה בייט (Terra Byte).

ניתוח המידע הביא למציאת מקורות המידע הגנוב וזיהוי הפעולות אשר בוצעו לעיבוד ולטיוב המידע. במהלך ניתוח מאגרי המידע, ביצעו החוקרים במעבדה השוואות בין קבצי מאגרים שונים והתחקו אחר מחזור החיים של המידע שנתפס. באופן זה, התגלו במאגרים אלה שכבות המידע השונות שהיו חומרי הגלם המקוריים של מאגרי המידע הבלתי חוקיים.

המעבדה הפורנזית מכילה אמצעים לניתוח ולהפקה של ראיות דיגיטליות ולחקירת מאגרי מידע ובסיסי נתונים שונים על תשתית של מערכות וירטואליות. תשתית זו מאפשרת לחוקרים

לשחזר קבצים שנמחקו או שובשו על ידי החשודים, וכך הצליחה המעבדה הפורנזית לשחזר שרידי מידע בעלי חשיבות ממשית לביסוס האישומים. במעבדה ניתן להקים סביבות עבודה ממשיות מתוך מחשבים וקבצים שנתפסו במהלך פעילות האכיפה של רמו"ט, וכך לאפשר לחוקר המחשב לבחון את המידע הדיגיטלי מנקודת מבטו של החשוד ולדמות פעילות רגילה ויומיומית אותה ביצע החשוד במחשבו.

בנוסף, מאפשרת המעבדה הפורנזית כלים לחקירת קוד תוכנה ייחודי שנכתב על ידי חשודים. חקירת הקוד מאפשרת להוכיח כי התוכנה המקורית מיועדת לפעילות במאגר המידע הלא חוקי ואף מציגה את המורכבות החבויה בתוך פרטי המידע של המאגר. בעותקי התוכנות ובמאגרי מידע שנתפשו בוצעו פעולות חקירה מתקדמות של רמו"ט לניתוח המידע וזיהוי הפרות ועבירות.

# פרק ד' חקיקה ומדיניות צבורית בנושאי משפט וטכנולוגיה

## הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב-2011

הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2012, גובשה ביוזמת רמו"ט עם מחלקת ייעוץ וחקיקה במשרד המשפטים, והיא אמורה לקדם את יכולות האכיפה של הנורמות הקבועות בחוק הגנת הפרטיות, התשמ"א–1981 לאתגרים של זמננו.

בתחילת שנת 2011 נוהל מו"מ בעניין תחולת החוק גם עם גופים ממערכת הביטחון, עד לקבלת ההחלטה להחריג, בשלב זה, מתחולת התיקון את גופי הביטחון המנויים בסעיף 19 לחוק העיקרי.

ההצעה הובאה לראשונה לועדת השרים לענייני חקיקה ביום 27.3.2011 והדיון בה נדחה לאור התנגדות המפקח על הבנקים, שדיונים עימו נערכו מאז תחילת 2011.

הצעת החוק פורסמה ברשומות ב–16.11.2011, לאחר שאושרה בועדת השרים לחקיקה ביום 5.6.2011. ביום 28.11.11 התקבלה הצעת החוק במליאת הכנסת בקריאה ראשונה. הצעת החוק אמורה להידון בכנסת במהלך שנת 2012. נוסח הצעת החוק מצ"ב כנספח א' לדו"ח.

## טיוטת תזכיר חוק הגנת הפרטיות (תיקון מס'...) (צמצום חובת הרישום וקביעת חובה לקיום סדרי ניהול וכללי עבודה ולעריכת מסמכים)

בחודש יולי התחדשו הדיונים עם מחלקת יעוץ וחקיקה על טיוטת תזכיר החוק, אשר אמור לעדכן את משטר הרגולציה של הגנת מידע אישי, ולהשלים את מהלך השינוי ברגולציה של הגנת פרטיות במידע אשר החל בתיקון סמכויות האכיפה האמור לעיל.

עיקרו של התזכיר המוצע הוא צמצום משמעותי של חובת הרישום של מאגרי מידע על פי המלצות דו"ח שופמן והנסיון שנצבר ברמו"ט בהפעלת סמכויותיו השונות של רשם מאגרי מידע, במקביל לקביעת חובות "ניהול תקין" של מידע אישי על בעלי מאגרי מידע כהגדרתם בחוק.

עד לסוף שנת 2011 הושגה התקדמות ממשית בגיבוש התזכיר, אולם טרם הופץ תזכיר בנושא לתגובות הציבור.

## חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע

בשנת 2011 המשיכה רמו"ט ללוות מהלכים שונים הקשורים ביישום חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009 והפעלתו הצפויה.

במסגרת זו נדרשה התקנת תקנות העוסקות באופן נטילת המידע הביומטרי (תקנות הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התשע"א־2011), וכן ניסוח צו המסדיר את קיום תקופת המבחן (פיילוט) לפי החוק (צו הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, (תקופת מבחן), התשע"א־2011). רמו"ט הציגה למשרד הפנים ולמחלקת ייעוץ וחקיקה במשרד המשפטים את עמדותיה בעניין זה, וחלקן התקבלו וייושמו בנוסח אשר התקבל. בנוסף, השתתפו נציגי רמו"ט בדיוני הכנה ובדיוני ועדת הכנסת בנושא.

בנוסף לכך, העבירה רמו"ט למשרד הפנים בחודש אוגוסט 2011 טיוטה של תקנות בנושא תפקידיו של הממונה על הגנת הפרטיות במאגר הביומטרי, תפקיד שהוגדר בפעם הראשונה בחקיקה זו ביוזמת רמו"ט.

## הסדר חקיקתי למסלקה הפנסיונית ותקנות לפיו

בשנת 2011 נערכו מספר סבבי דיונים עם אגף שוק ההון, ביטוח וחסכון במשרד האוצר לצורך התקנת תקנות הפיקוח על שירותים פיננסיים (ייעוץ, שיווק ומערכת סליקה פנסיוניים) (אבטחת מידע במערכת סליקה פנסיונית מרכזית), התשע"ב–2011 שנועדו לקבוע את ההוראות שחלות על המסלקה הפנסיונית ועל המשתמשים בשירותיה.

תקנות אלה מפרטות החובות החלות על מי שינהל מערכת סליקה פנסיונית מרכזית, ובין היתר קובעת חובות בנושאים הבאים:

- קביעת מדיניות אבטחת מידע למערכת הסליקה
- מינוי של ממונה על פרטיות ואבטחת מידע
- כתיבת נוהל אבטחת מידע
- מיפוי רכיבי המערכת וביצוע סקר סיכונים לגביהם
- עקרונות עיצוב לפרטיות במסלקה (privacy by design)
- האבטחה הפיזית וניהול כח האדם המועסק במסלקה

- הרשאות הגישה, זיהוי העובדים ותיעוד גישה ואירועי אבטחה
- אבטחת תקשורת
- שימוש בהתקנים ניידים
- ביקורות תקופתיות
- גיבוי, התאוששות והמשכיות עסקית
- זיהוי משתמשים ולקוחות
- תיעוד המידע שהועבר ומתן זכות עיון לנושאי המידע
- מעמדו הראייתי של פלט במערכת המסלקה הפנסיונית

רמו"ט היתה מעורבת בניסוח התקנות, וכן בשילוב מנגנוני שמירה על הפרטיות ומנגנוניים כגון זיהוי חזק, אמצעי בקרה, וחובת מינוי ממונה אבטחה ופרטיות במסלקה ובארגונים המתחברים למסלקה שיש בהם יותר מ–10 עובדים.

## השימוש בחתימה אלקטרונית מאובטחת במרשמי תרופות

בשנת 2011 יזם משרד הבריאות תיקון תקנות הרופאים (מתן מרשם), התשמ"א–1981, כך שתתאפשר הנפקת מרשמים אלקטרונים לתרופות, אשר ייחתמו על ידי רופאים בחתימה אלקטרונית מאובטחת, כמשמעותה בחוק חתימה אלקטרונית, התשס"א–2001 כתחליף לעריכת המרשמים בנייר וחתימה פיזית עליהם.

כזכור, ההבדל בין חתימה אלקטרונית מאובטחת לחתימה אלקטרונית מאושרת נובע בין היתר מהעובדה שחתימה מאושרת מלווה בתעודה אלקטרונית שהונפקה על ידי גורם מאשר, המשמש כצד שלישי נאמן על הצדדים. בהתאם לכך, נקבע בחוק הסדר הגבלת אחריות המאפשר למי שנפגעה שליטתו בחתימה האלקטרונית להודיע על כך לגורם המאשר, ולא לחוב באחריות בגין שימוש לרעה לאחר מכן.

נושאים אלה אינם מוסדרים ישירות בחתימה אלקטרונית מאובטחת. בנוסף, המטרה המרכזית של יוזמת משרד הבריאות היא חתימה של רופא על מרשמים, בשם ארגון בריאות (כגון קופת חולים או בית חולים), כך שאין מדובר בחתימה אישית של אדם, אלא בחתימתו מכח תפקידו בארגון הבריאות.

יוזמה זו חייבה לאפשר הסתמכות על מערך ניהול הזיהוי וההרשאות הפנימי של ארגוני הבריאות השונים (בפרט קופות חולים ובתי חולים) תוך התחשבות באינטרסים של הרופאים החותמים. על כן, נקבעו בתקנות הוראות בנושא הסדרה של מערכי ניהול הזהויות בארגוני

הבריאות לצורך הנפקת אמצעים לחתימה אלקטרונית מאובטחת לרופאים. כך יכול ארגון בריאות להקים לעצמו מערך ניהול זהויות המיישם את היתרונות של חוק חתימה אלקטרונית, מבלי הצורך בהסתמכות על גורם חיצוני כגורם מאשר, ותוך קביעת הוראות שמטרתן ביצוע פעולות אלה בהתאם לדרישות החוק.

בהתאם לכך, התקנות מסדירות את הליך זיהוי הרופא מנפיק המרשם, ומגבלות על אחריותו לשימוש בחתימה האלקטרונית. על מנת לסנכרן הסדר זה עם ההסדרה של ניהול גורם מאשר (המנפיק תעודות לחתימה אלקטרונית מאושרת), נקבע בתקנות כי ההוראות שמנכ"ל משרד הבריאות יקבע לעניין ניהול מערכי ניהול הזהויות האלקטרוניות של מנפיקי המרשמים במערכת הבריאות, יקבעו לאחר התייעצות עם רשם הגורמים המאשרים.

רמו"ט ליוותה את הליך ניסוח התקנות במשותף עם משרד הבריאות ומחלקת ייעוץ וחקיקה (אזרחי). לאחר התקנתן העביר מנכ"ל משרד הבריאות אל הרשם סט נהלים מוצע, ולגביו הועברו הערות על ידי הרשם. ההערות התקבלו ויושמו בנוהל מתוקן במהלך 2012.

## תקנות מרשם רוקח

בהתאם למדיניות הממשלה הוחלט על קידום אפשרות הסמכה של רוקח בכיר, להנפיק מרשמים לחולים כרוניים. לצורך כך, נדרש הרוקח הבכיר לגשת לתיק הרפואי של הלקוח טרם הנפקת המרשם. דרישה זו מעלה סוגיות של פרטיות במידע, אבטחת מידע. בנוסף, נדרש לאפשר כי הרוקח הבכיר יוכל לחתום על המרשם בחתימה אלקטרונית, בהסדר דומה לזה שנקבע לעניין חתימת מרשמים על ידי רופאים.

רמו"ט שותפה בתהליך, והציעה למשרד הבריאות הסדר מקיף בתחום אבטחת המידע הרפואי שמטרתו מניעת שימוש לרעה במידע הרפואי בשל נגישותו לאלפי רוקחים. נוסח ההצעה תוקן באופן שארגון הבריאות שמנהל את התיק הרפואי ינהל את הגישה למידע תוך יישום אמצעים שמטרתם צמצום שימוש לרעה בידי משתמש הקצה. באופן כללי נדרש כי ההתקשרות אל מערכות המידע של ארגון הבריאות תעשה באופן שהמידע לא יוצא ממערך המידע של ארגון הבריאות, הוא לא יישמר בתחנה המקומית של הרוקח, והרוקח יזוהה באמצעות זיהוי חזק מול המערכת. בהצעה זו יושמה, שוב, תפישת ה"עיצוב לפרטיות" (privacy by design) אשר מקדמת רמו"ט מזה מספר שנים. בנוסף, נדרש ביצועו של סקר סיכונים מקיף לאיתור הסכנות למידע.

בהיבט של חתימה אלקטרונית על המרשמים, תקנות אלה כוללות הוראות דומות להוראות ששולבו בתקנות הרופאים (מתן מרשם) כמתואר לעיל.

## הסרת גישה לרשימות לקוחות וחשבונות מוגבלים מאתר בנק ישראל

לאור פניית רמו"ט והנחיית המשנה ליועץ המשפטי לממשלה (אזרחי), ולאחר דיונים ממושכים, הפסיק בחודש יוני 2011 בנק ישראל לפרסם באתר האינטרנט שלו את הקובץ המלא של חשבונות הבנק והלקוחות המוגבלים שהם יחידים ולאפשר גישה למידע בשאילתה ספציפית בלבד.

להפסקת פרסום הקובץ באינטרנט קדם הליך שימוע שאיפשר לגופים בעלי אינטרס לגיטימי להגיש לבנק בקשה להמשיך ולקבל את הקובץ באופן ישיר.

רמו"ט ליוותה את בנק ישראל לאורך כל משך ההליך, ובכלל זה בחנה את הבקשות שהוגשו, המליצה לבנק ישראל אילו מהן ניתן לאשר, וקבעה את התנאים המפורטים להיתר להמשך השימוש בקובץ המלא.

עד לסוף 2011 סיימה רמו"ט את הטיפול במרבית הבקשות מתוך למעלה מ– 60 שהוגשו.

## היבטי פרטיות במנגנון הטעינה של רכב חשמלי - smart grid

רמו"ט פנתה למשרד התשתיות והפנתה תשומת לבו לכך שעקרונות המדיניות להפעלת רכב חשמלי בישראל מיום 15.02.2011 ואשר גובשו על ידיו, דורשים הפעלת רשת חשמל חכמה. רשת חכמה מחייבת, לכאורה, הקמת מאגר מידע ואיסוף מידע אישי מכל צרכן אשר יהיה מעוניין להשתמש ברשת על מנת לטעון את רכבו.

רמו"ט הפנתה את תשומת לב משרד התשתיות לכך שמוטב לבחון ולנמק בשלב עיצוב המדיניות את הצורך באיסוף מידע אישי במסגרת קידומה. במקביל נדרש המשרד לבחון חלופות המאפשרות קיום תכליות הפרוייקט תוך צמצום או מיזעור החשש לפגיעה בפרטיות, למשל בדרך של אנונימיזציה חלקית או מלאה של הפרטים, או שימוש בפתרונות טכנולוגים מקובלים אחרים בנושא זה.

יצויין כי נושא רשת חכמה הוא כר נרחב לפעילות עיצוב לפרטיות (Privacy By Design), המתאימה מאוד ליוזמה זו.

## ועדת אנגלרד
## - בחינת פרסום מידע פרטי מזוהה בפסקי דין המפורסמים אלקטרונית

במהלך שנת 2011 החלו דיוניה של ועדה אשר מינה שר המשפטים, בראשות השופט בדימוס פרופ' יצחק אנגלרד, לבחינת ההסדר הראוי לפרסום פסקי דין בפורמט אלקטרוני נוכח תלונות הולכות ורבות של אזרחים על אודות פגיעה בפרטיותם הנגרמת בשל יכולות אחזור המידע במדיה אלקטרונית.

ראש רמו"ט משמש כחבר הועדה.

הוועדה בוחנת את האיזון הראוי בין עקרון פומביות הדיון, לעניין הליך פרסום פסקי דין ופרוטוקלי דיונים בבתי המשפט בפורמט אלקטרוני ומתן יכולת אחזור מידע full-text לגביהם מחד גיסא, והגנת הפרטיות במידע מאידך גיסא. יכולות אחזור המידע הנ"ל, אשר קיימות במנועי איתור מידע משפטי ייעודיים כגון "תקדין" ו"נבו", או במנועי חיפוש כלליים כגון google, מאפשרות איתור מידע על אודות שם אדם, בין אם הופיע בפסק הדין כצד להליך, כעד בו או כנשוא הדיון. לעיתים פסקי הדין מכילים מידע אישי רגיש, כגון מידע רפואי בתיקי נזיקין. בהקשר של דין פלילי, הפרסום המזוהה פוגע בעקרון הקבוע בחוק המרשם הפלילי ותקנת השבים, התשמ"א- 1981, שכן מאגרי המידע המשפטיים מכילים פסקי דין ישנים יותר מתקופת ההתיישנות הקבועה בסעיף 14 לחוק זה.

ועדה זו עוסקת, בפעם הראשונה בישראל, בשאלת ה"זכות להשכח" (The Right to Oblivion), שהיא אחד מהנושאים המטרידים את העוסקים בעולם הפרטיות נוכח האגירה אשר כמעט אינה מוגבלת בנפח ובזמן של מידע על אודות אנשים במאגרי מידע.

## ועדת לבחינה מיסוי רכב על פי שימוש

במהלך שנת 2011 החלו הדיונים של ועדת מומחים ממשלתית אשר בוחנת את האפשרות לשנות את מודל המיסוי על כלי רכב באופן שיגלם את השימוש בפועל בכלי הרכב וההשפעות שלו על עומסי תנועה וזיהום אויר.

מאחר ויוזמה כזו כרוכה, בדרך כלל, באיסוף מידע על אודות השימוש בפועל בכלי הרכב על ידי האזרחים, בקשה רמו"ט להיות נוכחת בדיוני הועדה וראש רמו"ט משתתף בה במעמד של משקיף.

במהלך דיוני הוועדה הוכנסו, בעצת רמו"ט, שיקולי פרטיות לתהליכי הניתוח והבחינה של היוזמה, לרבות במסגרת ניסוי אשר יתקיים בנושא. רמו"ט תלווה את התהליך עד לגיבוש ההמלצות הסופיות.

## ועדת רשומות אלקטרוניות

במהלך שנת 2011 התחדשו דיוניה של ועדת ההיגוי הממשלתית לנושא רשומות אלקטרוניות, אשר אמורה לגבש את ההסדר הראוי לשימור ארכיוני של רשומות אלקטרוניות הנוצרות במסגרת השירות הציבורי.

ראש רמו"ט הוא חבר בוועדה.

מטרת ועדה זו לשמש כועדת היגוי לתהליך אשר משנה את אופן הפעולה של גנז המדינה, אשר אחראי מכוח חוק הארכיונים, התשט"ו–1955 על ההבטים הארכיוניים של מסמכים הנוצרים בגופי המדינה השונים. המציאות היום–יומית היא שכמויות עצומות של מסמכים ומידע נוצרים בגופי מדינה באופן דיגיטלי – באמצעי תקשורת מקובלים כגון דואר אלקטרוני, באמצעי ייצור מסמכים כגון מעבדי תמלילים, ובבסיסי נתונים רבים המשמשים את השירות הציבורי.

היקף מידע כזה בפורמט דיגיטלי מעלה, מטבע העניין, שאלות של פרטיות במידע, אך עוסק גם בנושאים נוספים הקשורים לתחום עיסוקה של רמו"ט, כגון ראיות אלקטרונית, חתימה אלקטרונית, חופש מידע אלקטרוני וכד'.

## הסדרי שיתוף פעולה עם רגולטורים אחרים

בחודש מאי 2011 שלחה רמו"ט למפקח על הבנקים בבנק ישראל (להלן – הפיקוח על הבנקים), ולממונה על אגף שוק ההון, הביטוח והחסכון במשרד האוצר (להלן – הפיקוח על שוק ההון), טיוטות של הסכמים לשיתוף פעולה (memorandum of understanding) בינם לבין רמו"ט.

מטרת טיוטת ההסדרים להתוות את מסגרת העבודה בין רמו"ט לבין הפיקוח על הבנקים ובין רמו"ט לפיקוח על שוק ההון. רמו"ט זיהתה כי נדרש שיתוף פעולה ותקשורת בעניינים שהם בעלי עניין הדדי לה ולרגלטורים אלה, כמו גם נדרשת הסדרת הטיפול במקרים שבהם ישנה חפיפה בין הסמכויות ותחומי הפעילות של רמו"ט ובין אלה שלהם. תחומים אלה הם בעיקרם בסוגיות של הגנת הפרטיות ואבטחת מידע במאגרי מידע בגורמים המפוקחים על ידי אותם רגולטורים, במקביל לסמכותו הכללית של רשם מאגרי מידע, הפועל במסגרת רמו"ט.

מזכרי ההבנה יושמו במהלך שנת 2011 בהליכים שונים הקשורים לגיבוש הנחיות רמו"ט בנושא הגנת פרטיות במידע.

# פרק ה' פעילות בינלאומית של רמו"ט

## הכנס הבינלאומי ה-33 של נציבי הגנת מידע ופרטיות

בסוף חודש אוקטובר 2011 השתתפה משלחת של רמו"ט בראשות ראש רמו"ט בכנס הבינלאומי ה-33 של נציבי הגנת מידע אישי ופרטיות אשר נערך במקסיקו-סיטי, מקסיקו. לעניין זה יש להזכיר כי הכנס בשנת 2010 (בו הוחלט גם כי הכנס ב-2011 ייערך במקסיקו) אורח על ידי רמו"ט בירושלים, והיה העוגן המרכזי באירועי שבוע הפרטיות במידע (25-29/10/2010).

ראש רמו"ט השתתף במושב המרכזי ביום השני של הכנס אשר עסק בחשיבות ובמורכבות של אבטחת מידע בהקשר של הגנת הפרטיות.

הכנס נערך מספר ימים לאחר הפרסום הפומבי של תוצאות חקירת גניבת מרשם האוכלוסין (ראו להלן בפרק הדיווח של רשם מאגרי מידע), וראש רמו"ט וסגן מנהל מחלקת חקירות עו"ד אריאל שהם הציגו את השתלשלות האירוע והפרטים הפומביים של החקירה לקהילה הבינלאומית בכנס.

## קבוצת העבודה WPISP של הארגון לשיתוף פעולה כלכלי (OECD)

ראש רמו"ט משמש נציג ישראל בקבוצת העבודה WPISP – Working Party on Information Security and Privacy, וכן נציג ישראל (בשיתוף עם משרד התקשורת) בועדת ICCP – Information, Communication and Computers Policy, של הארגון לשיתוף פעולה כלכלי (OECD).

WPISP עוסקת בסוגיות של פרטיות במידע, אבטחת מידע ו-cybersecurity, תוך מתן דגש על ההיבטים הכלכליים שלהם.

בישיבת WPISP מספר 31, אשר נערכה בדצמבר 2011 בפריס, נבחר ראש רמו"ט יורם הכהן, לשמש כסגן-נשיא של קבוצת העבודה WPISP. בנוסף, משמש ראש רמו"ט כסגן ליו"ר קבוצת המומחים אשר בוחנת את העדכון הנדרש בהנחיות ה-OECD משנת 1980 בנושא של הגנת פרטיות במידע והעברות מידע בין-לאומיות.

## רשת שיתוף פעולה באכיפה הגנת הפרטיות במידע (GPEN)

רמו"ט חברה בצוות המייסד של רשת שיתוף הפעולה הבינלאומי לאכיפת הגנת הפרטיות במידע (GPEN – Global Privacy Enforcement Network). לשיתוף פעולה בינלאומי באכיפת פרטיות במידע חשיבות גבוהה, שכן עיקר פעולות איסוף המידע האישי והשימוש בו נעשה באמצעות תשתית האינטרנט ועל ידי חברות בינלאומיות, או חברות לאומיות הפועלות במרחב הוירטואלי. בנוסף, אתגרי האכיפה של פרטיות במידע הינם דומים ברוב המדינות הדמוקרטיות, בהן לפרטיות מעמד של זכות יסוד חוקתית. מהטעם הזה יש צורך ממשי בשיתוף פעולה בין הרשויות השונות העוסקות בנושא ברחבי העולם, הן משיקולים של אפקטיביות אכיפתית והן משיקולים של הקצאה יעילה של משאבים.

בפגישת GPEN שנערכה בשולי הכנס הבינלאומי של רשויות הגנת מידע אישי ופרטיות במקסיקו באוקטובר 2011, הציגה רמו"ט תובנות בנושא אכיפה פלילית של הגנת פרטיות במידע, אשר עלו מחקירת גניבת מרשם האוכלוסין והפצתו באינטרנט (ראו להלן בפרק הדיווח של רשם מאגרי מידע).

על GPEN ניתן לקרוא באתר האינטרנט של הרשת https://www.privacyenforcement.net

## סיום תוכנית ה-twinning עם רשות הגנת המידע הספרדית (AEPD)

בתחילת שנת 2011 הגיעה לסיומה המוצלח תוכנית ה-twinning לחיזוק רמת ההגנה על מידע אישי בישראל, שקיימה רמו"ט עם רשות הגנת המידע הספרדית (AEPD) במימון הנציבות האירופית. על התוכנית ניתן לקרוא בדו"חות השנתיים הקודמים של רמו"ט.

## תכנית המסגרת האירופית השביעית למחקר FP7

תכנית המסגרת האירופית השביעית למחקר (FP7) היא תכנית רב שנתית המשמשת מסגרת למימון מחקרים באירופה ובמדינות נוספות, בתקציב רב שנתי כולל בסך 50 מיליארד אירו. התכנית פתוחה בפני חוקרים באקדמיה, חברות מסחריות וגופים ציבוריים.

לפי תנאי תכנית המסגרת, פרויקטים המבקשים לקבל את מימונה נדרשים, בין השאר, לעבור בדיקה אתית וכן להציג אישורים של רשויות הגנת המידע (Data Protection Authority) בכל אחת מן המדינות הרלבנטיות – בדבר עמידה בהוראות חוקי הגנת הפרטיות המקומיים. בשנת 2011 החלה רמו"ט בשיתוף פעולה עם ISERD, המנהלת הישראלית לתכנית המסגרת האירופית. במסגרת זו ניסחה רמו"ט טופס בקשה לקבלת אישור כאמור ונדרשה לחוות דעתה בדבר היבטי הגנת המידע של מספר פרוייקטים בהם נטלו חלק שותפים ישראלים.

כמו כן, בחודש ספטמבר השתתף נציג רמו"ט בסדנת עבודה בנושא "Ethical issues in Security Research – a practical approach" שאורגנה בידי תחום מחקרי הביטחון ב– REA (Research Executive Agency) – סוכנות של נציבות האיחוד האירופי המנהלת את תכנית המסגרת. במסגרת הכנס הוצגה סקירה כללית של שיטת המשפט הישראלית ושל משטר הגנת הפרטיות והמידע הנובע ממנה, תוך שימת דגש על הדמיון בינה לבין משטר הגנת המידע האירופי והחלטת הנציבות האירופית לפיה ישראל מספקת רמת הגנה נאותה למידע אישי (adequacy).

## פעילות במסגרת FESA

ב–12–13.04.2011 התקיים בשטוקהולם, שוודיה, המפגש התקופתי של רשויות הפיקוח האירופאיות על חתימה אלקטרונית (Forum of European Supervisory Authorities – FESA), באירוח הרשות השבדית לטלקומוניקציה ולדואר (Swedish Post and Telecom Agency).

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 חבר בפורום זה כחבר משקיף, ובשנת 2008 הרשות למשפט טכנולוגיה ומידע אף אירחה מפגש של הפורום בתל אביב.

במפגש נכחו 19 נציגים של 14 רשויות הפיקוח של המדינות הבאות: גרמניה, פולין, הולנד, צ'כיה, שבדיה, איסלנד, פינלנד, אוסטריה, שוויץ, הונגריה, דנמרק, נורבגיה, סלובקיה ואלבניה. כמו כן, נכח שליח נציבות האיחוד האירופי הממונה על נושא חתימה אלקטרונית. את רמו"ט ייצג עו"ד עזמי טנוס, מפקח במחלקת רישוי ופיקוח מנהלי, העוסק בנושאי חתימה אלקטרונית.

במפגש נדונו הנושאים הבאים:

- עדכונים מנציבות האירופית על מגמות ההסדרה והחקיקה של חתימה אלקטרונית באירופה, מהלכי הרמוניזציה של הרגולציה בין המדינות, ההסדרה של רשימה ממוחשבת של גורמי אמון באיחוד האירופי (ה–TSL), פעילות גופי התקינה האירופיים לעדכון התקינה הקיימת, פיתוח טכנולוגיות ייעודיות לשימוש המדינות לקידום ההרמוניזציה בין המדינות. בנוסף נמסר דיווח על אודות תוצאות ביניים לשאלוני Public Consultation שהופצו לציבור באירופה ושמטרתם לספק ידע לגבי האופן שבו חתימה, הזדהות ואימות אלקטרוניים, נתפסים ומיושמים בכל אחת מהמדינות על ידי גופים ציבוריים ופרטיים. תהליך זה נעשה במסגרת הכנת הרפורמה בדירקטיבה האירופית בדבר חתימה אלקטרונית.
- עדכונים של כל המדינות המשתתפות לגבי התפתחויות אחרונות בכל מדינה בתחום החתימה אלקטרונית.

- תיאור של כל אחת מהמדינות המשתתפות לגבי משטר הרישום והפיקוח הקיים אצלה, במסגרת הניסיון להגברת הרמוניזציה למשטר רגולציה אחיד בין המדינות.
- הצגת נציג הרשם על המצב בישראל, משטר הרישום והפיקוח, והניסיון הפיקוחי של רמו"ט בתחום.
- חלוקת ידע באתגרים משותפים.

# פרק ו' דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2011

## הערות המועצה להגנת הפרטיות לפי סעיף 10א לחוק הגנת הפרטיות

### המועצה הציבורית להגנת הפרטיות

י"ג באלול תשע"ב
30 באוגוסט 2012

לכבוד
ח"כ דוד רותם
יו"ר ועדת החוקה חוק ומשפט
הכנסת
ירושלים

נכבדי,

הנדון: **הערות המועצה הציבורית להגנת הפרטית על דו"ח רשם מאגרי מידע לשנת 2011**

המועצה הציבורית להגנת הפרטיות מתכבדת להגיש את הערותיה לדו"ח רשם מאגרי המידע לשנת 2011, בהתאם לסעיף 10א לחוק הגנת הפרטיות, התשמ"א-1981.

לצערנו, גם השנה מוגש הדו"ח באיחור. הוא הועבר לעיון המועצה באמצע חודש יולי 2012. מדובר אמנם באיחור קטן יותר מאשר בשנים עברו, אך כיוון שמועד הגשת הדו"ח קבוע בחוק, יש להקפיד על עמידה בלוח זמנים זה. יחד עם זאת, נראה שיש מקום לשקול מחדש את מסגרת הזמן הקבועה בסעיף 10א, שאינה נותנת זמן מספיק לערוך את הדו"ח ולהגישו להערות המועצה. מאז חוקק הסעיף גדל היקף הפעילות של הרשם באופן דרמטי, וככל שיש ציפייה שהדו"ח יכלול פירוט מהותי

ולא רק מידע סטטיסטי, נראה כי יש מקום להאריך את התקופה הקבועה בחוק בחודשים מספר.

שנת 2011 הייתה שנה של הישגים משמעותיים בתחום הגנת הפרטיות, בזכות פעילותה של הרשות למשפט, טכנולוגיה ומידע. אך היא הייתה גם שנה שבה נמשכה המגמה של איומים על הגנת המידע האישי של תושבי ישראל. אלה גם אלה באים לידי ביטוי בדו"ח.

שנת 2011 נפתחה בהישג חשוב במישור הבינלאומי. בסוף חודש ינואר, החליטה ה- European Commission להכיר במשטר הגנת הפרטיות ישראל כתואמת את אמות המידה האירופיות הקבועות בדירקטיבה של הפרלמנט האירופי. החלטה זו ניתנה במידה רבה בזכות פעולותיה של רמו"ט בשנים שמאז הקמתה. כפי שעולה מנוסח ההחלטה, ניתן גם משקל רב להודעתה של מדינת ישראל כי היא מתכוונת ליזום תיקוני חקיקה שישפרו את כלי האכיפה של דיני הגנת הפרטיות, וכן תעדכן את הדינים המהותיים עצמם על מנת להתאימם לסטנדרטים בינלאומיים ולהתפתחויות הטכנולוגיות האדירות מאז חוקק חוק הגנת הפרטיות. למרבה הצער, פעילות החקיקה מתקדמת באיטיות. הצעת חוק בדבר דרכי האכיפה הוגשה לכנסת לפני חודשים מספר, ואילו הצעות החוק בתחום הדין המהותי נמצאות בשלבי הכנה שונים במשרד המשפטים. המועצה קוראת למשרד המשפטים להאיץ את קצב ההכנה של הצעות חוק שטרם הוגשו לכנסת, ומקווה שהשלמת הליכי החקיקה של הצעת החוק הנמצאת כרגע על שולחן ועדת החוקה חוק ומשפט של הכנסת תיעשה בקרוב.

לקראת סוף השנה פורסמה תוצאת החקירה המוצלחת של מחלקת החקירות של רמו"ט בעניין דליפת מרשם האוכלוסין ופרסומו באינטרנט (פרשת האגרון). הצלחתה של יחידה ייעודית זו לפצח פרשה חמורה זו מקום שחקירת המשטרה לא הניבה תוצאות היא עדות לכך שתחום מיוחד זה של עבירות במאגרי מידע מצדיק הקצאת משאבי חקירה מיוחדים ומיומנים. שאלת אשמתם של הנאשמים בפרשה תיקבע על ידי בית המשפט, אך כבר בשלב זה יכולה המועצה לברך את העוסקים במלאכת ברמו"ט על שחשפו את הפעולות שהובילו להפצת המרשם ברבים. המועצה מקווה שמעבר להליכים הפליליים, חשיפה זו תביא להפקת לקחים ולשיפור דרכי אבטחת המידע אצל רשויות המדינה כדי למנוע עד כמה שניתן דליפת מאגרים הכוללים מידע אישי.

אלה החדשות הטובות. אך לא ניתן להתעלם מהחדשות הרעות שלצידן. הסיכונים לזכות לפרטיות רק הולכים ומתעצמים. חלק מהם באים לידי ביטוי בדו"ח הרשם. כך, למשל, פרויקט ה"רב קו" בתחבורה הציבורית יצא לדרך בשנת 2011. נאסף מידע רב מתושבי המדינה, לרבות מידע על קטינים, בלי שניתנה הדעת לצורך

לצמצם את היקף המידע שנאסף. לא ניתנה לתושבים בצורה מספקת האפשרות להשתמש בתחבורה הציבורית בלי צורך למסור מידע אישי. אף לא נקבעה שיטת איסוף והחזקה המיועדת למנוע שימוש במידע שנאסף שלא למטרה שלשמה נמסרה. מערכת הרב-קו תוכננה ללא כל מודעות לצורך לאמץ עקרונות של עיצוב לפרטיות (privacy by design). רק כאשר ניגש משרד התחבורה לקבוע את ההסדר החקיקתי לשימוש ברב-קו נחשפו הבעיות בתחום הפרטיות (בין השאר, בעקבות החלטת המועצה לקיים דיון עם נציג משרד התחבורה בנושא). שיתוף הפעולה עם רמו"ט החל בשלב מאוחר מדי, ומשרד התחבורה הפעיל את השיטה החדשה עוד לפני סיום הבחינה של רמו"ט ולפני השלמת הליכי החקיקה (שטרם הסתיימו). התנהלות זו חמורה בעינינו, כיוון שהיא חושפת מאות אלפים לקוחות "שבויים" של מערך התחבורה הציבורית לפגיעה בזכותם החוקתית לפרטיותם מבלי שזו תעוגן בחוק של הכנסת. מערכת הרב-קו נבנתה ועוצבה במטרה לשרת את צרכי משרד התחבורה והמפעילים ותוך התעלמות מהצורך להימנע מפגיעה בפרטיות, ולכל הפחות - לצמצמה ולהפכה למידתית. כפי שדיווח נציג רמו"ט בוועדת הכלכלה של הכנסת (בדיון מיום 21.2.12), ה"ארכיטקטורה של הטכנולוגיה" שנבחרה על ידי משרד התחבורה מכתיבה "סט של אילוצים", שמקשים היום על גיבוש הסדר מעשי וחוקי ראוי בהתאם לעקרונות של עיצוב לפרטיות. למרבה הצער, גם התחייבות של משרד התחבורה שניתנה למועצה, כי לכל נוסע תינתן אפשרות להשתמש ברב-קו ללא מתן פרטים מזהים (רב-קו אנונימי) לא התקיימה במועד ונערמו קשיים בפני מי שהעדיף להשתמש בכרטיס אנונימי.

המקרה של פרויקט רב-קו מהווה רק דוגמה לדפוס מדאיג שאפייני למיזמים נוספים של המדינה: רישות רחובות הערים במצלמות מעקב; מאגר ביומטרי של זרים, שהמדינה התחייבה בפני בג"צ לעגנו בדיעבד בחקיקה; מאגר התמונות "הביומטריות" במשרד התחבורה; מאגר המידע של ראמ"ה במשרד החינוך ועוד. רשויות המדינה בונות ומפעילות מערכות הפוגעות בפרטיות, ורק לאחר מכן - לעתים אחרי שנדרשו לעשות כן על ידי נציגי היועץ המשפטי לממשלה - נזכרים שיש צורך לעגן את הפעילות בחקיקה. בדרך זו הן עוקפת הרשות המבצעת את הכנסת, מונעת דיון ציבורי, וקובעת עובדות בשטח עוד לפני שהתקיים דיון ראוי לגבי האיזון הנאות בין הזכות לפרטיות לבין אינטרסים אחרים של הציבור.

עוד אירוע מדאיג בשנת 2011 היה אישור חקיקת המשנה להפעלת המאגר הביומטרי לתקופת מבחן ("הפיילוט"). הצו והתקנות אושרו בדיון חפוז אחד בוועדה מיוחדת של הכנסת, בלי מתן משקל מתאים, לדעת המועצה, לשיקולי הגנת הפרטיות. לאחרונה, בעת דיון בעתירה לבג"צ בנושא (בג"צ 1516/12), הבהירו השופטים שהצו לתקופת המבחן אינו עומד בדרישות החוק, והמדינה הסכימה לתקן את הצו כך שייקבעו בו הסוגיות שייבחנו בתקופת הפיילוט ומדדי ההצלחה. המועצה מברכת על כך שמדינה

הצהירה שבמסגרת תקופת המבחן, ולפני שתתקבל החלטה אם להקים מאגר ביומטרי שיכלול את כל תושבי המדינה, תישקל שוב הצעת פרופ' עדי שמיר למודל של מאגר שיכול להבטיח את אמינות מרשם התושבים ומסמכי הזהות בלי לפגוע פגיעה בלתי מידתית בפרטיות. המועצה מקווה שהצעה זו, עליה המליצו המועצה ורמו"ט בעבר, אכן תישקל בלב פתוח ובנפש חפצה, וכי לא יוחלט על הקמת מאגר כעניין שבחובה בלי לאמץ הצעה זו או מודל הדומה לו.

לפני ההתייחסות לדו"ח עצמו, מבקשת המועצה לברך את רמו"ט ואת העומד בראשה, עו"ד יורם הכהן, המסיים את תפקידו בימים אלה, על עשייה מקיפה ומרשימה ביותר למען הגנת הפרטיות של תושבי המדינה. עו"ד הכהן הקים את רמו"ט כמעט יש מאין, יחד עם הנהלת משרד המשפטים, ריכז צוות עובדים מצוין והצעיד את הרשות להישגים נכבדים. על כך נתונה לו תודת המועצה והערכתה.

## התייחסות לדו"ח

עיון בדו"ח מגלה פעילות רבה מאד של רמו"ט בתחום הגנת הפרטיות. ניתן לראות גידול בהיקף הפעילות בנושאי רוחב - חקיקה ומתן הנחיות. זו פעילות חשובה ביותר, ומקובלת עלינו גישת רמו"ט הנותנת קדימות לקביעת נורמות ולהכוונת הפעילות של הגופים מחזיקים מאגרי מידע. אך מובן שאין תחליף גם לאכיפה נמרצת ורחבת היקף. כדי לוודא שמחזיקי מאגרים ישקיעו את המאמצים ואת המשאבים הדרושים לקיום הוראות החוק, עליהם לדעת שקיימת סבירות ממשית שמעשיהם ייבחנו על ידי הגוף המסדיר והאוכף, וכי הם חשופים הן לעיצומים מינהליים והן להליכים פליליים.

בהקשר זה ניתן לשאוב עידוד גם מפסק הדין שניתן לאחרונה, שהכיר בסמכותה של רמו"ט לפרסם הנחיות ונהלים, ולהכריז בהם על הפרשנות של הדין, שלאורה תנהג רמו"ט בעת אכיפתו (עת"מ (ת"א) 24867-02-11 איי.די.איי חברה לביטוח בע"מ נ' רמו"ט (השופטת ד"ר מיכל אגמון גונן, 1.8.12).

נראה כי בשנת 2011 הייתה ירידה מסוימת במספר פעולות הפיקוח והאכיפה המינהלית. בשנת 2010 טיפלה הרשות ב - 233 תלונות בנושא הגנת הפרטיות, ואילו בשנת 2011 ב - 173 תלונות. בשנת 2010 נפתחו 76 תיקי פיקוח וטופלו 43 תיקים נוספים משנת קודמות, ובשנת 2011 נפתחו 55 תיקי פיקוח וטופלו 51 משנים קודמות. בשנת 2010 הוטלו 13 קנסות מינהליים (נגד 11 גופים) ובשנת 2011 - חמישה (נגד ארבעה גופים).

היינו רוצים לחשוב שהדבר נובע משיפור משמעותי בעמידתם של מחזיקי מאגרים בהוראות חוק הגנת הפרטיות, ולכן פחות תושבים גילו הפרות של זכותם לפרטיות

ונאלצו להגיש תלונות. אך אנו חוששים שאין הדבר כך. נראה כי ההפרות הן עדיין רווחות ומהותיות. ירידה במספר התלונות עשויה להצביע על מודעות בלתי מספקת ליכולת של תושבי המדינה להפנות תלונותיהם לרשות. בכל מקרה, לא מצאנו הסבר בדו"ח לתופעה זו. ייאמר מיד: אין אנו סבורים שהטלת קנסות היא מטרה בפני עצמה, ושהצלחתה של רשות אכיפה נמדדת במספר הקנסות שהיא מטילה. אך ירידה במספרים בתחום שבו ברור כי אנו רחוקים ממצב משביע רצון ברמת הציות לחוק טעונה לדעתנו הסבר. ייתכן מאד יש להפנות משאבים נוספים לרמו"ט כדי שהיא תשמור על רמת פעילות גבוהה בתחום הפיקוח והאכיפה. ייתכן גם שפחות מדי נעשה כדי להביא לידיעת הציבור שרמו"ט היא כתובת לפניות ולתלונות.

באשר לפירוט בדו"ח בעניין התלונות ובעניין תיקי פיקוח: אנו נאלצים לחזור על הערה שהערנו בעבר ואשר לא יושמה בדו"ח. בנתונים המפורטים בעמודים 3 - 6 לדו"ח חסרים פרטים על תוצאות פעולות הפיקוח. כאשר גוף מפקח המטפל בתלונות מדווח על פעולותיו, אין זה מספיק שידווח על מספר התלונות והתיקים ויאפיין אותם לפי הגוף שבו מדובר והנושאים שנבדקו. הדיווח צריך לשקף גם את תוצאות הטיפול, ולא רק בדרך של מתן דוגמאות. אנו מצפים כי הרשות תדווח כמה תלונות נמצאו מוצדקות, לפי אפיון של הגוף שעליה הייתה התלונה. נדרש גם דיווח על סוגי ההפרות שנמצאו והאמצעים שננקטו. אין אנו מצפים לתיאור מפורט של כל מקרה ומקרה, אך גם לא למספר סיפורי-מעשה בלבד. ראוי שהדיווח יכלול נתונים לגבי כלל התלונות, כדי שניתן לדעת מי הם הגופים המועדים להפרות בנושא הגנת הפרטיות ומה הן ההפרות הנפוצות.

הדיווח על מבחר תיקי הפיקוח הוא מאיר עיניים. כפי שכבר הערנו בעבר, חשוב ביותר שמידע זה יגיע לציבור לא רק אחת לשנה, עם פרסום הדו"ח, כי אם באופן שוטף. ואכן, לגבי חלק מהמקרים הופצו הודעות לעיתונות. חשיפת רמו"ט לתקשורת ולציבור אכן מתרחבת עם השנים. לפרסום בסמוך למועד ההתרחשות יש ערך הרתעתי רב, בנוסף כמובן לערך של שיתוף הציבור במידע כשלעצמו. נכון הוא שפרסום הודעה לעיתונות אינו מבטיח כיסוי תקשורתי, אך לכל הפחות יכולה הרשות לוודא שמידע על פעולות פיקוח שהסתיימו יועמד לרשות הציבור באתר האינטרנט של רמו"ט באופן שוטף. לא מצאנו פרסום מסודר ושיטתי כזה באתר הרשות היום.

מהדיווח לגבי תיקי פיקוח עולה כי לעתים מסתפקת הרשות בהודעת הגוף כי הוא יתקן את הליקויים ובמקרים אחרים נמסר על הטלת קנס מינהלי. אין בכך כל פגם, אך יש מקום להסבר לגבי מדינות האכיפה. נמחיש זאת בשתי דוגמאות.

בעמ' 11 לדו"ח מובא המקרה של חברת קדישא גחש"א בתל אביב. נמצא כי הייתה פעילות שלא כדין של עובד שבינתיים פוטר, והמידע בנושא הועבר למשטרה. אך

היה גם כשל מערכתי שאיפשר גישה למידע בניגוד להרשאה. נאמר כי נעשו פעולות לתיקון בעיות אבטחת המידע. לא ניתן הסבר מדוע לא ננקטו כלפי החברה קדישא גם פעולות אכיפה.

בעמ' 12 נדון המקרה של חברת אדם מילוא בע"מ. נמצא כי הייתה הפרה של סעיף 13 לחוק והוטל קנס מינהלי. ההפרה נבעה ממדיניות החברה להשמיד עותקים של דו"חות אבחון אחרי שהאדם שעליו הדו"ח ביקש לעיין בו. החברה שילמה את הקנס, אך לא מצאנו בדיווח מידע לגבי שינוי מדיניות החברה. מקרה מסוג זה מחייב, כך נראה, מעקב ופיקוח חוזר, כדי לוודא שהחברה אינה ממשיכה לנקוט במדיניות הקודמת שנמצאה בלתי חוקית.

בדו"ח מובא בהרחבה סיפור חשיפת השגת עותק ממרשם האוכלוסין והפצתו באינטרנט (פרשת האגרון). אכן מדובר בעניין בעל חשיבות ציבורית רבה וההצלחה של רמו"ט בעניין זה היא מרשימה. התוצאה במישור הפלילי תיקבע בבית המשפט. לדידנו, לא פחות חשובות הן המסקנות והתוצאות המערכתיות בעקבות הפרשה. בהקשר זה נציין, כי לצד הנזקים הכבדים שנגרמו בפרשת האגרון (ר' עמ' 29 - 32 לדו"ח), נראה כי היא הביאה גם לסקפטיות בריאה בדבר היכולת להגן באופן הרמטי על מידע אישי במאגרי מידע גדולים. פרסום הפרשה יוסיף, יש לקוות, מידה מוגברת של זהירות בשיח הציבורי בקשר להקמת מאגרי מידע ממשלתיים נוספים.

במהלך החקירה נחשפה עובדה שאי אפשר להפריז בחומרתה - החזקת עותק של פנקס האימוצים בידי אדם פרטי. למרבה המזל, מאגר זה, החסוי ביותר, לא הועלה לאינטרנט ואין אינדיקציה שהוא הועבר לידיים נוספות. אך הוצאת עותק מפנקס אימוצים מחייבת צעדים נחרצים כדי למנוע כל אפשרות שמעשה זה יחזור על עצמו. אף שהדבר אינו מופיע בדו"ח, אני מקווים שצעדים אלה נעשו כבר, וכי הרשות דואגת לפקח על כך כיאות. נראה למועצה כי עניין זה צריך להיות בראש סדר העדיפויות של רמו"ט.

המועצה ממליצה כי וועדת החוקה חוק ומשפט תקיים ישיבה שבה יוצג וייבחן הדו"ח השנתי. המועצה מציעה כי בדיון זה תבקש הוועדה מגופים הנוגעים בדבר דיווח על הפעולות שנעשו במשרדי הממשלה ובגופים ציבוריים אחרים כדי להפיק לקחים מכשלי האבטחה שהתגלו בפרשת האגרון, ובפרט - בעניין פנקס האימוצים.

בברכה,

יהושע שופמן
יו"ר המועצה

## מבוא

רשם מאגרי מידע היא פונקציית הרגולציה של הגנת הפרטיות במידע על פי חוק הגנת הפרטיות, התשמ"א–1981 (להלן בפרק זה – **החוק**), והיא פועלת במסגרת רמו"ט על בסיס החלטת הממשלה להקמתה. ראש רמו"ט מחזיק במכלול סמכויותיו של רשם מאגרי המידע על פי החוק, ומפקחי רמו"ט פועלים מכח סמכויות הפיקוח המוקנות בו. פעולות החקירה הפלילית המתוארות בדו"ח זה, נעשו מכח הסמכה ספציפית של השר לבטחון פנים לחקור עבירות על החוק ועל חוק שירות נתוני אשראי, התשס"ב–2002.

פרק זה של הדו"ח השנתי מוגש לועדת החוקה, חוק ומשפט על בסיס סעיף 10א לחוק, ובראשיתו מובאות הערות המועצה להגנת הפרטיות לגביו.

## פיקוח

### מבוא

בשנת 2011 המשיכה רמו"ט בפעולות פיקוח על קיום הוראות החוק, בהתאם לסמכויות רשם מאגרי המידע, והגבירה את נוכחותה בתודעת המשק הישראלי, הציבורי והפרטי כאחד.

בשנה זו טופלו בתחום הגנת הפרטיות 106 תיקי פיקוח בנושאים מהותיים שונים בחוק הגנת הפרטיות ובהם שימוש שלא למטרה במידע אישי, קיום דרישות החוק בפנייה לאדם בדיוור ישיר, אבטחת מידע שמצוי במאגרי מידע, איסוף מידע מאנשים שלא כדין והעברות מידע בין גופים ציבוריים.

החלטות שנתקבלו בתיקים כללו הטלת קנסות מינהליים, קביעה כי הופר החוק והנחייה לתיקון ליקויים. לעיתים עצם הפתיחה בפיקוח והפניה למפוקח גורמת לשינוי אופן הפעולה של הגורם המפוקח כך שיעמוד בחובות החוק.

הטלת קנסות מינהליים ופירוט סנקציות אחרות מפורסמות באתר האינטרנט של רמו"ט בקישור: http://www.justice.gov.il/MOJHeb/ILITA/Pirsumim/enforcementact.htm.

### נתונים

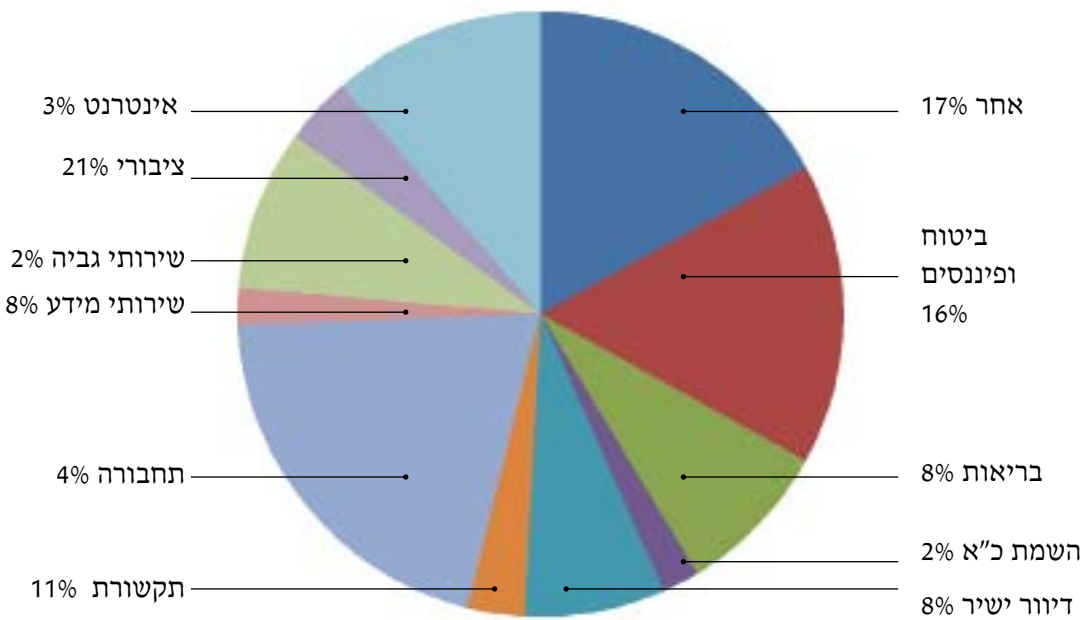
בתחום הגנת הפרטיות הוגשו בשנת 2011 לרמו"ט **173** תלונות, המהוות כ–**80**% מכלל התלונות שהגיעו לרמו"ט. נתון זה מציג ירידה של כ–25% בכמות התלונות ביחס לשנה הקודמת. הירידה מיוחסת לסיומה של פעילות תקשורתית ענפה שביצעה רמו"ט בשנת 2010 וחזרה של כמות התלונות להיקפן בשנת 2009. אחוז התלונות בתחום הגנת הפרטיות מתוך כלל התלונות המגיעות לרמו"ט נותר כשהיה.

במהלך השנה נפתחו ברמו"ט **55** תיקי פיקוח חדשים בנושא הגנת פרטיות, המהווים **70**% מכלל תיקי הפיקוח שנפתחו בשנה זו. בנוסף נמשך טיפול ב–51 תיקי פיקוח בתחום זה שנפתחו קודם לשנת 2011, ובסה"כ טופלו בשנת 2011 בתחום הפיקוח **106** תיקים.

## שיעורי תיקי הפיקוח לפי חתך מגזרי

השקף להלן מציג את התפלגות תיקי הפיקוח לפי חתך מגזרי. הוא נותן תמונה יחסית מדויקת לגבי מגוון תחומי הפיקוח של רשם מאגרי מידע, וזאת לאור העובדה שמידע אישי מעובד היום במשרדי הממשלה, בגופים ציבוריים אחרים, בכל סקטור במגזר העסקי, וכן בגופים ללא מטרת רווח.

מטבע הדברים, החלוקה להלן מעידה רק על הפקוחים בפועל שנעשו על ידי רמו"ט, ולא בהכרח על התחומים בהם יש סכנות גדולות יותר לפרטיות מאשר אחרים.



## נושאים שנבדקו בתיקי פיקוח

הנושאים שבהם עסקה רמו"ט בתיקי הפיקוח כללו:

א. שימוש במידע שלא למטרה לשמה נמסר (סעיף 8(ב) לחוק) – בכ–55% מהתיקים;

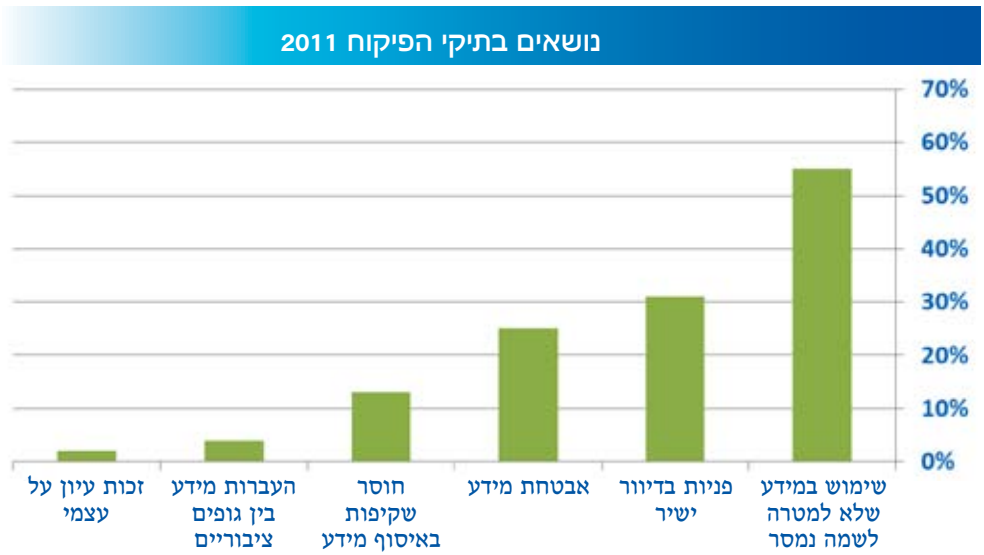
ב. פניות בדיוור ישיר (סעיף 17ד – 17ו לחוק) – בכ–31% מהתיקים;

ג. אבטחת המידע במאגרי המידע (סעיף 17 לחוק) – בכ–25% מהתיקים;

ד. אי מתן הודעה בטרם איסוף מידע למאגר מידע (סעיף 11 לחוק) – בכ–13% מהתיקים;

ה. העברות מידע בין גופים ציבוריים (פרק ד' לחוק) – בכ–4% מהתיקים;

ו. אי מתן זכות עיון (סעיף 13 לחוק) – בכ–2% מהתיקים.




1 בתיקי פיקוח נבחנות לעתים קרובות הפרות אפשריות של יותר מסעיף חוק אחד, ולכן הדיווח באחוזים הינו לגבי כל סעיף חוק מתוך כלל התיקים.

# תיקי פיקוח נבחרים במגזר הציבורי

## משרד הביטחון

הפיקוח בחן העברות מידע מרשות המסים, מהמוסד לביטוח לאומי, וממשרד הפנים (רשות האוכלוסין, ההגירה ומעברי הגבול) לאגף שיקום נכים במשרד הבטחון. במסגרת הפיקוח נבחנה תקינות הליך העברת המידע בין גופים אלה, נוכח הוראות פרק ד' לחוק והתקנות מכוחו.

העברת מידע בין גופים ציבוריים מוסדרת בפרק ד' לחוק, בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבורים), התשמ"ו–1986 ובהנחייה ליועצים המשפטיים במשרדי הממשלה מטעם המשנה ליועץ המשפטי לממשלה (ייעוץ), מר בלס, מיום 16.03.2006, בנושא "העברת מידע בין גופים ציבורים".

ההליך כולל חובת הגשת בקשה לועדה להעברת מידע בין גופים ציבוריים של הגוף בעל המידע וקבלת אישורה. הבקשה אמורה להבדק על ידי הועדה רק לאחר אישורה על ידי מנהל מאגר המידע, הממונה על האבטחה והיועץ המשפטי של הגוף ממנו נתבקש המידע. על בעלי התפקידים הרלוונטיים והועדה לבחון, בין השאר, אם הגוף המבקש את המידע הוא "גוף ציבורי" הרשאי לדרוש אותו על פי דין. כמו כן, יש לבחון את המידתיות והסבירות של הבקשה ואת התאמת רמת אבטחת המידע בגוף המבקש לאופי המידע שהיא מבקשת לקבל, אופי והיקף מורשי הגישה והטיפול במידע בגוף המבקש. אישור הועדה עשוי להינתן לתקופה קצובה.

בפיקוח נמצא כי –

א. בחלק מהמועדים שבהם הועבר מידע מהמוסד לביטוח לאומי למשרד הבטחון לא היה אישור ועדה להעברת מידע תקף המאשר את העברת המידע. משרד הבטחון הודיע כי הוא פעל מיידית לחידוש האישור, כי הודגש בפני העובדים כי אין לבצע העברות מידע ללא אישור תקף, וכי הוא פועל ליצירת מנגנון בקרה והתרעה ממוחשב לניהול הנושא על מנת למנוע מקרים כאלו בעתיד.

ב. העברת מידע מרשות האוכלוסין, ההגירה ומעברי הגבול במשרד הפנים למשרד הביטחון לצרכי אגף שיקום נכים מבוצעת באופן ובהיקף שאינו סביר, אינו מידתי וכולל מידע עודף רב. הועדה להעברת מידע נתבקשה לבחון מחדש את החלטתה בהתאם לעקרונות החוק, התקנות והנחיית היועמ"ש. סוגייה זו ממשיכה להתברר בימים אלו.

ג. משרד הבטחון לא העמיד לעיון הציבור באתר האינטרנט שלו את רשימת מקבלי המידע ממנו כנדרש. המשרד נדרש לתקן ליקוי זה.

## רשות האכיפה והגבייה

הפיקוח בחן את המרשם המקוון של החייבים שהוכרזו מוגבלים באמצעים ע"י רשות האכיפה והגבייה. תקנות ההוצאה לפועל, תש"מ–1979 מכוחן פועל המרשם קובעות, כי משתמש לא יוכל להגיש ולקבל מענה מהמרשם על יותר מ– 10 שאילות ביום.

בפיקוח נמצא כי –

א. ניתן במניפולציה להגיש מספר בלתי מוגבל של שאילתות ולמעשה לייצר עותק של כל המידע.

ב. נמצאו ליקויי אבטחת מידע נוספים.

ג. הרשות הונחתה לתקן את הליקויים שנמצאו, לבצע סקר סיכונים ומבדק חדירות לשם איתור פרצות האבטחה באתר ולבצע תוכנית עבודה לתיקון הליקויים שיאותרו. הרשות דיווחה על ביצוע הנדרש.

## משרד התחבורה - רשות הרישוי

הפיקוח בחן את המוקד הטלפוני הממוחשב שמפעיל משרד הרישוי למתן מידע על רישיונות נהיגה.

בפיקוח נמצא כי –

הליך הזיהוי לצורך קבלת מידע ושירות מהמוקד התבסס על פרטים המופיעים במרשם האוכלוסין בלבד, בניגוד להנחיית הרשם 2010–1 אשר קבעה כי הסתמכות על פרטי מידע אלה בלבד, לאור קיומו של עותק ממרשם האוכלוסין באינטרנט, היא הפרה של חובת אבטחת המידע הקבועה בסעיף 17 לחוק.

רשות הרישוי הונחתה לפעול לתיקון הליקויים והודיעה שתפעל בהתאם.

## רשות ניירות ערך

הפיקוח בחן את אופן הפרסום של מידע אודות יועצים, משווקים ומנהלים להשקעות בעלי רשיון מאת הרשות לניירות ערך באתר האינטרנט של הרשות.

בפיקוח נמצא כי –

א. באתר מפורסמת רשימה הכוללת פרטים אישיים וביניהם שם, שם משפחה, מספר תעודת זהות, מספר רישיון ופרטים אודות הרישיון.

ב. מטרות הפרסום ע"י רשות ניירות ערך הן בקרה, פיקוח והסדרה של פעילות מבקשי הרישיון במטרה לשמור על ציבור המשקיעים.

ג. ישנו מזהה חד–חד–ערכי שהוא מספר רישיון שהוענק ע"י רשות ניירות ערך, ויכול להחליף את השימוש במס' ת.ז.

ד. נקבע כי פרסום מספרי הזהות בצמוד לשם בעל הרישיון אינו מידתי, שכן ניתן ללמוד רבות אודות אדם ממספר הזהות שלו[2], וכן ניתן לנקוט באמצעים למימוש המטרה שפגיעתם פחותה. למשל ציון מספר הרישיון שניתן לבעל הרישיון על ידי רשות ניירות ערך.

ה. רשות ניירות ערך הודיעה לרשם כי היא מסירה את מס' ת.ז. מהפרסום באתר האינטרנט שלה.

## עיריית אשקלון

הפיקוח בחן את אופן יישום השימוש במערך מצלמות אבטחה שנפרש בעיר אשקלון במסגרת פרויקט עיר ללא אלימות. יצויין, כי הגם שמניעת אלימות היא מטרה חשובה וראויה, נדרשת תשומת לב ביישום פרוייקט מסוג זה גם להיבטים של הפגיעה בפרטיות האנשים, שהיא פועל יוצא של הצבת מצלמות במרחב הציבורי.

הפיקוח בחן את הפרוייקט אל מול חוות הדעת שפרסמה המחלקה המשפטית ברמו"ט "מצלמות מעקב – הדין החל ואופן השימוש" מיום 3.11.10 (ע"י עו"ד ניר גרסון).

בפיקוח נמצא כי –

א. הפרויקט נדון ע"י צוות מקצועי ואושר בועדת היגוי עירונית בהשתתפות נציגי ציבור, משטרה, ועד הורים מרכזי, נציגי ועדי שכונות, מנהלי בתי ספר, מפקחים, פסיכולוגים, עו"ס ומפקח ארצי לנוער וצעירים;

2 בגץ 6824/07 ד"ר עאדל מנאע נ' רשות המסים, פסקה 37.

ב. מטרות הפרוייקט הוגדרו בנוהל כתוב: איתור קטטות, תקיפות, נפילות טילים, סדר ותנועה, השלכות פסולת, איתור גניבות, פעילות פלילית וכיו"ב. בהתאם לכך נקבע מיקום ומספר המצלמות.

ג. לא נערך תסקיר של השלכות השימוש במצלמות על זכויות הציבור ובמיוחד על הזכות לפרטיות;

ד. המוקד הוקם במבנה הביטחון העירוני ופועל במשך כל שעות היממה במשך כל השנה;

ה. הוגדרו 14 מורשי צפייה מטעם העירייה; המורשים עברו ועדת קבלה ונבדק עברם הפלילי. הם קיבלו הדרכה וקיימות הוראות כתובות כי חל איסור צפייה בשטחים שאינם ציבוריים;

ו. מידע מועבר למשטרת אשקלון, בהתאם לנהלי עבודה, כאשר נצפה אירוע פלילי;

ז. המידע המצולם מוקלט ונשמר במערכת המחשב במוקד. לאחר חודש המידע נמחק באופן אוטומטי;

ח. למצלמות אין יכולת ראיית לילה, הקלטת קול או זיהוי אנשים;

ט. כדי לצפות במידע המצולם יש להיכנס להיסטוריה של כל מצלמה בנפרד;

י. לא ניתן לצפות במידע המצולם באמצעות האינטרנט;

יא. מנהלת המוקד מפקחת באופן שוטף על קיום ההנחיות, אך אין נוהל בקרה כתוב;

יב. המידע אודות המוקד והצבת המצלמות פורסם במקומונים בשפה עברית ורוסית, באתרי אינטרנט וברדיו;

יג. במועד הפיקוח טרם הוצב שילוט המספק מידע לתושבים.

ראוי לציין כי הפיקוח העלה כי עיריית אשקלון יישמה רבים מהעקרונות אשר גובשו על ידי רמו"ט בחוות הדעת האמורה, עובר לפיקוח כתוצאה מעבודת מטה סדורה שנעשתה בעניין זה החל משנת 2006, ובהחלט ראוי לציין זאת לחיוב. העיריה הונחתה להציב שילוט ולגבש נהלי בקרה על קיום ההנחיות לתפעול המוקד.

# תיקי פיקוח נבחרים במגזר הפרטי והשלישי

## אתר MAKO.CO.IL – איסוף מידע מקטינים

בירור תלונה שהוגשה לרמו"ט על ידי המועצה לשלום הילד לגבי חריגות באיסוף מידע על קטינים במסגרת מיון לתוכניות ריאליטי על ידי אתר האינטרנט של חברת התקשורת "קשת" (mako.co.il) העלה כי קטינים יכולים ואף מוזמנים להירשם כמועמדים לתוכניות ריאליטי באתר, תוך מסירת מידע אישי רב על אודותיהם, על אודות משפחתם ועל אודות חבריהם, וזאת ללא הסכמה הורית. גם נוסח ההסכמות עליהם נדרשו קטינים "להסכים", לכאורה, הביאו לויתור גורף על זכויותיהם.

במסגרת הפיקוח הוצגו הממצאים לחברת קשת, ונוהל משא ומתן על האופן שבו יכולה קשת, באמצעות "מאקו", לגייס מועמדים לתוכניות ריאליטי לילדים, תוך צמצום החשש של מסירת מידע אישי רב ללא הסכמה או פיקוח הוריים.

במסגרת ההתדיינות עם קשת נדונו עקרונות שמשלבים מחד גיסא את התכליות הנדרשות לקשת לצורך פעילותה העסקית, ומאידך גיסא, עמידה בהוראות חוק הגנת הפרטיות ועקרונותיו. העקרונות התבססו על נייר העמדה שפרסמה רמו"ט בנושא איסוף מידע על קטינים.

העקרונות מבוססים על החלופות הבאות:

א. איסוף פרטי קשר בלבד – בחלופה זו יאספו פרטי קשר בסיסיים בלבד מקטין שהביע התעניינות בתוכנית, כאשר איסוף מידע רב יותר אודותיו לצורך הליך המיון יעשה רק לאחר קבלת הסכמה של אפוטרופוס.

ב. איסוף מידע ללא פרטים מזהים – איסוף מידע בהיקף נרחב אודות קטין לצרכי הליך המיון, אולם ללא איסוף פרטים המזהים אותו. הקישור לפרטים מזהים ייעשה רק בהסכמה של אפוטרופוס.

ג. איסוף מידע הכולל פרטי קשר ומידע נרחב יותר בשיטה סבירה המוודאת הסכמה של אפוטרופוס – ניתן לאסוף מידע רב יותר בתנאי שננקטה פרקטיקה סבירה לוודא כי ניתנה הסכמה של אפוטרופוס, כגון קבלת טופס הסכמה חתום, קיום שיחה טלפונית מתועדת עם ההורה, שימוש במספר כרטיס אשראי ועוד.

במסגרת כל אחת מחלופות אלה, נדרשה קשת לתת גילוי נאות, בשפה ברורה ובהירה התואמת את רמת ההבנה של הנמען ובהתאם להוראות סעיף 11 לחוק, לעניין זהות הגורם המעבד את המידע, מטרות השימוש במידע, הגורם האחראי על השימוש במידע, אופן העיון במידע ואופן מחיקתו במידה שנושא המידע מעוניין בכך.

במסגרת ההתדיינות עם קשת הוברר כי המידע שנאסף לא הועבר לגורם חיצוני מחוץ לקשת והגורמים הפועלים מטעמה, ולא שימש לכל מטרה פרט להליך המיון לתוכניות. במסגרת הפיקוח התחייבה קשת להפסיק את איסוף המידע מקטינים באופן שפעלה בו בטרם הפיקוח. קשת נדרשה בהמשך לכך, למחוק את המידע שנאסף על קטינים ללא הסכמה מדעת של הורה, ושהמשך השימוש בו לא הותר על ידי הורה, בהתאם למנגנון קבלת הסכמה סביר.

על רקע האמור, ומאחר שהמידע לא הועבר לכל גורם חיצוני ולא שימש לכל מטרה פרט להליך המיון, ובשים לב לשיתוף הפעולה של קשת בתיקון אופן פעילותה, מצאה רמו"ט לנכון לסיים את הטיפול בתלונה בצעדים המתקנים שננקטו על קשת.

## חברה קדישא גחש"א תל אביב - יפו והמחוז

בפיקוח נבחנו תלונות שהעלו חשד להעברת מידע של משפחות נפטרים שהובאו לקבורה באמצעות חברה קדישא תל אביב -יפו לקבלני מצבות.

בפיקוח נמצא כי –

א. עובד החברה קדישא הוציא ללא רשות מידע ממערכת המידע של החברה ומכר אותו לקבלן מצבות.

ב. מערכות המידע של החברה אפשרו את השימוש במידע בניגוד להרשאה ולא אפשרו ניטור הפעילות הלא מורשית של העובד.

בעקבות ממצאי הפיקוח העובד פוטר מעבודתו בחברה והחברה פעלה לתיקון ליקויי אבטחת המידע במערכותיה, לביצוע בקרה למניעת קרות אירועים כאלו ולהדרכת עובדיה בהתאם. תיק הפיקוח דווח המשטרה.

## סמארט קלאב בע"מ

החברה עוסקת במכירות באמצעות דיוור ישיר טלפוני של מוצרי אלקטרוניקה.

בפיקוח נמצא כי –

א. הדיוור הישיר מתבצע על בסיס מידע שנרכש ממאגר לשירותי דיוור ישיר.

ב. החברה הפרה את חובותיה בפנייה בדיוור ישיר לציין את מספר הרישום של המאגר המשמש לשירותי דיוור ישיר שעל בסיסו פנתה לאדם, ומהו המען אליו עליו לפנות על מנת להסיר את פרטיו ממנו.

הוטלו על החברה קנסות מינהליים אשר שולמו על ידיה.

## אדם מילוא בע"מ

בפיקוח נבחנה תלונה של אדם שביקש לממש את זכותו בסעיף 13 לחוק לעיין במידע שמוחזק עליו במאגר מידע וסורב.

בפיקוח נמצא כי –

א. המתלונן עבר מבחן התאמה לעבודה מטעם מעסיק במכון גיוס והשמת כח אדם "אדם–מילוא".

ב. כאשר ביקש לעיין במידע נענה ע"י המכון כי על פי נוהל עבודה שלו, המכון מוחק מידע על אדם לאחר שהגיש בקשת עיון במידע. זאת משום שהוא ויתר על זכותו לעיין במידע בכתב ויתור עליו חתם לטובת המכון בטרם בוצע המבחן.

ג. בפיקוח במשרדי אדם מילוא נמצא עותק מחוות הדעת.

נקבע כי המכון הפר את חובתו למתן עיון למתלונן על מידע שעל אודותיו במאגר מידע, וכי עצם הניסיון למחוק את חוות הדעת לאחר שאדם מבקש לעיין במידע בהתאם לזכותו בסעיף 13 לחוק מהווה הפרה של החוק.

על החברה הוטל קנס בסך– 2000 ₪ ששולם על ידיה. חוות הדעת הועברה לעיון המתלונן לאחר שהמעביד שהזמין אותה קיבל הודעה מרמו"ט על כוונתה לפעול כך ולא התנגד.

## גפן מדיקל בע"מ

בפיקוח התבררה תלונה של אדם שרכש מכשיר למדידת רמת סוכר בדם ונדרש למסור מידע אישי רגיש לצורך קבלת שרות ואחריות למכשיר.

בפיקוח נמצא כי –

א. החברה, העוסקת במכירת ציוד רפואי, נהגה לאסוף מרוכשי מוצרים במעמד מכירת המוצר בנוסף לשם וכתובת גם מין, תאריך לידה ופרטי קופת חולים.

ב. בנוסף אספה החברה בשובר שנדרש הלקוח למלא פרטים אודות מחלתו, הרופא המטפל ועוד. באותיות זעירות נכתב כי אין חובה למלא את השורות הבאות.

ג. המידע האישי הוזן למאגר המידע של החברה.

נקבע כי איסוף המידע באופן זה אינו עומד בדרישות סעיף 11 לחוק הקובע כי יש לפרט האם חלה על האדם חובה חוקית למסירת המידע או שהיא תלויה ברצונו ובהסכמתו. וכן לפרט את המטרות והשימושים שיעשו במידע, למי יימסר המידע ומה מטרות המסירה.

עוד נקבע כי כריכת איסוף המידע עם מתן אחריות מוצר המחויבת על פי חוק פוגמת באפשרות של הלקוח לתת הסכמה חופשית לשימוש במידע האישי שהוא מוסר ולכן אסורה.

על החברה הוטל קנס בסך 2000 ₪ בגין ההפרה במקרה התלונה. בנוסף, הונחתה החברה לשנות את אופן הפניה לקבלת מידע בהתאם לחוק, ולמחוק את המידע הרגיש ממאגר המידע שלה שנאסף בניגוד לחוק.

החברה שילמה את הקנס שהוטל עליה ודיווחה על ביצוע הנדרש ממנה.

## הראל חברה לביטוח בע"מ

הפיקוח בחן שימוש שעושה הראל חברה לביטוח בע"מ, במידע שבמאגרי המידע שלה שמקורו בעריכת ביטוחי רכב לעובדי מדינה כזוכה במכרז.

בפיקוח נמצא כי –

א. החברה העבירה מידע על מבוטחים שלה בביטוחי רכב לסוכנות ביטוח איריץ–דושינסקי;

ב. הסוכנות פנתה למבוטחי הרכב בדיוור ישיר טלפוני בהצעות לביטוח חיים על בסיס המידע שנתקבל;

ג. החברה טענה שהסכמת נושאי המידע לשימוש בפרטיהם למטרה זו ניתנה בטופס התקשרות לביטוח רכב;

ד. בטופס ההתקשרות היה אזכור עמום של מטרה שיווקית לשימוש במידע, מעורב במשפט ארוך ומורכב שעיקרו הצהרה כי הפרטים ישמשו למטרת הטיפול בביטוח הרכב.

נקבע שבנסיבות אלו החברה הפרה את חובת הגילוי בסעיף 11 לחוק. בהתאם נפגמה ההסכמה מדעת של המבוטח למטרות שימוש נוספות ואחרות מלבד קבלת ביטוח הרכב.

החברה נדרשה לתקן את הליקויים באופן פעולתה מול לקוחותיה.

## WWW.NEXTMODEL.CO.IL – גרטלר דוידוב תקשורת ש"מ

הפיקוח נפתח לבירור תלונה שהעבירה לרשם המועצה לשלום הילד, המצביעה על מיזם של החברה נקסט מודל, שהקימה אתר אינטרנט המשמש כסוכנות דוגמנות וירטואלית, הכוללת פרסומים שנחזים להיות על קטינים.

בפיקוח נמצא כי –

א. המידע באתר מועלה ע"י הגולשים, לאחר שמסרו פרטים מזהים המאפשרים להנהלת האתר ליצור עימם קשר;

ב. החברה מסרה שהיא נהגה לנטר תכנים בלתי נאותים ופוגעניים. במקרים אלו הוסר הפרופיל האישי ופרטי ההרשמה שנמסרו לצורך הרישום נמחקו;

ג. פרט לפרסום הפרופיל באתר ושימוש במידע שלא פורסם, לזיהוי, לא נעשה שימוש אחר או נוסף במידע שנמסר על ידי הנרשם, כמו כן לא נמסר ולא נאגר מידע אודות גולשים שלא נרשמו לאתר;

ד. נרשם אשר ביקש למחוק את הפרופיל האישי שלו, לאחר זיהוי, הוסר מן האתר וכל פרטי ההרשמה שלו נמחקו כליל.

ה. מיד עם פניית רמו"ט לחברה היא הודיעה על הפסקת פעילותו של האתר.

## WWW.INFORMER.CO.IL

בפיקוח נבחנה חוקיות שירות מכירת דו"חות אימות נתונים ובדיקות רקע שהוצע באתר האינטרנט www.informer.co.il.

בפיקוח נמצא כי –

א. השירות ניתן ע"י בעל רישיון לחוקר פרטי;

ב. השירות ניתן לכל מזמין באמצעות אתר האינטרנט, מבלי שמבוררת זהות הלקוח;

ג. החוקר הפרטי עשה שימוש בנתוני אשראי שהתקבלו מבעל רישיון שירות נתוני אשראי די.אנד.בי החברה לנתוני אשראי בע"מ שלא למטרה לשמה הוקם המאגר;

ד. החוקר הפרטי השתמש בהליך הנפקת הדו"חות, במידע כהגדרתו בחוק הגנת הפרטיות ממקורות מידע אשר אינם, לכאורה, זמינים לציבור באופן פומבי וחוקי;

נקבע, כי החוקר הפרטי הפר את סעיף 8(ב) לחוק בשימוש שלא למטרה במידע ממאגר מידע של בעלת רישיון שירות נתוני אשראי, ושהוא הפעיל שירות נתוני אשראי ללא רישיון תוך הפרה של חוק שירותי נתוני אשראי, תשס"ב–2002.

על החוקר הפרטי הוטלו 2 קנסות מינהליים בסך כולל של 10,000 ₪, ונאסר עליו להמשיך בפעילות המפרה. דיווח על ממצאי הפיקוח הועבר למועצה לרישוי חוקרים פרטיים ושירותי שמירה, אשר דנה בחידוש רישיון החוקר הפרטי, והחליטה שלא לחדשו בשנת 2012.

במקביל, בעלת הרישיון די.אנד.בי הודיעה כי הפסיקה את מכירת דו"חות האשראי לחוקר הפרטי.

בהמשך פעולות פיקוח בשנת 2012 נמצא עוד כי החוקר הפרטי עשה שימוש שלא למטרה ותוך הפרה של החוק במידע ממרשם האוכלוסין מההפצה הבלתי חוקית שלו ברשת האינטרנט המכונה אָגְרוֹן. גם על הפרה זו הוטל עליו קנס מינהלי.

על רקע הממצאים בתיק פיקוח זה גיבש רשם שירותי נתוני אשראי ומידע על עוסקים הנחיה לשירותי נתוני אשראי, כמפורט בהמשך הדו"ח השנתי.

## סלקום ישראל בע"מ

בשנת 2011 הסתיים הטיפול במספר תיקי פיקוח על חברת סלקום ישראל בע"מ (להלן **-סלקום**).

**תיק פיקוח ראשון** בחן את היקף איסוף המידע האישי ממנויים והשימושים שנעשים במידע ע"י החברה אל מול ההסכמה שניתנת ע"י הלקוחות.

בפיקוח נמצא כי –

א. סלקום אוספת מידע אישי מסוגים שונים בהיקף עצום על אודות נושאי מידע במהלך פעולותיה השונות, ועושה בו שימושים רבים למטרות מגוונות, וזאת בנוסף על השימוש הבסיסי והמקורי של מתן שירותי טלפון נייד.

ב. האיסוף כולל פרטים אישיים שנמסרים ע"י הלקוח בעת ההתקשרות לצורך מתן השירות העיקרי; טיוב נתוני הלקוח ממאגרי מידע אחרים; איסוף מידע על אנשים שאינם לקוחות על בסיס המידע של הלקוחות; איסוף נתוני מיקום לצורך מתן שירותים מבוססי מיקום ולשימוש אחר בהם שאינו מתן השירות; איסוף מידע ע"י צדדי ג' (דוגמא: ספקי שירותי תוכן שאוספים נתוני גלישה באתרי תוכן או תכני גלישה) והעברתו לסלקום שעושה בו שימוש שאינו מתן השירות.

ג. נמצא גם כי סלקום עושה שימושים במידע שנצבר על מנוי תוך כדי ההתקשרות באמצעות מתן גישה לצדדי ג' כגון ספקי תוכן וספקי אפליקציות במידע.

סלקום הונחתה, במכתב אשר מוען למנכ"ל החברה, לפעול לקבלת הסכמה מדעת כחוק של נושאי המידע לשימושים השונים שנעשים במידע עליהם ולהימנע משימושים שלא ניתנה

להם הסכמה. לצורך קבלת הסכמה מדעת, הונחתה סלקום לתת שקיפות מלאה לבעל המידע בטרם קבלת ההסכמה לגבי סוגי המידע הנאסף והשימושים המיועדים לו. עוד הונחתה סלקום לפעול לגיבוש מדיניות פרטיות מפורטת להגנה על פרטיות עובדיה ולקוחותיה, במגוון הרחב של השימושים שהיא עושה במידע.

סלקום השיבה כי היא בוחנת את הממצאים ותפעל בהתאם.

ראוי לציין כי במקביל לפיקוח נבחנה בבית הדין לחוזים אחידים שאלת ההסכמה שנדרש לקוח לתת בחוזה האחיד עליו הוא מוחתם בעת ההתקשרות עם סלקום. עמדת היועץ המשפטי לממשלה היתה כי נוסח ההסכמה שקיים בחוזי סלקום מהווה תנאי מקפח בחוזה אחיד.

**תיק פיקוח שני** מול סלקום בחן יישום משחקי (אפליקציה) מבוסס נתוני מיקום לשימוש בטלפונים סלולריים שהציעה סלקום על גבי פלטפורמת הרשת החברתית פייסבוק. מאופי הרשת החברתית כמחזיקה מידע מזוהה, פעולות המשתמשים באפליקציה מזוהות עם הפרופיל האישי שלהם. קהל היעד אליו שווקה האפליקציה, והשימוש בה בפועל, כלל קטינים. הפעלת המשחק הופסקה לאחר שנה ביוזמת סלקום.

לאור פניית הרשם הודיעה סלקום כי מחקה את כל הנתונים שנאספו במהלך המשחק.

**בתיק פיקוח שלישי** נבחנה העברת מידע על לקוחות סלקום לחברת נטרואדס תקשורת בע"מ לצורך שיווק שירות התראה על מכמונות מהירות בעת נהיגה.

בפיקוח נמצא כי –

א. הפניות בדיוור ישיר ללקוחות נעשו שלא בהתאם להוראות פרק הדיוור הישיר בחוק.

ב. בפיקוח נקבע כי סעיף 17ו. לחוק מתייחס לכל פנייה בדיוור ישיר, ואין חובה שהמאגר על פיו בוצעה הפניה יהיה מאגר לשירותי דיוור ישיר.

ג. הובהר כי הגם שלקוח של החברה לא יוכל להימחק לחלוטין ממאגרי החברה, מאחר שחלות על החברה חובות חוקיות לשמור את המידע לתקופות מסוימות, על החברה לאפשר את מחיקתו מקבלת פניות בדיוור ישיר.

סלקום נדרשה לפעול להתאמת פעילותה לדרישות החוק.

## הטלת קנסות מנהליים

לנוחות הקוראים מצורפת בזאת טבלה המרכזת את כל הקנסות המינהליים שהוטלו על ידי רמו"ט בנושאי הגנת הפרטיות בשנת 2011:

| מועד קביעת ההפרה | שם המפר | סקטור | מספר ח.פ. | סעיף החוק שהופר | תיאור ההפרה |
|---|---|---|---|---|---|
| 30/08/2011 | **אדם מילוא** | מיון והשמת כוח אדם | 511033086 | 13 | המכון סרב לאפשר לנבחן לעיין בחוות הדעת שנמסרה למעסיק הפוטנציאלי. כמו כן, המכון טען כי כחלק מנהלי העבודה המידע נמחק בעת הגשת בקשת עיון. בפיקוח במשרדי המכון נמצא עותק מחוות הדעת. |
| 21/07/2011 | **חוקר פרטי** | חוקרים פרטיים | | 8(ב) | שימוש במידע ממאגר שירות נתוני אשראי למכירת דוחות מידע אישי במסגרת פעילות חוקר פרטי |
| 17/04/2011 | **מועדון חכם בע"מ (סמרט קלאב)** | שיווק ישיר | 512010653 | 17ו(א) | בפניה לא מסרה החברה למלין כי הפניה היא בדיוור ישיר, לא צוין מספר המאגר ממנו נרכש המידע, לא ניתנה הודעה על זכותו של מקבל הפניה להימחק מהמאגר והמען אליו יש לפנות לצורך כך. כאשר המלין שאל למקור המידע נמסר לו מידע מטעה. |
| 17/04/2011 | **מועדון חכם בע"מ (סמרט קלאב)** | שיווק ישיר | 512010653 | 17ו(א) | בפניה לא מסרה החברה למלין כי הפניה היא בדיוור ישיר, לא צוין מספר המאגר ממנו נרכש המידע, לא ניתנה הודעה על זכותו של מקבל הפניה להימחק מהמאגר והמען אליו יש לפנות לצורך כך. בשיחה נוספת של החברה עם המלין נמסרו פרטי מידע שגוי אודות מספר המאגר וכתובת שגויה לצורך הסרה מהמאגר |
| 29/03/2011 | **גפן מדיקל** | שיווק ישיר | 512219361 | 11 | אי יידעו כי מסירת המידע תלויה בהסכמת המוסר ואי פירוט המטרות והשימושים שיעשו במידע |

# חקירות פליליות

## מבוא

מחלקת החקירות של רמו"ט הוקמה בשנת 2009 במטרה לכונן אכיפה פלילית בתחום של הגנת פרטיות במידע אישי, נושא אשר לא זכה במדינת ישראל לעדיפות מספקת עד הקמתה של רמו"ט. לצורך כך הוחל בבנייתו של צוות מקצועי ומיומן אשר מסוגל להתמודד עם עבריינות מורכבת בנושא זה.

במהלך 2010 הוענקה ע"י השר לביטחון פנים הרשאה לחוקרי מחלקת החקירות של רמו"ט לחקור עבירות על חוק הגנת הפרטיות וחוק שירות נתוני אשראי בהתאם לסמכויות המוקנות בפקודת הפרוצדורה הפלילית (עדות).

בשנת 2011 מנתה המחלקה שישה חוקרים. במקביל לניהול החקירות המתוארת בפרק זה, נבנתה תורת העבודה לחקירת עבירות בתחום הפרטיות במידע, והתגבש צוות חוקרים בעלי מומחיות ייחודית בתחום. מחלקת החקירות היא הטרוגנית בהרכב המקצועי שלה בצורה לא אופיינית – והיא כוללת מארג של חוקרים–משפטנים ואנשי טכנולוגיה, רובם בעלי רקע טכנולוגי ייחודי בתחום בסיסי נתונים וראיות אלקטרוניות. מחלקת החקירות משמשת מעין "משטרת פרטיות במידע ממוחשב" המטפלת בתופעות של שימוש לא חוקי פלילי במידע אישי המעובד במערכות מחשבים.

בדו"ח השנתי של רמו"ט לשנת 2010 אוזכרה חקירה פלילית שנוהלה ע"י המחלקה, אלא שנכון למועד פרסום הדו"ח היה מוטל צו איסור פרסום על החקירה. הצו הוסר באוקטובר 2011 ולפיכך מובאת בדו"ח זה לראשונה תמצית פרשת "גניבת מרשם האוכלוסין של מדינת ישראל והפצתו באינטרנט", המכונה "פרשת הָאֶגְרוֹן".

בנוסף לפרשת הָאֶגְרוֹן, התקיימה פעילות חקירה פלילית נוספת במחלקה ואף זו מדווחת בפרק זה.

## תיק ה"אֶגרוֹן" – גניבת מרשם האוכלוסין והפצתו באינטרנט

### רקע

תיק החקירה בעניין גניבת מרשם האוכלוסין הוא תיק חקירה פלילית ראשון בישראל של פרשה מסועפת של שימוש לרעה במידע אישי. במרכזה עומד קובץ מחשב דיגיטלי שמקורו במאגר מידע של מרשם האוכלוסין במשרד הפנים, אשר בטכנולוגיה של ימינו ניתן לנשיאה על גבי אמצעי אחסון נייד אישי (Disk on-Key).

קיומה של התופעה נודע לציבור הרחב בחודש יוני 2007, עת נחשף בתקשורת דבר קיומו של אתר אינטרנט המאפשר הורדה (Download) של גרסה "פרוצה" של תוכנת איתור מידע המיושמת על בסיס נתונים ושמה "אֶגְרוֹן 2006" (להלן – **אֶגְרוֹן**) ואשר כללה מידע מקיף ממרשם האוכלוסין. תוכנה זו לא הייתה ידועה בציבור הרחב עד למועד זה.

המידע שנגנב ממשרד הפנים והופץ באֶגְרוֹן היה, נכון למועד גניבתו, המידע הרחב, האמין והמעודכן ביותר על אודות כלל אוכלוסיית מדינת ישראל מאז קום המדינה (למעלה מ-9 מיליון אזרחי מדינת ישראל, כולל בגירים, ילדים ונפטרים) וכלל שדות מידע רבים בכל רשומה ורשומה, לרבות קשרי המשפחה של כל אחד מתושבי המדינה.

רשויות מדינה רבות, לרבות הכנסת ומבקר המדינה, ואמצעי התקשורת, מתחו ביקורת קשה על עצם קיומה של תופעה זו בה מידע רגיש על כל אוכלוסיית המדינה חשוף לעין כל. ראוי לציין כי אירוע זה מיוחד אף ברמה הבינלאומית, שכן לא ידוע מקרה דומה בו נתונים כה רבים, מפורטים ועדכנים על כלל האוכלוסייה של מדינה שלמה זמינים לעין כל בצורה לא חוקית.

חומרת הדברים משתקפת, למשל, בהתבטאויות שנאמרות בסמוך לפרסום אודות האתר, המובאות מהסיפא של פרוטוקול ישיבת ועדת הפנים ביום 7/3/2007 ע"י יו"ר ועדת הפנים של הכנסת (דאז), ח"כ אופיר פינס:

***"...העניין של זליגת מרשם האוכלוסין כולו, הכול בחוץ, זה דבר מטורף...שתהיה פניה של משרד הפנים למשטרה, אני רוצה שהמשטרה תודיע על פתיחת חקירה, אלה לא דברים של מה בכך... זה עולם ומלואו...יש פה עסק עם עשרות נתונים בחוץ על כל בן אדם ואין משטרה אין חקירה אין העמדה לדין ואין עונשי מאסר אני מבקש שהדבר הזה ייכנס לסדר עדיפות גבוה...".***

לאחר הגשת תלונה רשמית ע"י משרד הפנים, משטרת ישראל פתחה בנובמבר 2007 בחקירה. במרץ 2008 נסגר תיק החקירה בעילה של עבריין לא נודע (על"ן), עקב חוסר יכולת להתחקות אחר עקבות העבריין בשל ריבוי הגופים מהם עשוי היה המידע לדלוף. משטרת ישראל הסבירה כי המידע של משרד הפנים מועבר (בצורה חוקית) ללקוחות חיצוניים רבים במשרדי ממשלה ובמגזר הפרטי. יש גורמים רבים, אלפים במספר, שהם בעלי גישה למידע זה ועל כן לא ניתן לאתר את הגורם העברייני.

בין לבין המידע שנגנב והועלה לאינטרנט קיבל חיים משל עצמו, וההד הציבורי והתקשורתי גרם לחשיפת קיומו לקהל גדל והולך, לרבות מעבר לגבולות מדינת ישראל.

רמו"ט יחסה לאירוע זה חשיבות מיוחדת עם גילויו. בדו"ח רשם מאגרי לשנת 2007, נאמר כדלהלן:

ב. משרד הפנים

1. במהלך השנה התפרסמו כתבות בעיתונות, לפיהן מידע מעודכן יחסית ממאגר המידע של מרשם האוכלוסין, לרבות תוכנת אחזור מידע המיושמת עליו ומאפשרת ביצוע חיתוכים שונים, זמין להורדה (download) מרשתות ביטורנט (BitTorrent). אפשרויות איתור המידע אודות אנשים המתאפשרות בתוכנה מרובות, וכוללות את האפשרות לאתר את מספר תעודת הזהות של אדם, כתובתו במרשם האוכלוסין, קשרי המשפחה שלו וכדי.
2. החי"מ פנה אל ראש מנהל האוכלוסין במשרד הפנים, אשר אחראי על איסוף המידע הנאגר מאגר המידע של מרשם האוכלוסין וניהולו, בבקשה לבירור אופן הטיפול של המשרד בתופעה המתוארת לעיל.
3. התשובות שהתקבלו עד ליום כתיבת דו"ח זה ממנהל האוכלוסין אינן מספקות, וחלקן מעידות על אי הכרה בחומרת האירוע – הן של המשרד והן של משטרת ישראל, אשר תלונה בנושא הוגשה אליה על ידי משרד הפנים.
4. ראוי לציין כי מעבר לרגישותו הבסיסית של המידע המתואר (מעמד אישי, קשרי משפחה וכדי) הרי שבהצלבתו עם מידע אחר, או בשימוש חכם בו, ניתן להגיע למידע רגיש ביותר אודות אדם ו/או לגרום לו נזק כלכלי. הסיבה לכך היא שמספר תעודת הזהות הוא המפתח הראשי (Primary key) במאגרי המידע השונים, וידיעתו מאפשרת הגעה על מירב פרטי המידע אודות אדם. לעיתים, ארגונים מסתמכים על ידיעת פונה מרחוק את מספר תעודת הזהות של האדם כהוכחה מספקת לזהותו של אדם ומתן גישה למידע (או ביצוע פעולות) – ובכך טמונה סכנה מרובה.
5. אירוע זה מעיד גם על החשיבות כי למחלקת האכיפה של הרשות יהיו הכלים המשפטים והטכנולוגיים לבצע פעולות חקירה מעין אלה בעצמה.

כגוף האמון על הגנת מידע האישי, רמו"ט לא יכלה להשאר אדישה לתופעה של הימצאות מרשם האוכלוסין של מדינת ישראל באינטרנט. עם תחילת הקמת מחלקת החקירות בשנת 2009, כשנתיים לאחר פרסומו הפומבי של האירוע ופרסום תוצאות החקירה המשטרתית ועל רקע עושר הדיון הציבורי בכנסת, בתקשורת ובדו"ח מבקר המדינה (וכפי שהסתבר, כארבע שנים לאחר גניבת המידע), הוחל בחקירת הפרשה.

תיק החקירה, כפי שיפורט להלן, הסתיים בפיצוח מלא של הפרשה וזיהוי המעורבים המרכזיים בביצועה והיה רצוף באתגרים חקירתיים וטכנולוגיים רבים. התיק פותח צוהר אל עולם רחב של עבריינות מידע, בעל מאפיינים ייחודים ומאתגרים במיוחד. זהו תיק שכל ענייננו גניבה, סחר והפצה של מאגרי מידע באופן בלתי חוקי, אשר נעשה ברובו על ידי מומחי מידע ומחשבים. הוא מעיד על הצורך החיוני בהבנה מעמיקה ומומחיות פרטנית בתחום מאגרי המידע, התפתחותם והכלים המתאימים להתמודד עם האתגרים שהם מציבים.

### האֶגְרוֹן – התוכנה ואתר ההפצה שלה

הפרשה נודעה לציבור עם פרסומו של אתר אינטרנט בכתובת www.agron2006.exe.co.il שכותרתו "אֶגְרוֹן 2006 פלוס" ביוני 2007. אדם שכינה עצמו "aRi" ("ארי") העלה באתר קישור למספר אתרי אחסון קבצים ברשות האינטרנט בהם ניתן להוריד את האֶגְרוֹן, הוראות התקנה ומדריך משתמש לתוכנה. לכך הוסיף מניפסט אידיאולוגי ואנרכיסטי המתריס ומזלזל במדינה, במוסדותיה, בפרטיות אזרחיה ובסודיותו של המידע על אודותם. האתר שימש כפלטפורמה לקידום השימוש בתוכנת האֶגְרוֹן, ובאמצעותו דאג ארי לתחזוקה שוטפת בהפצת התוכנה ונתוניה.

תוכנת האֶגְרוֹן הינה תוכנת חיפוש במאגר מידע אשר יושמה על בסיס נתונים הכולל למעלה מ-9 מיליון רשומות על אודות אזרחי מדינת ישראל. לאֶגְרוֹן ממשק משתמש המאפשר חיתוכים, למקד את איתור המידע על פי מאפיינים כלליים (תאריך לידה, מקום מגורים, שם, ארץ מוצא וכד') ולייצר רשימות מטרה מאופיינות. אֶגְרוֹן מאפשרת גישה לרשומה מסוימת על אודות אדם (על פי שמו ו/או מספר תעודת הזהות שלו ו/או פרמטרים אחרים), ומציגה את מארג המידע האישי על אודותיו (שם, מספר תעודת זהות, תאריך לידה, כתובת, טלפון וכד') ועל אודות קשרי המשפחה שלו (ילדיו, הוריו, אחיו ואחיותיו, בני/בת זוגו). מהצגת מידע זה על אודות אדם, ניתן להגיע לכל אדם אחר הקשור אליו, ולקבל את אותו מארג מידע גם לגביו. אין מגבלה על רוחב הטיול בפרטי המשפחה של אזרחי מדינת ישראל. בנספח ב' ניתן לראות צילומי מסך מוסברים של יכולות האֶגְרוֹן.

פרסום אתר האֶגְרוֹן בתקשורת עורר כאמור באופן מיידי עניין רב ותעבורת משתמשים נלהבת, וזו ליבתה את הפצתו באתרי הפצת מידע שונים ובתוכנות לשיתוף קבצים דוגמת Torrent ו-eMule. פעילות זו, אף שנעשתה למורת רוחה של רשויות המדינה העוסקות בנושא, אינה ניתנת, מעשית, לעצירה עם חריגתה מהיקף מוגבל.

## מהלך ראשון של החקירה – ממשרד הפנים ועד לאֶגרוֹן

במהלך 2009 נפתחת חקירה סמויה. מטעמים מובנים דו"ח זה אינו יכול לחשוף פרטים רבים על טיבה. חקירה גלויה, אשר לגביה התקבל צו איסור פרסום, נפתחה באוקטובר 2010.

התמונה הראשונית שהצטיירה הראתה כי המידע השלם והמלא אודות כל אזרחי מדינת ישראל, הפעילים והנפטרים, מתנהל על פי חוק על ידי מנהל האוכלוסין במשרד הפנים. מנהל האוכלוסין אחראי על מלאכת האיסוף, העיבוד, העדכון וההפצה של המידע, והוא מנוהל במערכת "אביב" המופעלת במיקור חוץ על ידי חברת HP ישראל. לפרטי מידע ממרשם האוכלוסין נדרשים לקוחות חיצוניים רבים, במגזר הציבורי והפרטי, המקבלים אותו על פי הסמכה חוקית. חלקם בעלי חיבור מקוון (on-line) למערכת "אביב" וחלקם מקבלים דו"חות מרוכזים של מידע ("גזירות") המועברים אליהם בקבצים.

החקירה העלתה כי במדינת ישראל מספר גורמים המקבלים גזירות כאמור, ובאמצעות עדכונים שוטפים מחזיקים בעותק מלא ועדכני של מרשם האוכלוסין.

הסתבר כי משרד הרווחה והשירותים החברתיים (להלן: **משרד הרווחה**) הינו אחד הלקוחות החיצוניים, אשר קיבל בשעתו גזירה מלאה של המרשם לצרכי עבודתו השוטפת ומאז הוא מקבל עדכוני מידע עיתיים הכוללים נתונים מעודכנים על כלל אוכלוסיית מדינת ישראל. הנתונים נטענו לבסיס נתונים ייעודי הכולל מאגר מקביל למרשם האוכלוסין במשרד הפנים בו מתנהלת מערכת "מיני מרשם" המשמשת את יישומי המחשב והמערכות התפעוליות הפנימיות במשרד.

ה"מיני מרשם" הוחזק בבסיס נתונים ייעודי שעל הקמתו והפעלתו היה אחראי איש מקצוע אשר תמך בהיבטי המידע של התפעול השוטף של משימות המשרד. אותו אדם היה עובד קבלן חיצוני אשר הועסק כמנהל תשתיות מערכות המידע במשרד הרווחה בדרך של מיקור חוץ. בחקירה התברר כי נגישותו החוקית למאגר המידע נוצלה למטרות פליליות והוא האדם אשר בשל מעשיו החלה שרשרת העבירות הפליליות המתוארת בפרק זה (להלן – העובד החשוד).

העובד החשוד נהג לקחת באופן קבוע עותק ממרשם האוכלוסין לביתו, ולעבוד על הנתונים שבו באופן פרטי ועצמאי. נמצאו אצל החשוד כל קבצי העדכון החודשיים שמקבל משרד הרווחה, והחומר כולו אוחסן באופן לא מוגן ומרושל במספר עותקים, במחשבים שונים בבית. דפוס הפעולה המתואר אפיין את שגרת עבודתו, שכן בחזקתו נמצאו מאגרי מידע שלמים נוספים ברמת רגישות גבוהה ביותר, כפי שמפורט בהמשך.

העובד החשוד סיים את עבודתו במשרד הרווחה בשנת 2006, אך בחזקתו השאיר חומרים רבים עימם בא במגע במסגרת תפקידו. בחקירה עלה כי עוד בעת עבודתו במשרד הרווחה ניהל החשוד באופן פרטי מספר פרוייקטי תוכנה. באחד מפרוייקטים אלה, הוא נשכר לצורכי שדרוג מערכת תורמים קיימת במוסד חרדי תורני. החקירה העלתה כי העובד החשוד התקין

במחשבי המוסד עותק של קובץ מרשם האוכלוסין, לרבות תוכנת איתור מידע מיוחדת שכתב לשימושו של איש המחשוב של המוסד החרדי (להלן – הלקוח החשוד). החקירה העלתה כי קובץ המרשם נמסר ע"י העובד החשוד ללקוח החשוד כמעין "בונוס".

הלקוח החשוד, הבין את ערכו של קובץ נתוני המרשם, והכין גרסה גולמית חדשה ונוחה של מאגר המידע, עם תוכנה אחרת המאפשרת אף היא חיפוש בנתונים. את התוכנה ומאגר המידע הוא טען על מדיה הפצת מידע ניידת והעבירה בין היתר, לחבר (להלן – המתווך החשוד).

המתווך החשוד איתר קונה פוטנציאלי (להלן – הקונה החשוד) ועניין אותו ברכישת קובץ המידע. תנאי העסקה נקבעו, ולאחר העברת התשלום הקונה החשוד קיבל את קובץ המידע מהמתווך החשוד.

על הקונה החשוד ניתן לומר כי "מאגריו – אומנותו". הוא אספן אדוק של מאגרי מידע ותוכנות, רבים מהם בלתי חוקיים, והוא עצמו עוסק בתחום התוכנה והמחשבים. הוא טייב והעשיר את קובץ המידע שקנה מהמתווך החשוד על בסיס קבצי מידע חלקיים וישנים של המרשם שהיו ברשותו, ועדכן אותו במידע של פנקס הבוחרים הארצי אשר הופץ לקראת הבחירות הארציות בשנת 2006. הקונה החשוד אף בנה תוכנת איתור מידע בשם "מרשם 2006" אשר יושמה על המידע האמור, ומכר אותה לעשרות מלקוחותיו.

במקביל, העביר הקונה החשוד את קובץ המרשם המטויב למתכנת עמו הוא קיים קשר מקצועי מוקדם על בסיס עניין משותף במאגרי מידע אישי (להלן – המתכנת החשוד). המתכנת החשוד בנה תוכנת איתור מידע משלו, ויישם את התוכנה על הקובץ המטויב. המאגר והתוכנה נקראו על ידו "אֶגְרוֹן פלוס 2006".

האֶגְרוֹן נכתבה לשימוש מסחרי חשאי ומוגבל, ועל כן יישם המתכנת החשוד עליה אמצעי הגנה כנגד שימוש בלתי מורשה. הוא הצפין את הנתונים, יישם מנגנון סיסמאות אשר נתנו על ידו באופן מוגבל, והעבירה רק למקורבים וללקוחות. למורת רוחו של המתכנת החשוד, בסמוך לשלבי ההפצה המסחריים הראשונים של האֶגְרוֹן, נפרצו על ידי מאן דהוא מנגנוני ההגנה של התוכנה ונוטרלו. הגרסה הפרוצה מצאה דרכה לידיו של טכנאי מחשבים, אשר כינה עצמו "ארי" (להלן – ארי).

פיצוח חלק זה נבע בעיקרו מחקירה אשר נוהלה בעיקרה על בסיס ניתוח המידע שנגנב והופץ, ניתוח של מארג נתוני תקשורת של חשודים וחקירה פרונטלית שהתקיימה בעת שעברה החקירה לשלב הגלוי שבה. לבו של שלב חקירה זה הוא הבנה וניתוח מעמיקים של רבדי המידע אשר נכללו באגרון, אשר בעזרתם ניתן היה להצביע על קישורם למי מהעבריינים.

### מהלך שני של החקירה – העלאת האֶגְרוֹן לאינטרנט על ידי "ארי"

דבר קיומה של גרסת אֶגְרוֹן פרוצה, מגיעה לידיעתו של החשוד כארי. באתר האינטרנט המוזכר לעיל, העיד על עצמו שהוא "שונא אנשים ששומרים הכל לעצמם".

בחודש מאי 2007 החל החשוד כארי להקים את מערך ההפצה של תוכנת האֶגְרוֹן הפרוצה, תוך הסתתרות סדורה ומתוכננת מאחורי זהות פיקטיבית ("aRi") ושימוש בעזרים טכנולוגיים שמטרתם טשטוש עקבותיו הדיגיטליים. אלה אכן הקשו עד מאוד את גילוי זהותו. על פי דברים שכתב באתר החשוד כארי, הוא היה ער לעובדה שרשויות האכיפה יחפשו אותו, כמו גם לפליליות מעשהו ולנזקים הקשים שנגרמו מכך, ועל כן עשה את כל שיכול היה להסתיר את זהותו האמיתית.

האתר שהקים החשוד כארי היה בן עשרות עמודים, ובו הוסברו האופנים בהם ניתן להוריד (Download) את אֶגְרוֹן, אפשרויות השימוש בה, ומניעיו להפצת התוכנה. בנוסף הוא העלה לאתר גרסה פרוצה של תקליטור פרוייקט השו"ת של אוניברסיטת בר–אילן, אשר זכה אף היא לעניין מיידי. האתר זכה לפופולאריות עצומה בציבור, וזו, כדבריו באתר, המריצה והלהיבה אותו ל"שפר" את האתר, להוסיף מדריכי שימוש ולהעשיר את תכניו.

עם התפתחות החקירה ופריצת הדרך אשר סופה היה מיפוי מלא של כל החוליות הקודמות בשרשרת (ממשרד הפנים ועד פיתוח האֶגְרוֹן), נותרה בפני צוות החקירה המשימה האחרונה של פיענוח זהותו האמיתית של ארי.

זו נחשפה בשל איתור טעות בתהליך ההסתתרות הדיגיטלית של החשוד על ידי צוות החקירה, אשר נתוני תקשורת לגביה הצביעו אל מקום עבודתו. לאחר הצלבה ואימות מידע מקיפים החשוד נתפס, נחקר, ובחצריו נתפסות ראיות אלקטרוניות רבות הקושרות בין זהותו הפיקטיבית כארי, וזהותו בעולם האמיתי.

### מאגר אימוץ ילדים

בבדיקת החומר שנתפס בביתו של העובד החשוד בגניבת המאגר ממשרד הרווחה עלה כי ברשותו של החשוד עותקים של מאגרי מידע אחרים בעלי רגישות גבוהה ביותר, אליהם נחשף במקומות בהם עבד או סיפק את שירותיו המקצועיים.

אחד ממאגרי המידע שאותרו בבית העובד החשוד הוא מן הרגישים ביותר בהיבט של פרטיות במידע שניתן להעלות על הדעת – מאגר נתוני מערכת תיעוד אימוץ הילדים במחוזות ירושלים, תל–אביב וחיפה, המשרתת את מערך האימוץ במשרד הרווחה. מדובר במערכת רגישה ביותר אשר מנהלת את כלל נתוני מערכת אימוץ ילדים בישראל, וכוללת פרטים מלאים על אודות ההורים הביולוגיים, ההורים המאמצים, הזהות החדשה של הילדים המאומצים וקישור בין כולם. קובץ נוסף במערכת כולל פרטים על אודות נשים בהריון אשר פונות לרשויות הרווחה בבקשה למסור את ילדן לאימוץ.

העובד החשוד היה גורם מרכזי בתכנון הארכיטקטורה של המערכת, ובמימוש פתרון של הפרדה בין נתוני המאמצים, נתוני המאומצים והוריהם הביולוגיים, לצורך צמצום האפשרות לחשיפת הקשרים בין שלוש הקבוצות. העובד החשוד השתתף בהקמת המערכת ותיחזק אותה. על אף הרגישות העצומה הברורה של המידע, מאגר המידע נלקח ונשמר בביתו.

במסגרת החקירה לא נמצאה עדות לחשש כי מאגר האימוץ הועבר מחזקתו של העובד החשוד לאחרים.

### נזקי פרשת האֶגְרוֹן

גניבת המרשם, פיתוח אֶגְרוֹן (ותוכנות דומות) והפצתה באינטרנט גרמו נזק חמור לציבור הישראלי, שמידע על אודותיו נאסף ומוחזק במאגרי מידע מכח החובה החוקית של ניהול מרשם האוכלוסין.

רמו"ט עסקה בהיבטים שונים של אֶגְרוֹן החל מגילוי הפצתה באינטרנט בשנת 2007 ונתנה ביטוי לכך בדו"חות השנתיים שלה החל משנת 2008. כגוף הרגולציה הפועל להגנת הפרטיות במידע, הופיעו אירועי שמוש באֶגְרוֹן בתיקי הפיקוח השונים שנוהלו על ידי רמו"ט. גם השיח הציבורי שנוגע למאגרי המידע הממשלתיים, ובפרט לעניין הקמתו של המאגר הביומטרי, הושפע מאירוע זה. כרשות המתמחה באבטחת מידע היה ברור לרמו"ט כי לאירוע זה גם השלכות משמעותיות על חוזקם של מנגנונים שונים להגנה על מידע וכי את תוצאותיו נראה במופעים שונים של הפעילות המשקית, ציבורית ופרטית כאחד. בפרק זה נבקש לפרט, אחד לאחד, את הנזקים אשר נגרמו.

הנזק הראשון, הברור לעיני כל המתבונן בתוכנה, הוא **פגיעה חמורה בפרטיות כלל אזרחי מדינת ישראל**. שימוש קצר בתוכנה ממחיש זאת באופן מיידי לכל מעיין בה. על כל אדם המצוי במאגר, ניתן לדעת באמצעות האֶגְרוֹן מארג פרטי מידע על אודותיו (שמו המלא, מספר תעודת הזהות שלו, כתובתו, תאריך לידתו, תאריך עלייתו לישראל אם עלה, שמות הוריו וילדיו ופרטיהם באותה רמת פירוט). בשל המידע המדויק על קשרי המשפחה של נושא המידע, ניתן לבצע חשיפה מעמיקה של כל מארג קשרי המשפחה של אותו אדם, ללא כל מגבלה על היקפה.

הנזק השני, עניינו **פגיעה חמורה ב**מעטפת **אבטחת המידע של כלל אוכלוסיית מדינת ישראל**. בראש ובראשונה, מדובר ב**החלשה משמעותית של מנגנוני ההגנה באמצעות סיסמאות** על שימוש במערכות מחשב. חיבור סיסמא על ידי אדם נעשה, לרוב, תוך שימוש בפרטי מידע על אודות סביבתו הקרובה (שמות ילדים וחברי משפחה אחרים, תאריכי לידה וכד') וזהו בדיוק המידע הקיים באֶגְרוֹן. מי שמנסה לפצח סיסמאות, מלאכתו קלה בהרבה אם הוא יודע את פרטי המידע המפורטים באֶגְרוֹן שכן עליו לבחון מרחב מידע קטן משמעותית מאשר

ניסיון לנחש סיסמא מקום בו המידע האישי הנ"ל אינו ידוע. שנית, הפצת האֶגְרוֹן גורמת ל**החלשת מנגנוני אימות זהות מרחוק (Remote Authentication)** של אנשים. בעקבות הפצת האֶגְרוֹן פורסמה על ידי רשם מאגרי מידע ביום 20.5.10 הנחייה האוסרת להסתמך על פרטי זיהוי הנמצאים באֶגְרוֹן בתהליכי אימות זהות של מתקשר מרחוק (בין אם בתקשורת מחשבים ובין אם בתקשורת טלפונית). רבים ממנגנוני אימות הזהות מתבססים על ידיעת המתקשר מרחוק פרטי מידע, האמורים להיות מוכמנים, כגון מספר זהות, תאריך לידה, שם של קרוב משפחה (סבים וסבתות, שם משפחה קודם של האם) וכד'. כל אלה הפכו למידע שהוא נחלת הכלל עם הפצת האֶגְרוֹן באינטרנט. פגיעה שלישית באבטחת המידע היא **ערעור מידת הביטחון שניתן לתת באמצעי הזדהות חזקה**, כגון כרטיסים חכמים ואמצעים אחרים, לרבות תעודת הזהות החכמה אשר אמורה להיות מונפקת במהלך שנת 2012. ערעור אמינות זה נובע מהקלת היכולת להציג תיעוד מזויף הנחזה להיות אמין, אשר על בסיסו יונפקו אמצעי הזדהות חזקים, כגון תעודות אלקטרוניות לחתימה אלקטרונית או תעודות להזדהות מול מערכות מחשב.

הנזק השלישי קשור **בפגיעה באמון הציבור באיכות שמירת המידע על אודותיו**, אשר מובילה להתנגדות להקמתם של מאגרי מידע ממשלתיים. דוגמת ההתנגדות למאגר הביומטרי. כרגולטור של מאגרי מידע, רמו"ט עוקבת אחר השיח הציבורי בנושא, ואין ספק שהוא מושפע מאירוע הפצת האֶגְרוֹן. עמדות אלה מובעות הן על ידי הציבור הרחב והן על ידי גורמי מקצוע בתחום אבטחת המידע אשר נחרדו לאור הפצת האֶגְרוֹן.

הנזק הרביעי עניינו שימוש במידע מהאֶגְרוֹן לצורך **עבירות גניבת זהות, זיוף והונאה**, שכן הפרטים הכלולים באֶגְרוֹן מקילים על גורמים עבריינים לתכנן ולבצע עבירות כאלה, שכן גופים רבים עדיין מסתמכים על ידיעת פרטי הזיהוי הנמצאים באֶגְרוֹן לצורך אימות זהות לפני מתן הרשאות לפעולות שונות או הסתמכות על מסמכים. המידע המקיף הקיים באֶגְרוֹן מקל על גורמים עבריינים ועויינים לזייף תיעוד ואף להשיג תיעוד אותנטי מגופים רשמיים (דוגמת משרד הפנים, משרד התחבורה, לשכת עורכי הדין), או רשמיים למחצה (כרטיסי עובד בארגונים, חברות במועדונים דוגמת "חבר" או "טוב").

הנזק החמישי עוסק בשימוש במידע מהמרשם לצורך **פעולות שיווק, העשרת מידע וסחר בלתי חוקי במידע**, שכן עושר המידע האישי באֶגְרוֹן הוא כר נרחב לפעולות שיווק בלתי חוקיות על פי חתכים שונים. על מקרה של שימוש כזה דווח בדו"ח רמו"ט לשנת 2009.

הנזק הששי הוא **סיכונים הקשורים לבטחון המדינה**, שכן להפצת מאגר תשתית מידע על אודות כלל אוכלוסיית ישראל, לרבות שמות, תאריכי לידה, קשרי משפחה יש השלכה על בטחון המדינה. דומה שאין צורך להכביר במילים על המשמעות שמרשם האוכלוסין המלא של מדינת ישראל זמין לכל שירות מודיעין ברחבי העולם, עויין ואף ידידותי. זמינות תשתית מידע מקיף זה על כל האוכלוסייה של מדינת היעד, לרבות בכירים במערכות שלטוניות,

הוא חלומו של כל קצין מודיעין, למטרות שונות – פגיעה פיזית, ניסיון גיוס ו/או סחיטה וכד'. בנוסף, היכולת לזהות אדם על פי מספר פרטי מידע לגיטימיים שהופיעו לגביו במקורות אחרים (כגון רשתות חברתיות, כתבות בעיתון וכד') מאפשרת להסיר מעטה אנונימיות שניתנת לאנשי בטחון, לעיתים בצורה קלה יחסית. גם לפגיעה המתוארת בחליפת אבטחת המידע המתוארת לעיל בהקשר של סיסמאות, יש כמובן גם היבט הקשור בביטחון המדינה, אם בשל ההקלה על פגיעה בתשתיות קריטיות (שהן מערכות אזרחיות בעלות ערך שפגיעה בהם נחשבת כסיכון בטחוני) ואם ישירות בתשתיות מחשוב ומידע צה"ליות, שגם הן עושות שימוש באמצעי אבטחת מידע אשר מתבססים, לעיתים, על מידע אישי של אנשי מערכת הביטחון.

הנזק השביעי הוא השימוש האפשרי במידע מאֶגְרוֹן לצורך **פעילות גביה, עיקוב וחקירה בלתי חוקיים** שכן הוא מאפשר להגיע בקלות אל חייבים, ואל קרובי משפחתם לצורך פעולות גביה, חוקיות ובלתי חוקיות. פיקוח שבוצע על ידי רמו"ט בשנת 2010 הצביע על תופעה זו. אֶגְרוֹן הוא, כמובן, כלי רב ערך לחוקרים פרטיים, אשר המידע בו משמש אותם באופן דומה לפעולות עיקוב המבוססות על מידע זה. בדו"ח זה מפורטת פרשת פיקוח אצל חוקר פרטי שעשה שימוש במידע זה.

הנזק השמיני שגורם האֶגְרוֹן הוא פוטנציאל **זיופי בחירות**, שכן הוא מקל ביותר לאתר בוחרים שאינם פעילים, או להגיע לבוחרים פונטציאליים שאינם מתכוונים לבחור ולהשתמש בזהותם. המידע הכלול באֶגְרוֹן יכול גם לשמש לפקוד אנשים למפלגה בלי ידיעתם והסכמתם, ובכך להשפיע על תוצאות הבחירות. כל העניינים המפורטים להלן נוגעים לליבו של ההליך הדמוקרטי.

הנזק התשיעי עניינו ה**משמעות כלכלית** של הפצת האֶגְרוֹן למשק, שכן בעקבותיו נדרשו תאגידים וגופי מדינה להתמודד עם פוטנציאל הנזק, ולהשקיע באמצעי אבטחת מידע על מנת להתגבר על הכשלים המתוארים.

### סיכום ומסקנות

פיצוח פרשת האֶגְרוֹן הוא אבן דרך משמעותית המבשרת על כינונה של מערכת אכיפה פלילית בתחום של מאגרי מידע המכילים מידע אישי. מערכת זו נדרשת למגוון כלים אפקטיבים להתמודדות עם פעילויות לא חוקיות כגון גניבה, מכר, סחר והפצה של מידע אישי. חומרת הפרשה מדגישה את הצורך וההכרח בקיומה של אכיפה פלילית ייעודית ומקצועית.

תיק החקירה חשף בשלמותו את רצף האירועים שקדם להפצת תוכנת האֶגְרוֹן על גבי רשת האינטרנט תוך מיפוי החוליות המעורבות במעשה, החל מיצירת קובץ המידע הגולמי שהופק על ידי העבריין ועד להעלאתו לרשת האינטרנט בשלמותו. המידע שנגנב עבר בין שרשרת של גורמים שונים, אשר לכולם עניין משותף ועבר עשיר של עיסוק טכנולוגי ומסחרי במאגרי מידע אישי.

חומר החקירה בתיק, כלל תפיסה, בדיקה, עיון וניתוח של כ–70 טרה–בייט של מידע שנתפס אצל החשודים והנחקרים בפרשה. אצל חשוד אחד נמצאו מאות מאגרים של מידע אישי, הכוללים גרסאות לא–חוקיות מוקדמות של מוצרים לחיפוש על מרשם התושבים, פנקסי בוחרים, מאגרי מידע של רשויות מקומיות, מאגרי טלפונים וכד', בהיקף של מיליוני רשומות.

תיק החקירה הועבר לפרקליטות ת"א עם המלצה להגיש הגשת כתב–אישום. בתחילת שנת 2012 נערכו שימועים לחשודים ובמאי 2012 הוגש כתב אישום בפרשה הכולל עבירות מחוק הגנת הפרטיות, מחוק המחשבים, ומחוק העונשין כדוגמת הוצאת מסמך ממשומרת חוקית וכן השמדת ראיות.

עבירות כדוגמת גניבת מרשם האוכלוסין מעוררות דאגה ומחייבות דיון מעמיק בשאלות של האופן שבו מפותחים ומנוהלים מאגרי מידע אישי בשירות הציבורי. כשלים רבים שהתגלו במהלך החקירה היו יכולים להמנע לו הייתה מיושמת תפישה, שהוצגה על ידי רמו"ט כבר בדו"ח שנת 2009 ומקודמת מאז על ידה, של "עיצוב לפרטיות" (Privacy by Design). לעניין זה חשוב שרשות האוכלוסין וההגירה תיישם תפישה זו בתכנון מערכת הידע אשר אמורה להחליף את מערכת "אביב", וכן יש לבחון את תפישת מתן אפשרות הגישה למידע לצרכנים אחרים מחוץ לרשות האוכלוסין וההגירה, דוגמת משרד הרווחה ממנו נגנב המידע בסופו של עניין.

עוד ראוי להדגיש, שמנגנוני פיקוח והגנה כאמור, עשויים להכשל נוכח הגורם האנושי, של העובד הסורר אשר יש לו נגישות כדין למידע לצורך תפקידו, אך מנצל אותה למטרה אחרת. לעניין זה יש לתת את הדעת לתהליכי המיון והסיווג של אנשים אשר יש להם נגישות מלאה למאגרי מידע, ואופן וידואה העיתי. פרשת האֶגְרוֹן המחישה את פוטנציאל הנזק העצום והבלתי הפיך של גניבת מידע אישי והפצתו, ומשקלו הסגולי הרב של הגורם האנושי בעבירות מסוג זה.

פיצוח פרשת האֶגְרוֹן מבהירה גם את ההצדקה לקיומה של רשות עצמאית המגינה על מידע אישי ועל פרטיות האזרח בעידן הדיגיטאלי. במישור החקירתי הפלילי, נדרשת יכולת חקירה מסורתית גבוהה המלווה במגוון יכולות נוספות מתחום טכנולוגית המידע ככלל, ומאגרי מידע ואבטחת מידע בפרט, ראיות אלקטרוניות והבנה של עולם כלכלת המידע. זהו עולם תוכן ייחודי, אשר מחייב מוקד ידע עצמאי שעומדים לרשותו הכלים החקירתיים והמשפטיים הנכונים להשגת מטרותיו.

**יובהר כי כל המפורט ביחס לתיק האֶגְרוֹן, מתבסס על הראיות שנאספו במסגרת החקירה הפלילית שנוהלה על–ידי רמו"ט, כפי שאלה מפורשות על–ידה. בעקבות הגשת כתב–האישום, עתידות להישמע הראיות בבית–המשפט אשר יקבע את הממצאים העובדתיים ואת המסקנות המשפטיות המחייבות.**

## תיק מ.נ.ר

תיק חקירה פלילית נוסף שנחקר בשנת 2011 ע"י מחלקת החקירות ברמו"ט קרוי "תיק מ.נ.ר". עיקרו של תיק זה הוא סחר במידע אישי שמקורו לא חוקי והוא אחד התוצרים של גניבת מרשם האוכלוסין של מדינת ישראל והפצתו באינטרנט. התיק דווח בדו"ח השנתי של רמו"ט לשנת 2010, עת טופל בכלים מנהליים פיקוחיים (בתקופת החקירה הראשונית, טרם היו לרמו"ט סמכויות חקירה פליליות מלאות).

תיק הפיקוח נסב על שימוש שלא כדין במאגר מידע בלתי חוקי על אודות כלל תושבי מדינת ישראל, לצרכים מסחריים. כבר בשלבים המקדמיים של ההפצה הלא חוקית של מרשם האוכלוסין באינטרנט, כמתואר בפרק הקודם, זיהו גורמים שונים את הפוטנציאל המסחרי הגלום בנתונים אלו, לצורך איתור חייבים לשם גביית חובות. מטבע הדברים, חייבים רבים נוטים להסתתר ולהעלם מאימת הנושים. פרטים על אודותם, ועל אודות קרובי משפחתם, והצלבות נוספות שניתן לעשות עקב זמינות הנתונים אישיים על כלל תושבי מדינת ישראל, הם מכרה זהב עבור קהל גובי החובות.

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 לא חוקי 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. מאגר המידע מכיל פרטים על אודות כ–7 מיליון אנשים וכולל כאמור ממשק לחיפוש מידע.

מ.נ.ר מכרה את רכיב איתור החייבים, בצירוף מאגר המידע הלא–חוקי, לכ–80 לקוחות שונים, מרביתם משרדי עורכי דין. כחלק מתהליך המכירה הותקן אצל הלקוח ממשק לחיפוש במאגר המידע וכן מאגר המידע עצמו.

כפי שדווח בדו"ח רמו"ט לשנת 2010, בחודש יוני אותה שנה שלחה רמו"ט הודעה לחברה לפיה הוחלט על הטלת 86 קנסות מינהליים בגין 86 מקרים שונים לגביהם נאספו ראיות מנהליות לפיהן החברה עשתה שימוש שלא כדין במאגר המידע הנ"ל באמצעות העברתו לאחר. מדובר בהפרה של הוראת סעיף 8(ב) לחוק הגנת הפרטיות, המהווה עבירה על סעיף 31א(א)(1) לחוק הגנת הפרטיות, וזו ניתנת להמרה בקנס מנהלי על פי חוק העבירות המנהליות, התשמ"ה–1985 (להלן – חוק העבירות המנהליות).

חברת מ.נ.ר והעומדים בראשה מימשו את זכותם שבחוק העבירות המנהליות וביקשו להישפט חלף הקנס. בשל כך, נדרשה בשנת 2011 מחלקת החקירה לקיים חקירה פלילית בנוגע לתיק

זה, ונגבו הודעות מהגורמים המעורבים. הממצאים מצביעים על מכירת מאגר מידע לא חוקי, במסגרת התוכנה שפותחה לעשרות רבות של לקוחות.

התיק הועבר לטיפול בפרקליטות חיפה (פלילי).

כאמור בדוח רמו"ט ל–2010 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 עבירות, לרבות הפעלת סנקציות אישיות כלפי נושאי משרה בתאגיד. החברה ומנהליה שימשו כחוליית ההפצה של מידע ותוכנות, שעיקר פעילותן מבוסס על עותק לא חוקי של מאגר מידע, אודות אזרחי מדינת ישראל.

## הנחיות רשם מאגרי מידע

במהלך שנת 2011 המשיכה רמו"ט לפרסם הנחיות בתחום הגנת הפרטיות. מטרת הנחיות אלה להבהיר לציבור את פרשנות הדין החל בהקשר של פעילות עיבוד מידע ספציפיות, וליידע אותו על אופן הפעלת הסמכויות המוקנות לרשם בעתיד בהקשר העניין נשוא ההנחיה.

### כרטיס חכם בתחבורה ציבורית

בשנת 2011 נמשכה העבודה על הסדרת היבטי הפרטיות בכרטיס חכם לתחבורה ציבורית (רב–קו), וזאת בהמשך להליכי פיקוח שקיימה רמו"ט בנושא ודווחו בשנת 2010. פרוייקט הכרטיס החכם בתחבורה הציבורית מובל על ידי משרד התחבורה, והוא החל לפעול עוד בטרם התקיימה חקיקה סדורה בהקשרו.

המחלקה המשפטית של רמו"ט היתה מעורבת בלימוד מעמיק של ההיבטים הטכנולוגים הקשורים בפרוייקט, על מנת לסייע ב"עיצוב לפרטיות"(Privacy By Design) שלו, תהליך המקודם על ידי רמו"ט בהקשר של כל יוזמה אשר במרכזה נאסף מידע אישי.

שיתוף הפעולה עם משרד התחבורה התנהל בקצב לא מספק, והודות לסיוע של משרד המשפטים והצורך להשלים את החקיקה, הוא זכה לקידום. סיוע משמעותי להליך זה התקבל מדיון בועדת הכלכלה של הכנסת, אשר נדרשה לנושא עם תחילת הדיונים בהצעת החוק לתיקון פקודת התעבורה (מס' 100) (רישיון מפעיל וכרטיס חכם), התשע"א–2010 בחודש פברואר 2011.

באפריל 2011 הפיצה רמו"ט הנחיית ביניים שמטרתה הסדרת היבטים הקשורים בנושאי הליבה של החוק בהקשר של הכרטיס החכם בתחבורה הציבורית, עד להשלמה של החקיקה, ובדגש על אופן איסוף המידע, מטרות השימוש במידע, וחובות אבטחת המידע. במקביל המשיכו להתנהל דיונים עם משרד התחבורה לגבי אופן עיצוב הפרוייקט באופן כללי, ואופן הסדרת הכנסת טכנולוגיה זו תוך מיזעור סיכוני הפרטיות שלה.

נכון לסוף שנת 2011 הטיפול בנושא זה לא הושלם. נכון למועד פרסום הדוח, ולאחר תיאום בין–משרדי, פורסמה הנחיית רשם מאגרי מידע בנושא זה, שמטרתה הסדרת הנושא עד להשלמה של החקיקה.

## מיקור חוץ (OUTSOURCING)

בנובמבר 2011 פורסמה לאחר תהליך הכנה מקיף, אשר כלל שימוע ציבורי והתייעצות עם גורמים שונים, הנחיית רשם מאגרי במידע בנושא מיקור חוץ (Outsourcing) במאגרי מידע. הנחייה זו מצ"ב כנספח ג' לדו"ח זה.

ההנחיה נועדה להנחות ארגונים לגבי האופן הראוי, לפי פרשנות רשם מאגרי מידע, לפעול בעת ביצוע פעולות עיבוד מידע במיקור חוץ, באופן המסדיר את החובות החלים בעת עיצוב השירות, הסדרתו המשפטית והארגונית והבקרות הנדרשות בידי הארגון.

במהלך שנת 2012 צפויה רמו"ט לעקוב אחר הטמעת הנחיה זו במגזרים העסקי והציבורי, ולהחל להפעיל את סמכויות הפיקוח שלה בעניין זה.

## טיוטה: פרטיות והגנת מידע בחוזה הלקוח של חברות הטלפון הסלולארי (רט"ן)

הצורך להכנת הנחיה בנושא של פרטיות והגנת מידע בחוזה לקוח של חברות הרט"ן עלה לאור קשיים בהם נתקלה רמו"ט בהליכים לאישור חוזי חברות הסלולר בבית הדין לחוזים אחידים.

בגיבוש טיוטת ההנחיה הוטמעו לקחים מפיקוח רוחבי במגזר הסלולר שערכה מחלקת רישוי פיקוח מנהלי בשנת 2010, וכן מעמדות שנתבקשו מרמו"ט לגבי מספר תובענות ייצוגיות שהוגשו בנושא. בנוסף, הסתמכה רמו"ט על פרסומים ביחס לאיסוף נתוני המיקום המתבצע במכשירים הסלולריים.

הפרק השני של טיוטת ההנחיה מסביר את החובה לקבלת הסכמת הלקוח לשימוש במידע על אודותיו, תוך הבחנה בין שימוש הדרוש לאספקת השירות הבסיסי לבין שימוש נטול זיקה לשירות זה; הפרק השלישי מצביע על המגבלות בתוכן ובסוג ההסכמות שניתן לבקש מהלקוח בחוזה אחיד, ועל הצורה בה צריכה להתבקש ההסכמה (OPT IN – OPT OUT);

הכנת הטיוטה הסתיימה בשלהי 2011 והיא הופצה בפברואר 2012 להערות ראשוניות של חברות הטלפון הסלולארי, משרד התקשורת ומחלקת יעוץ וחקיקה במשרד המשפטים.

## טיוטה: תחולת חוק הגנת הפרטיות על פעולות מכוני מיון לקבלה לעבודה

בחודש ינואר 2011 פרסמה רמו"ט להערות הציבור טיוטת ההנחיה המבהירה את מעמדם של המעסיקים ומכוני המיון ביחס למידע הנאסף על המועמדים לעבודה במסגרת מבחני מיון. ההנחיה מפרטת אלו שימושים מותר למכונים לעשות במידע האישי הנצבר אצלם, מה תוכן ההסכמה שהמכון נדרש לקבל מן המועמדים כתנאי לעיבוד המידע, וכיצד על המעביד והמכון לממש את זכותו של המועמד לעיין במידע האישי שנאסף עליו ולתקנו.

בעקבות ההערות שהתקבלו, פרסמה רמו"ט בחודש יולי טיוטה מעודכנת ולאחר פרסומה קיימה רמו"ט "שולחן עגול" בהשתתפות כל המגיבים לטיוטת ההנחיה: בדיון השתתפו נציגים של הסתדרות הפסיכולוגים, האגודה לזכויות האזרח, איגוד הבנקים, המוסד לביטוח לאומי ומכוני המיון. בהמשך, עד לסוף שנת 2011 המשיכה וניהלה רמו"ט סדרה של מפגשים עם הגורמים הנוגעים בדבר.

במקביל העבירה רמו"ט הערות בנושא זה במסגרת הטיפול בעתירה כנגד חוקתיות חוק היישובים הקהילתיים, שעוסק בשימוש במכוני מיון בקבלה ליישובים קהילתיים.

עיקר ניסוח ההנחייה הסתיים בשלהי שנת 2011 והיא התפרסמה בתחילת מרץ 2012.

## איסור שימוש במידע בדבר הטלת עיקול אצל צד שלישי

בחודש ינואר 2011 התפרסמה להערות הציבור טיוטת הנחיה שעניינה איסור שימוש במידע בדבר הטלת עיקול אצל צד שלישי, וזאת בעקבות ממצאי פיקוח בחברת אי.די.איי חברה לביטוח, אשר דווחו בדו"ח לשנת 2010.

בחודש ספטמבר 2011 פרסמה רמו"ט את נוסח הסופי של ההנחייה, וזו נועדה להבהיר כי גורם המקבל ממערכת ההוצאה לפועל, מערכת בתי המשפט או רשויות המדינה צו עיקול כצד שלישי המחזיק אצלו כספים או נכסים המגיעים לחייב נשוא העיקול – אינו רשאי לעשות במידע שימוש אלא לצורך קיום מטרת צו העיקול.

במהלך התקופה שבין פרסום טיוטת ההנחיה ופרסום הגרסה הסופית הוגשה לבית המשפט לעניינים מנהליים עתירה כנגד החלטת הרשם המסתמכת על העמדה הבאה לביטוי גם בהנחיה. לאחר פרסום ההנחיה ביקשה העותרת לתקן את העתירה.

## טיוטה: השימוש במצלמות מעקב

בחודש דצמבר 2011 פרסמה רמו"ט להערות הציבור טיוטת הנחיה בנושא "שימוש במצלמות מעקב ובמאגרי הצילומים הנקלטים בהן". ההנחייה מיועדת להבהיר את תחולתם של דיני הפרטיות והגנת המידע על השימוש במצלמות המעקב, ומציגה את עקרונות השימוש במצלמות לאור דיני הפרטיות. הטיוטה מבוססת על חוות דעת משפטית בנושא "מצלמות מעקב – הדין החל ואופן השימוש" שפרסמה רמו"ט בשלהי שנת 2010.

במהלך השנה השתתפו נציגי רמו"ט בדיונים במחלקת יעוץ וחקיקה (חקיקה) במשרד המשפטים במטרה לגבש נוהל להפעלת מצלמות מעקב בערים המשתתפות בפרוייקט "עיר ללא אלימות", והביעה את הערותיה על תנאי מכרז מסגרת מס' 16.11 לעניין "הקמת מערך טכנולוגי, מצלמות סנסורים ומוקדי שליטה ובקרה עירוניים" שפורסם בידי המשרד לבטחון הפנים.

נושא מצלמות מעקב במרחב הציבורי עלה גם במסגרת הליך פיקוח על אופן השימוש במערכת המצלמות בעיריית אשקלון. בנוסף, התריעה רמו"ט בפני עיריית תל אביב על פרסומים בדבר כוונת אתרים, החברה לפיתוח אתרי תיירות בתל אביב, לפרוס עשרות מצלמות בחופי העיר באופן בלתי מידתי החורג, לדעת רמו"ט, מהוראות הדין.

## טיוטה: הגנה על מידע אישי במקום העבודה - מדריך למעבידים ולעובדים

בראשית שנת 2011 סיימה המחלקה המשפטית של רמו"ט הכנה של טיוטת מדריך הכולל ריכוז מקיף של עקרונות הגנת המידע במסגרת יחסי עבודה, ומטרתו לסייע למעסיקים ליישם אותם בהתאם להוראות חוק הגנת הפרטיות ולעזור לעובדים להכיר את זכויותיהם. המדריך לא הופץ לציבור שכן בחודש פברואר פורסם פסק דינו של בית הדין הארצי לעבודה בעניין איסקוב (ע"ע 90/08 טלי איסקוב ענבר נ' מדינת ישראל ואח') בו נקבעה הלכה מקיפה ותקדימית בסוגיית הפרטיות במקום העבודה.

רמו"ט השתתפה במהלך השנה בדיונים במחלקת ייעוץ וחקיקה בעניין אופן יישומה של הלכת איסקוב ובשאלת עמדת המדינה בעתירה שהוגשה בעניינה לבג"צ (העתירה נמחקה בחודש דצמבר 2011). לנוכח העתירה שהייתה תלויה בעניינה ולאור חוסר הבהירות בדבר פרשנותה, נמנעה רמו"ט לפרסם את טיוטת המדריך למעבידים ולעובדים בשנת 2011 וזו פורסמה בשנת 2012.

# רישום מאגרי מידע

## נתונים

בשנת 2011 הוגשו **532** בקשות רישום מאגרי מידע לרשם. נתון זה מהווה עליה של כ–**45**% בבקשות הרישום החדשות ביחס לשנת 2010. בהשוואה לנתוני השנתיים הקודמות ישנה מגמה בולטת של גידול בכמות בקשות הרישום המוגשות לרמו"ט ביחס לשנים קודמות (בשנת 2009 – 408; בשנת 2010 – 366).

הגידול בכמות בקשות הרישום המוגשות מוסבר ע"י פעילויות שמבצעת רמו"ט שגורמות להעלאת מודעות לנושא הגנת הפרטיות בניהול מאגרי מידע בקרב גופים במשק, שבעקבותיה הם יוזמים או נדרשים לרישום מאגרי המידע שלהם. דוגמא לכך היא הסדרת לשכות פרטיות להעסקת עובדים זרים בענף הסיעוד ע"י משרד התמ"ת ופרוייקט כרטיס חכם בתחבורה הציבורית של משרד התחבורה.

במסגרת פרוייקטים אלו נדרשו הגופים הפרטיים המנהלים מאגרי מידע לשימושים שנוגעים למתן שירותים לציבור המפוקחים ע"י משרדי הממשלה, לרשום את מאגריהם בפנקס מאגרי המידע ולעמוד בחובות המהותיות שקובע החוק הנובעות מכך שהם מנהלים מאגרי מידע אלו.

א. במהלך שנת 2011 אושר רישומם של כ–300 מאגרי מידע.

ב. בנוסף במהלך שנת 2011 עודכן רישומם של כ–4,200 מאגרים. עדכון כולל למשל שינוי פרטי בעל המאגר, שינוי במינוי מנהלים למאגר, העברות בעלות במאגר עקב מיזוג או מכירה או מחיקת המאגר.

## גביית אגרות

במהלך שנת 2011 נגבו כ– 2,210,000 ₪ 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 הן מוטלות על הגורמים שיש בידם מאגרי מידע.

## רישום מאגר מידע לשירות GOOGLE STREET VIEW

בחודש אוגוסט 2011 קיבלה רמו"ט את בקשת חברת גוגל לרישום בפנקס מאגרי המידע, כנדרש בסעיף 10 לחוק הגנת הפרטיות, של מאגר מידע לצורך הפעלת שירות Google Street View (GSV) – יישום המאפשר למשתמשי שירות המפות Google Maps לצפות בצילום פנורמי סטטי של רחובות ושטחים ציבוריים אחרים המופיעים בשירות המפות.

בהתאם לסמכויות המסורות לו בחוק, בחן הרשם את בקשת גוגל לרישום המאגר, והחליט לאשר אותה בכפוף לקיומם של תנאים מפורטים המיועדים לשמור על זכויותיו של הציבור הישראלי, במיוחד נוכח העובדה שמקום מושבה של גוגל נמצא מחוץ לתחום השיפוט של ישראל. אלה עיקרי התנאים:

א. סמכות שיפוט אזרחית – Google INC מינתה את חברת גוגל ישראל כמורשה לקבלת כתבי בי דין מטעמה בישראל, לפי סעיף 478 לתקנות סדר הדין האזרחי, התשמ"ד – 1984 באופן שיאפשר לפתוח בישראל הליכים משפטיים אזרחיים נגד החברה האמריקאית.

ב. סמכות שיפוט מנהלית ופלילית – גוגל התחייבה שלא לטעון כנגד סמכות רמו"ט להפעיל נגדה הליכים פליליים או מנהליים בקשר להפעלת שירות GSV.

ג. בקשות לטשטוש – אתר האינטרנט של שירות GSV יציע מנגנון מקוון יעיל ואמין לבקש טשטוש נוסף של דמויות, לוחיות רישוי ובתי מגורים לאחר פרסומן.

ד. שקיפות – גוגל פרסמה לציבור באינטרנט ובעיתונות הסברים על מהות השירות, על זכויות המצולמים, ומידע כללי על מסלול הצילומים המיועד.

# פרק ז' דין וחשבון של רשם גורמים מאשרים לפי תקנה 16 לתקנות חתימה אלקטרונית (ניהול גורם מאשר וניהולו), התשס"ב-2002

## כללי

רשם גורמים מאשרים (בפרק זה – הרשם או רשם גורמים מאשרים) אחראי מכוח חוק חתימה אלקטרונית, התשס"א–2001 (בפרק זה – החוק או חוק חתימה אלקטרונית) על ניהול מרשם הגורמים המאשרים והפיקוח עליהם.

עד 10 בספטמבר 2011 שימש בתפקיד הרשם עו"ד עמית אשכנזי, וזאת במקביל להיותו היועץ המשפטי של רמו"ט. החל מיום זה מונה ראש רמו"ט, יורם הכהן, לרשם לאחר שנקבע על ידי הייעוץ המשפטי של משרד המשפטים כי אין במינוי זה חשש לניגוד עניינים, לאור עיסוקו של עו"ד הכהן בתחום החתימה האלקטרונית טרם מינויו לתפקיד ראש רמו"ט. תהליך זה השלים את הקבוע בהחלטת הממשלה על הקמת רמו"ט, לפיה ראש רמו"ט אמור לשאת בתפקיד שלושת הרשמים[3] שנכללו ברמו"ט.

הפיקוח על הגורמים המאשרים מחייב הבנה טכנולוגית מעמיקה בתחום החתימה האלקטרונית, התשתית הטכנולוגית המשמשת בבסיסה (PKI – Public Key Infrastructure) והיכרות עם מבנה מערכות המידע ומערך אבטחת המידע של הגורמים המאשרים. כמו כן נדרש ידע מקצועי במגוון של תקנים מקצועיים בינלאומיים והבנה בתחום הקריפטוגרפיה (תורת ההצפנה). הפיקוח מצריך שעות עבודה מרובות וניתוח תהליכי עבודה מורכבים וממושכים.

הפעלת סמכויות הפיקוח של רשם גורמים מאשרים מבוצעת על ידי הרשם בסיוע צוות מפקחים ממחלקת רישוי ופיקוח מנהלי ברמו"ט, אשר עוסקים במקביל גם בפיקוח בנושאי הגנת פרטיות ונתוני אשראי. בשנת 2011 כלל הצוות הכשיר לנושא החתימה האלקטרונית 5 מפקחים (כולם בעלי רקע במשפט וטכנולוגיה) בלבד. בשנת 2011 נעזר הרשם בשירותי ייעוץ ממומחה מקצועי חיצוני בהיקף של 300 שעות עבודה.

3 רשם מאגרי מידע מכוח חוק הגנת הפרטיות, התשמ"א–1981, רשם שירותי נתוני אשראי ומידע על עוסקים מכוח חוק שירותי נתוני אשראי, התשס"ב–2001 ורשם גורמים מאשרים מכח החוק.

בשנת 2011 טופלו ע"י הרשם וצוות הפיקוח שתי בקשות רישום של גורמים מאשרים חדשים: חברת פרסונל איי.די בע"מ והגורם המאשר הממשלתי. בקשות אלה חייבו הקדשה של מספר רב של שעות עבודה. בנוסף לכך, לפיקוח באתרי הגורמים המאשרים, הוקדשו בשנת 2011 כ–21 ימי עבודה בהם נכחו צוותים של שניים עד שלשה מפקחים.

**נוכח מצב דברים זה סבור הרשם, כי יש להקצות כח אדם ייעודי לתחום החתימה האלקטרונית, בנוסף על כח האדם שקיים ברמו"ט כעת.**

## נתונים

בתחום חתימה אלקטרונית טופלו ברמו"ט 14 תיקי פיקוח בשנת 2011, מתוכם 10 תיקים כהמשך מהשנה הקודמת, ו– 4 תיקים חדשים.

לרשם גורמים מאשרים הוגשו 2 תלונות בשנת 2011.

חלוקת התיקים לפי סוגיהם היא כדלקמן –

| סוג התיק | כמות |
|---|---|
| תיקי פיקוח בבקשות שהוגשו לאישור הרשם | 9 |
| תיקי פיקוח לבקרה ביוזמת הרשם | 5 |
| תיקי פיקוח בעקבות תלונה | 0 |
| **סה"כ** | **14** |

## גורמים מאשרים רשומים

מרשם גורמים מאשרים לפי סעיף 9(ב) לחוק חתימה אלקטרונית, התשס"א–2001 בסוף שנת 2011 הוא כדלהלן:

| שם | תאריך רישום | פרטי התקשרות | כתובת אתר האינטרנט של הגורם המאשר |
|---|---|---|---|
| **פרסונל איי.די. בע"מ** | 7.7.2011 | דרך דוד בן גוריון 34<br>רמת גן 52573<br>טל' 073–2900047<br>פקס: 073–2900379 | www.personalid.co.il |
| **קומסיין בע"מ** | 13.2.2003 | קריית עתידים בנין 4<br>ת.ד. 58007<br>תל אביב<br>טל' 03–6443620<br>פקס 03–6474206 | www.comsign.co.il |

# בקשות רישום חדשות של גורמים מאשרים

## חברת פרסונל איי.די בע"מ

כמדווח בדו"ח רשם גורמים לשנת 2010, במהלכה החל טיפול בבקשת רישום חדשה של חברת פרסונל איי.די בע"מ (לשעבר סקיורנט גורם מאשר בע"מ). בבקשה זו יושמה לראשונה הנחיה 2–2010 שנועדה לתת בידי הרשם והגורם המאשר שיקול דעת רב יותר באשר לאופן המימוש הטכנולוגי של השירות, תוך שמירה על תכליות ומטרות החוק.

בשנת 2011 הסתיים תהליך בדיקת בקשת הרישום של פרסונל איי.די. במסגרת הטיפול בבקשת הרישום נערכו בדיקות מקיפות למסמך הנהלים של החברה (תקנון השירות), לנהלי העבודה שלה, להיבטי אבטחת מידע לוגיים ופיזיים בפעולתה וליישומה בפועל של הנחייה 2–2010 האמורה.

רישומה של פרסונל איי.די במרשם הגורמים המאשרים אושר בתנאים ביום 7.7.2011. לאחר מתן אישור הרישום, המשיכו מפקחי הרשם בבחינת עמידתה של חברת פרסונל איי.די בתנאים שונים שפורטו באישור שניתן לה.

## הגורם המאשר הממשלתי

נוכח החלטת המדינה להקים גורם מאשר ממשלתי, הוגשה בסוף שנת 2010 לרשם בקשה לרישום גורם מאשר זה (להלן – הגמ"מ). הגמ"מ מוקם בשיתוף פעולה של יחידת ממשל זמין במשרד האוצר ורשות האוכלוסין, ההגירה ומעברי הגבול. מערך הגורם המאשר הממשלתי מתוכנן לספק שירות הנפקת תעודות אלקטרוניות לחתימה אלקטרונית מאושרת שישולבו בתעודת הזהות החכמה שתנפיק המדינה לאזרחים.

במהלך שנת 2011 נמשך הטיפול בבדיקת בקשת הרישום של הגמ"מ. במסגרת הטיפול בבקשת הרישום נבדקים מסמך הנהלים של הגמ"מ, נהלי העבודה המפורטים שלו, היבטי אבטחת מידע לוגיים ופיזים בפעולתו ובמתקניו השונים. הליך בחינת בקשת הרישום ימשך בשנת 2012, בד בבד לתהליך הקמת המסגרת הטכנולוגית והניהולית של הגמ"מ והתקדמות פרוייקט תעודת הזהות החכמה.

# פעולות פיקוח

## הגורם המאשר קומסיין בע"מ

בשנת 2011 טופלו 5 תיקי פיקוח יזומים ע"י הרשם מול חברת קומסיין, ובהם המשך בירור תקלת אי פרסום CRL, יישום הנחיות רשם 2/2010 ו– 4/2010 והפרה שעניינה הגבלת אחריותה של קומסיין בתעודות המונפקות על–ידיה. בנוסף, טופלו 7 בקשות של קומסיין הקשורות בהרחבת פעילותה כגורם מאשר.

### בקשות לאישור הרשם

בשנת 2011 טיפל הרשם ב–7 בקשות של הגורם המאשר קומסיין. 3 מהן עסקו באישור גורמים רושמים נוספים שישמשו כנציגי קומסיין בתהליך הנפקת תעודות אלקטרוניות. אחת עסקה בחידוש אישור הגורם הרושם ההוצאה לאור של לשכת עוה"ד המשמשת כנציגת קומסיין מזה מספר שנים.

בשנת 2011, כמו בשנת 2010, בשל הגידול בביקוש לתעודות אלקטרוניות, ביקשה קומסיין להוסיף אתרים פיזיים לאתרים בהם היא נותנת שירות. בהתאם טופלה בקשה לאישור מתחם פעילות הנפקה נוסף של קומסיין בירושלים.

בנוסף טופלה בקשה לאשור תהליך עבודה המאפשר חידוש תעודה אלקטרונית מרחוק באופן שלא מחייב הגעה חוזרת של הלקוח לאתר הגורם המאשר.

הטיפול בכל הבקשות שילב בחינה של החוק, התקנות, מסמך הנהלים (CPS) והנהלים המפורטים של הגורם המאשר. נבחנו תכניות בינוי ואבטחה פיזית, ארכיטקטורת רשת מחשבים ותכניות אבטחה לוגית, וסוגיות של רמת השירות שיינתן לצרכנים. בחלק מהמקרים יצאו צוותי מפקחים לאתרים השונים וביצוע פיקוחים במקום.

הבקשות להקמת אתר DRP, לחידוש אישור הגורם הרושם הוצאה לאור של לשכת עוה"ד והקמת סניף הנפקות בירושלים, אושרו בשנת 2011.

הליך הבחינה של יתר הבקשות נמשך בשנת 2012.

### עיצום כספי בגין הפרה של הנחיית הרשם

כפי שדווח בדו"ח השנתי לשנת 2010, בספטמבר אותה שנה אישר הרשם, לאחר תהליך בחינה מקיף, את מסמך הנהלים החדש של חברת קומסיין בהתאם לתקנות לפי החוק. מסמך הנהלים של הגורם המאשר מהווה את תקנון השירות שלו, ומסדיר את התחייבויותיו והצהרותיו כלפי לקוחותיו וכלפי מי שמסתמך על התעודה האלקטרונית שהנפיק.

כפי שדווח, במסגרת אישור מסמך הנהלים אושר 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. מסמך הנהלים הקודם של קומסיין לא הסדיר נושא זה.

במסגרת פיקוח שקיים הרשם עקב תלונות, לאחר סבב דיונים מקיף שנערך עד להסדרה של הנושא במסמך הנהלים, הנחה הרשם את קומסיין בדצמבר 2009 שלא להנפיק תעודות לשימוש תאגידי כאמור, עד הסדרת הנושא במסמך הנהלים המעודכן שלה. בקשות חוזרות של קומסיין לאפשר מהלך כאמור במהלך 2010 נענו בתשובה מפורשת הקושרת בין נושא זה לאישור מסמך הנהלים.

בפיקוח שערך הרשם התברר בהתאם לתצהיר שמסר מנכ"ל החברה, כי בתקופה שבין דצמבר 2009 למועד אישור מסמך הנהלים החדש הונפקו 9 תעודות אלקטרוניות לחתימה על שרתים, בניגוד להנחייה כאמור.

שתיים מההפרות בוצעו לאחר כניסתו לתוקף של תיקון מספר 2 לחוק, בו הוספה לרשם סמכות להטיל עיצום כספי על גורם מאשר בשל אי מילוי אחר הנחייה של הרשם. יוזכר כי סעיף זה הוסף ביוזמת ועדת המדע והטכנולוגיה במהלך הדיונים על תיקון מספר 2 לחוק, על רקע דיווחי הרשם לועדה על אודות חוסר הציות של הגורם המאשר והעדר כלי אכיפה מתאימים.

בהתאם לכך, עשה הרשם שימוש בסמכותו, ובתום שימוע, הוטלו בשנת 2011 שני עיצומים כספיים בסך 71,600 ₪ כל אחד בגין שני אירועי הפרה של ההנחיה. בקשות לעיון מחדש או שינוי סכום הקנס לא התקבלו על ידי הרשם, והעיצומים שולמו ללא ערעור משפטי.

### אי קיום התחייבות בנושא הגבלת אחריות

במסגרת דו"ח 2010 דווח על הנחיית הרשם בנושא איסור על שינוי הגבלת האחריות בתעודות, ועל הפרת הנחייה זו.

בעקבות הפרת הנחייה זו, ופיקוח הרשם, חזרה בה קומסיין משינוי הגבלת האחריות כלפי לקוחותיה, באופן שהגבלה זו אינה תקפה עוד.

הודעתה של קומסיין פורסמה באתר האינטרנט של הרשם.

### שימוע בשל כוונה להתלייה של הרישום בשל אי עמידה בתנאי סף לרישום גורם מאשר

במסגרת בחינת עמידת קומסיין בהנחייה 2010–2, התברר לרשם במרץ 2011 כי למרות מצגים מפורשים של קומסיין ושל המבקר הבלתי תלוי מטעמה, נכלל במערכותיה מזה זמן רב רכיב

קריטי במערך הנפקת התעודות האלקטרוניות שאינו מקיים את הוראות תקנה 5 לתקנות העמידה בתקן Common Criteria.

על רקע האמור, זומנה בחודש אפריל קומסיין לשימוע בטרם התלייה של רישומה במרשם. לאחר השימוע קבע הרשם כי קומסיין הפרה את הוראות התקנה, ואף לא דייקה בדיווחיה אל הרשם. על אף קביעה זו, מאחר שהמדיניות אשר באה לידי ביטוי בהנחייה 2010–2 היא להגמיש דרישות עמידה בתקן כאמור, ועל רקע היות קומסיין הגורם המאשר היחיד באותה עת, לא הותלה רישומה של קומסיין. היא הונחתה לנקוט צעדים מיידים למזעור הסיכון, קיום סקר סכונים חיצוני ומבדקי חדירה לגבי רמת אבטחת המידע של אותו רכיב על ידי גורם בדיקה חיצוני, ואלה בוצעו על ידה.

## הנחיות

### הנחייה 2010-2

כמתואר לעיל, בשנת 2011 הושלמו הליכי בדיקה של חברת קומסיין ושל חברת פרסונל איי. די, במסגרת רישומה במרשם, בהוראות הנחייה 2010–2.

בשתי החברות מימוש ההנחייה היה כרוך בבחינה מקיפה של מכלול מערכות המידע שלהן, אופן הקישוריות שלהן למערכות אחרות ולאינטרנט, ותהליכי העבודה נתמכי מערכות המידע בגורם המאשר.

תהליכי הבדיקה של הדו"חות כללו מספר סבבי דיונים מול הגורמים המאשרים וגופי הביקורת הבלתי תלויים שנשכרו על ידם. הבדיקה של צוות הפיקוח של הרשם מול החברות כלל דיונים לגבי הדו"חות שהועברו, ומספר פיקוחים שנועדו לבצע בדיקה מדגמית על הממצאים המפורטים בדוחות.

מהליכים אלה גובשו מספר תובנות, באשר לאופן היישום של ההנחיה. התובנה הראשונה היא כי לצורך גיבוש חוות דעת בלתי תלויה כנדרש בהנחייה, נדרש צוות בעל מספר התמחויות, ובהן לפחות התמחות בבדיקת היבטי תהליכי עבודה ובקרות, ויכולת ביצוע בדיקת חדירות ו–"תקיפה" של מערכות מידע.

תובנה שניה הינה השלכת הבדיקה על עיצוב מערכות המידע, שכן שתי החברות נדרשו לשינויים ושיפורים משמעותיים לעומת מצבן בתחילת התהליך. האחריות הכוללת על תקינות המערכות, היא כמובן של החברות עצמן, ובהתאם להיקף הבחינה, של הגורמים המבקרים למועד הביקורת.

בדיונים עם חברת פרסונל איי.די קויימו מספר סבבי פגישות, עד להגשת חוות דעת שהיתה מקובלת על הרשם.

בדיונים עם חברת קומסיין הוגשו מספר רב מאוד של דו"חות שהוגדרו על ידי גורמי הביקורת כסופיים, אך אלה נדרשו לתיקונים רבים ולעתים סמוך לאחר הגשת הדוחות מסרה החברה כי שינויים נוספים מבוצעים. תהליך זה החל, לאחר דחיות, בסוף שנת 2010, ונמשך עד סוף אוגוסט 2011 עת אושרה עמידת החברה בהוראות ההנחיה.

במסגרת הניסיון שנצבר במסגרת ההנחיה הוגדר בצורה ברורה יותר הממשק שבין חוות דעת לפי הנחייה 2010–2, לבין חוות דעת מבקר בלתי תלוי לפי תקנה 2 לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו). בהתאם לכך, חוות הדעת לפי הנחייה 2010–2 עוסקת בהיבטים הכללים והמפורטים של מערכת המידע, ואילו חוות הדעת של המבקר מאשרת את המימוש בפועל של היבטים אלה.

בהתבסס על הניסיון שנצבר בהפעלת ההנחיה בעת מתן הנחיות שוטפות לגורמים המאשרים, גובשה הנחיה פנימית מעודכנת בדבר אופן פרשנות סעיפי התקן. הנחיה זו תעדכן את הנחיה 2010–2.

## מעקב - מימוש הנחייה 2010-4 - עדכון אלגוריתמים

כפי שדווח בדוחות קודמים, פרסם הרשם את הנחייה 2010–4 בנושא האלגוריתמים המשמשים לחתימה אלקטרונית, וזאת בהתבסס על עבודת בדיקה שביצע פרופ' בני פנקס, מומחה להצפנות ומדעי המחשב מאוניברסיטת תל אביב.

בעקבות קשיי הערכות של הגורם המאשר קומסיין להנחיה, ושל גורמי הממשלה המרכזיים הנסמכים על שימוש בחתימה אלקטרונית, נערכו בשנת 2011 על ידי רמו"ט מספר דיונים לליבון הנושא. בעקבות דיונים אלה דחה בסוף מרץ 2011 הרשם את החובה להשתמש בפונקצית גיבוב SHA–2 (Hash), ליום 1.10.2011.

השימוש בפונקצית הגיבוב SHA–1 אמור להפסק לחלוטין לא יאוחר מיום 1.10.2013. משמעות החלטה זו היא שתעודות SHA–1 שהונפקו טרם מועד זה לא ישמשו עוד ויש להחליפן.

עקב פנייה קונקרטית של רשות ניירות ערך הוארכה התקופה במקצת, כך שהמועד האחרון נקבע ל–31.12.2011, והשימוש בתעודות שהונפקו קודם למועד זה תוך יישום פונקצית SHA–1 ייפסק עד ליום 31.12.2013.

לגורמים המאשרים ניתנה האפשרות להנפיק במקביל תעודות משני הסוגים (SHA–1 ו–SHA–2) בתקופת הביניים, אולם לא הוגשה כל בקשה כזו. על פי בקשתו, הועבר לרשם נוהל החלפה מהיר לאירוע של איתור כשל בפונקצית SHA–1 במהלך תקופת הביניים.

## אישור חומרה לפי תקנה 2(9)

ביום 29.11.11 אישר הרשם בהתאם לסמכות המוקנה לו בתקנה 2(9) לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות) התשס"ב–2001 כי שני כרטיסים חכמים של חברת אתנה (Athena) המשמשים, בין היתר, לחתימה אלקטרונית, מקיימים את דרישות החוק והתקנות לביצוע חתימה אלקטרונית מאובטחת. זהו אישור ראשון שניתן לפי סמכות זו בתקנות.

האישור התבסס על אישורי הסמכה שקיבלו המוצרים לפי תקני אבטחת המידע NIST FIPS 140–2 ו–Common Criteria for Information Technology, וכן על חוות דעת של מומחה אבטחה בלתי תלוי, שניתנו בהתאם לתבנית שנקבעה על ידי הרשם. במסגרת חוות הדעת נדרש המומחה החיצוני לאשר כי תנאי ההסמכה הזרה יושמו באופן הרלבנטי לדרישות החוק, וכן כי יושמו במוצר דרישות קונקרטיות הנובעות מדרישות והנחיות הרשם.

בהתאם להצהרות ובדיקות הרשם, שני המוצרים מספקים ללקוח הקצה את דרישות האבטחה והדרישות הפונקציונליות הנדרשות לפעולת חתימה לפי החוק, וכן עומדות בדרישות והנחיות הרשם לפי החוק הישראלי.

תוקף האישור הוא כל עוד מתקיימות ההסמכות האמורות. חברת אתנה התחייבה כחלק מהליך האישור לעדכן את הרשם בדבר שינויים באישורים אלה או לגבי ארועי אבטחה הפוגעים במידת הבטיחות של המוצר בהתאם לדרישות התקינה.

# פרק ח' 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.

## כללי

רשם שירותי נתוני אשראי ומידע על עוסקים (בפרק זה – הרשם או רשם שירותי נתוני אשראי) נותן רישיונות פעולה לגופים המבקשים לפעול כשירותי נתוני אשראי או כשירותי מידע על עוסקים בהתאם לחוק שירות נתוני אשראי, התשס"ב–2002 (בפרק זה – החוק, או חוק שירות נתוני אשראי) ומפקח עליהם מכוח הסמכויות המוקנות לו בחוק.

דו"ח זה מוגש ביוזמת רמו"ט לועדת כלכלה, אשר החוק נמצא בטיפולה, בדומה לדו"חות של שני הרשמים האחרים הפועלים ברמו"ט שלהם נקבעה חובת דיווח בחוק, וזאת אף שלא נקבעה חובה בדין להגישו.

## בעלי רישיונות

### בעלי רישיונות תקפים

בעלי הרישיון מכח חוק שירות נתוני אשראי בסוף שנת 2011 הינם:

| מס' 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 קופאס בע"מ** | www.bdi.co.il |
| 539000026 | שירות מידע על עוסקים | **בי.די.איי קופאס בע"מ** | www.bdi.co.il |
| 539000018 | שירות מידע על עוסקים | **דן אנד ברדסטריט ישראל בע"מ** | www.dbisrael.co.il |

## ביטול רישיון שירות מידע על עוסקים

ביום 7.2.11 הודיעה חברת לב אמון יזמים כי היא מוותרת על רישיון שירות מידע על עוסקים שקיבלה בשנת 2006.

בעקבות זאת, הודיע הרשם על ביטול הרישיון של החברה, ובוצעו הפעולות הנדרשות מכוח תקנה 81 לתקנות שירות נתוני אשראי, התשס"ד–2004 בגין סיום או הפסקת פעילות בעל רישיון שירות נתוני אשראי.

## שינוי בבעלות, דירקטורים ומנהל שירות

במהלך 2011 חלו שינויים בבעלות, דירקטורים ומנהל השירות של חברת דן אנד ברדסטריט ישראל בע"מ. כמו כן, חלו שינויים בדירקטורים ומנהל השירות של חברת די אנד בי החברה לנתוני אשראי בע"מ.

שינויים אלה נבדקו בהתאם להוראות החוק והתקנות ואושרו.

## דיווחים על פגם לפי תקנה 80

בשנת 2011 קיבל הרשם ארבעה דיווחים מבעלת רישיון שירות נתוני אשראי די אנד בי על פגם בפעילות בעל רישיון כנדרש בתקנה 80 לתקנות שירות נתוני אשראי, התשס"ד–2004. הפגמים שדווחו נבעו הן מתקלות בהעברת מידע ממקורות מידע שונים לבעלת הרישיון, והן מתקלות בקבלת מידע אצל בעלת הרישיון.

במסגרת הטיפול בכל פגם הוציאה בעלת הרישיון דוחות אשראי מעודכנים, לכל מי שקיבל דוח אשראי על לקוח שנכלל ברשומות הפגומות.

כל דיווח פורסם על ידי בעלת הרישיון בשני עיתונים יומיים וכן על ידי הרשם באתר האינטרנט של רמו"ט.

# פיקוח על בעלי רשיונות

בתחום נתוני אשראי שלושה סוגים של הליכי פיקוח –

א. תיקי פיקוח הנפתחים בעקבות פניה של אדם המתלונן על פגיעה בו על ידי בעל רשיון או מקור מידע.

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

ג. תיקי פיקוח הנפתחים בשל בקשות של בעלי הרישיונות לשינויים שונים במתאר עבודתם.

## נתונים

בתחום נתוני אשראי הוגשו בשנת 2011 55 תלונות המהוות כ–24% מכלל התלונות שהגיעו לרמו"ט. ביחס לשנת 2010, עלתה כמות הפניות בתחום נתוני אשראי בכ–10%, ונתח הפניות בתחום נתוני אשראי מכלל הפניות שהגיעו לרמו"ט, עלה בכ–40%.

במהלך השנה נפתחו ברמו"ט 20 תיקי פיקוח בנושא נתוני אשראי, המהווים כ–23% מכלל תיקי הפיקוח שנפתחו בשנה זו. כמו כן, המשיך הטיפול ב–5 תיקי פיקוח בתחום זה שנפתחו קודם לשנת 2011.

חלוקת התיקים בתחום נתוני אשראי שנפתחו ב–2011 לפי סוגיהם היא כדלקמן –

| סוג התיק | כמות |
|---|---|
| תיקי פיקוח בשל מהלך ייזום | 11 |
| תיקי פיקוח בעקבות תלונה | 6 |
| תיקי פיקוח לצרכי אישור רשם | 3 |
| **סה"כ** | **20** |

## תיקי פיקוח נבחרים

### פרטנר – בי.די.איי

הפונה התלונן על כך שהוזמן על אודותיו דו"ח אשראי מבעלת רישיון שירות נתוני אשראי בי.די.איי על ידי חברת פרטנר, אצלה לטענתו הוא היה בסטטוס "רדום" מזה מספר שנים.

לאחר בחינת התלונה מול בעלת הרישיון וחברת פרטנר, התברר כי לפונה חשבון נוסף אצל פרטנר בו הוא פעיל. במסגרת בדיקה תקופתית של כלל לקוחות פרטנר, לצורך מתן אשראי, הוזמן על אודות הפונה דוח אשראי, בהתאם לאמור בסעיף 28(א) לחוק שירות נתוני אשראי, התשס"ב–2002.

נמצא, כי במקרה זה בו הוזמן דוח אשראי המתייחס ללקוחות פרטנר (כל עוד חשבון הלקוח איננו מבוטל בחברה), לא ניתן לבסס הפרה של סעיף 28(א) לחוק.

### הפצת קבצי מושל"כ לבתי תוכנה

במסגרת שיתוף פעולה עם בנק ישראל בחנה רמו"ט בקשות של גופים עסקיים וציבוריים לקבלה מבנק ישראל של הקבצים המכילים רשימת מושכי שיקים ללא כיסוי (מושל"כ),

הנדרשים להם לצורך סליקת שיקים במסגרת פעילותם העסקית. זאת, לאחר שביוזמת רמו"ט הפסיק בנק ישראל להציג באתר האינטרנט שלו את קובץ המושל"כ המלא.

במסגרת זו הוגשו גם בקשות של חברות המספקות שירותי תוכנה, חומרה ואחסון ללקוחות (למשל בתי עסק) לצורך בדיקת שיקים המתקבלים אצלם. מאחר שחברות אלה הבהירו כי בכוונתן להעביר את הקבצים או מידע מתוכם ללקוחותיהם, הודיעה רמו"ט כי תיאלץ לסרב לבקשות משום שהעברת המידע ללקוחות נכנסת לגדר "שירות נתוני אשראי" – "איסוף ניהול והחזקה של נתוני אשראי .. לצורך מסירה לאחר, כדרך עיסוק" – כמשמעותה בחוק שירות נתוני אשראי, פעילות הטעונה רישיון בו המבקשות לא אוחזות.

עם זאת, הודיעה רמו"ט למבקשות שלא תתנגד להמשך שימוש שלהן בקובץ המושל"כ כקבלניות עבור מי מלקוחותיהן שיחתמו על התחייבות עצמאית להשתמש בקובץ רק למטרה הלגיטימית ולתקופה המותרת, ויציינו את בית התוכנה כמחזיק במידע מטעמם, כמשמעות המונח בסעיף 3 לחוק הגנת הפרטיות. מקצת מבתי התוכנה נהגו על פי מתווה זה והמשיכו לקבל את הקבצים עבור לקוחותיהם ולמטרותיהם.

## תיקוני חקיקה

ביום 29.12.11 פורסמו ברשומות תקנות שירות נתוני אשראי (תיקון), התשע"ב–2011. זהו תיקון ראשון ומשמעותי לתקנות שירות נתוני אשראי מאז התקנתן בשנת 2004, ונכללו בהן מספר שינויים עיקריים שמטרתם שיפור האפקטיביות של חוק שירות נתוני אשראי כמאיץ של שיפור התחרות בתחום האשראי. להלן עיקרי השינויים:

א. הוספת הנתון "רמת חוב" למידע השלילי הנאסף ונמסר;

ב. שינוי הכללים באשר לסף ממנו יימסר מידע שלילי, באופן המאפשר בחינת מכלול המידע הקיים על הלקוח לצורך מסירת המידע ולא לפי קטגוריית נתוני האשראי שבדוח. השינוי ירחיב את המקרים בהם יימסר מידע שלילי;

ג. הוספת נתונים למידע השלילי כגון הוצאת צו מניעה ביחס להגבלה לפי חוק שיקים ללא כיסוי, התשמ"א–1981, הצהרה של חייב בפני ראש הוצאה לפועל כי אינו יכול לשלם את חובותיו וכד';

ד. הוספת חברות כרטיסי אשראי כמקורות למידע חיובי.

תקנות אלה אמורות להכנס לתוקף במהלך שנת 2012, והן מחייבות שינויים במערכות המידע ונוהלי העבודה של בעלי הרשיונות ומקורות המידע. רשם שירות נתוני אשראי צופה כי תדרש עבודת פיקוח רבה לוידוא עמידת בעלי הרשיונות בהוראת התקנות.

# נספח א'

## הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב-2011



רשומות

# הצעות חוק

ה מ מ ש ל ה

י"ט בחשון התשע"ב 627 16 בנובמבר 2011

עמוד

הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2011 ..... 64

**מתפרסמת בזה הצעת חוק מטעם הממשלה:**

## הצעת חוק הגנת הפרטיות (תיקון מס' 12) (סמכויות אכיפה), התשע"ב–2011

שינוי מונחים

1. בחוק הגנת הפרטיות, התשמ"א–1981[1] (להלן – החוק העיקרי), בכל מקום, במקום "פנקס" יבוא "מרשם", במקום "בפנקס" יבוא "במרשם", במקום "מהפנקס" יבוא "מהמרשם", במקום "הרשם" יבוא "הממונה" ובמקום "לרשם" יבוא "לממונה".

### דברי הסבר

**כללי** מטרת התיקון המוצע היא לשפר את יכולות הפיקוח והאכיפה להבטחת קיום הוראות חוק הגנת הפרטיות, התשמ"א–1981 (להלן – החוק או חוק הגנת הפרטיות), הנוגעות לפרטיות במאגרי מידע. הזכות לפרטיות היא זכות חוקתית מוגנת על פי סעיף 7 לחוק־יסוד: כבוד האדם וחירותו. התיקון המוצע נועד להקנות ליחידת רשם מאגרי המידע, המופקדת על שמירה על הפרטיות במאגרי מידע ועל קיום הוראות החוק הנוגעות למאגרי מידע, כלי פיקוח וסמכויות אכיפה שיאפשרו התמודדות עם הסיכונים המאיימים על הפרטיות כיום, בהתחשב במעמדה של הזכות לפרטיות כזכות יסוד במשפט הישראלי, בהצעת חוק זו מוצע לקבוע מנגנון אכיפה מינהלי, שיהווה מנגנון חלופי לאכיפה במסגרת ההליך הפלילי, ביחס להפרה של הוראות החוק, וכן לערוך שינויים בחלק העונשין של החוק.

פרק ב' לחוק הגנת הפרטיות מסדיר את ההגנה על המידע במאגרי מידע ממוחשבים. הפרק האמור מגדיר מהו מאגר מידע, מקים מוסד רישום ופיקוח על מאגרי מידע, וקובע הוראות לגבי איסוף המידע למאגרי מידע, אופן ניהול מאגרי מידע והשימוש במידע האגור בהם. תכלית ההסדר בפרק ב' לחוק היא למנוע פגיעה בפרטיות בהקשר של השימוש במאגרי מידע ולהגן על זכויות נושאי המידע. פרק ד' לחוק הגנת הפרטיות מסדיר את מסירת המידע מגופים ציבוריים.

בהחלטת הממשלה מס' 4660 מיום כ"ג בסיוון התשס"ו (19 ביוני 2006) הוחלט על הקמתה של רשות משפטית להגנת פרטיות וטכנולוגיות מידע במשרד המשפטים, הקרויה הרשות למשפט, טכנולוגיה ומידע (להלן – רמו"ט). בעקבות זאת, מוזגה יחידת רשם מאגרי מידע ארגונית תחת רמו"ט. מטרת ההחלטת הממשלה היתה, בין השאר, לשפר את הפיקוח בנושא זה.

בדין וחשבון שהגיש לשרת המשפטים בחודש ינואר 2007 הצוות לבחינת החקיקה בתחום מאגרי המידע בראשותו של המשנה ליועץ המשפטי (חקיקה) דאז, מר יהושע שופמן (להלן – דוח צוות שופמן), המליץ הצוות, בין שאר המלצותיו, להרחיב את סמכויות רשם מאגרי המידע. במהלך שנות פעולתה של רמו"ט ולנוכח ההתפתחויות הטכנולוגיות בתחום, התווספו כמה תובנות לתובנות המנולמות בדוח צוות שופמן, אלו באים לידי ביטוי בהצעת חוק זו.

במהלך העשורים האחרונים, התרחשו שינויים טכנולוגיים ומשקיים מרחיקי לכת באופן שבו מידע נאסף, מעובד ונעשים בו שימושים נוספים, וזאת במסגרת הפעילות השגרתית של ארגונים ויחידים. שינויים אלה אף יוצרים איומים חדשים על הזכות לפרטיות במידע. המציאות מלמדת שדליפת מידע רגיש, גישה לא מורשית למאגרים ושימוש במידע מתוכם למטרות זרות – הופכים לשכיחים יותר ויותר.

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

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

כמו כן, יש להתמודד עם האתגרים הייחודיים של אכיפת הגנת הפרטיות במאגרי מידע ממוחשבים, ואלה המרכזיים שבהם:

– בכלל, מבוצעות ההפרות בדלת אמותיו של המפר ולרוב אין ראיה "חפצית" לקיומן, בשל טבעו של התחום, מידת התחכום של העוסקים בו ויתרונם בהכרת המערכת שלהם – קל מאוד לטשטש את העקבות בזמן קצר;

– ביצוע ההפרות הוא פשוט ועלות ביצוע ההפרה ושכפול עותקים "מפרים" של המידע – זניחה, ומנגד פוטנציאל הרווח הכספי מביצוען – גדול;

– מרגע שבוצעה ההפרה (בגון שדלף מידע ממאגר) במעט בלתי אפשרי לתקן את נזקיה. מכאן, שיש נסיבות שבהן נדרשת תגובה ופעולה מיידית;

– לא מדובר בפעילות המיוחדת לסקטור מסוים במשק, מאגרי מידע מוחזקים ופועלים בתחומים מגוונים – בסקטור הציבורי והפרטי, בכל תחומי המשק והחברה ובידי תאגידי ענק כמו גם אזרחים מן השורה;

– במציאות הטכנולוגית הנוכחית נאסף יותר ויותר מידע על אודות אנשים כחלק בלתי נפרד משירותים אחרים הניתנים, כגון "נתוני מיקום" במסגרת שימוש בטלפון סלולרי, נתוני גלישה באינטרנט במסגרת שירות חיבור לאינטרנט, ועוד.

[1] ס"ח התשמ"א, עמ' 128; התשע"א, עמ' 758.

2. בסעיף 7 לחוק העיקרי – תיקון סעיף 7

(1) ברישה, במקום "ובפרק ד'" יבוא "ובפרקים ד' עד ד'3";

(2) בהגדרה "מידע", בסופה יבוא "ולעניין סעיפים 23יג(ד) ו־23טו – מידע מכל סוג שהוא";

(3) במקום ההגדרה "רשם" יבוא:

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

"מרשם" – מרשם מאגרי המידע המנוהל על ידי הממונה על הגנת מידע מכוח סעיף 12 לחוק;".

3. בסעיף 10 לחוק העיקרי – תיקון סעיף 10

(1) במקום סעיף קטן (ה) יבוא:

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

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

## דברי הסבר

היקפם ועוצמתם של האיומים וההפרות, והאתגרים הייחודיים של אכיפת הגנת הפרטיות, כפי שתוארו לעיל, מחייבים אפוא לעדכן גם את ההסדר של ההגנה על הפרטיות, המפורט בפרק ב' לחוק.

עוד יצוין, כי סמכויות פיקוח ואכיפה אפקטיביות, הן גם נדבך מרכזי במתכונת פעילותן של רשויות הגנת מידע דומות בעולם ובמסמכי מדיניות מרכזיים של האיחוד האירופי ושל הארגון לשיתוף פעולה ופיתוח כלכלי (OECD).

התוספות המוצעות בהצעת החוק נועדו, כאמור לעיל, לחזק במידה משמעותית את יכולות האכיפה של יחידת רשם מאגרי המידע, ובמסגרת זו להקנות לו סמכויות מינהליות חלופיות לנקיטת הליכים פליליים. כמו כן מוצע להשלים את הכלים הקיימים בסמכויות אכיפה פליליות.

**סעיפים 1 ו־2** לאור הכוונה להרחיב את הסמכויות הנתונות לרשם מאגרי המידע (כאמור לעיל בחלק הכללי של דברי ההסבר), מוצע לקבוע תנאי כשירות מחמירים מאלה הקיימים כיום, כך שיוכל להתמנות לרשם מאגרי המידע רק מי שמתקיימים בו תנאי הכשירות להתמנות לשופט של בית משפט מחוזי, במקום שופט של בית משפט שלום כפי שנדרש כיום בהתאם לסעיף 7 לחוק. כמו כן, מוצע להחליף את המונח "רשם מאגרי המידע" במונח "הממונה על הגנת מידע", שהוא מונח המתאר בצורה מדויקת יותר את תפקידו של הרשם ואת הסמכויות הנתונות לו לפי הצעת החוק. לפיכך מוצע להוסיף בסעיף 7 לחוק הגדרה של "הממונה על הגנת מידע" ולהחליף בכל מקום בחוק את המונח "הרשם" במונח "הממונה".

עוד מוצע לתקן את החוק כך שבכל מקום, במקום "פנקס" מאגרי המידע יבוא "מרשם" מאגרי המידע, ובהתאמה לכך תיווסף הגדרה של "מרשם" בסעיף 7 לחוק. כמו כן מוצע להחיל את ההגדרות השונות הקבועות בסעיף 7 גם על פרקים ד'1 עד ד'3 שמוצע להוסיפם לחוק במסגרת הצעת חוק זו.

**סעיף 3 לפסקה (1)**

סעיף 10(ה) לחוק קובע כיום כדלקמן:

"(ה) הרשם יעמוד בראש יחידת הפיקוח, והוא ימנה את המפקחים לצורך ביצוע הפיקוח לפי חוק זה; לא יתמנה למפקח אלא מי שקיבל הכשרה מקצועית מתאימה בתחום מיחשוב ואבטחת מידע והפעלת סמכויות לפי חוק זה, ומשטרת ישראל לא הביעה התנגדות למינויו מטעמים של שמירה על בטחון הציבור."

מוצע להחליף את סעיף 10(ה) האמור ולקבוע כי הממונה, העומד בראש יחידת הפיקוח, יהיה רשאי להסמיך חוקר או מפקח, מבין עובדי המדינה, בסמכויות לפי החוק, כולן או חלקן. כמו כן מוצע לקבוע תנאי הסמכה הולמים למפקח ולחוקר, תוך מתן דגש על הכשרה ראויה לצורך הפעלת סמכות חדירה לחומר מחשב, במקובל בהוראות בדברי חקיקה דומים אחרים.

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה שר המשפטים בהסכמת השר לביטחון הפנים, ולעניין הפעלת סמכויות חדירה לחומר מחשב או העתקתו כאמור בסעיפים 23יא ו־23יג(א)(3) – הוא בעל תפקיד המיומן לביצוע פעולות כאמור;

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

(2) אחרי סעיף קטן (ה1) יבוא:

"(ה2) הוראות סעיף קטן (ה1) יחולו רק לגבי רשות ביטחון וגוף אחר שחלים עליהם הוראות סעיף 24א.";

(3) סעיף קטן (ז) – בטל.

תיקון סעיף 17

4. בסעיף 17 לחוק העיקרי, האמור בו יסומן "(א)" ואחריו יבוא:

"(ב) (1) השר רשאי לקבוע הוראות לעניין האחריות לאבטחת המידע הקבועה בסעיף קטן (א) ובסעיף 17ב(ב), ובכלל זה היקפה והחובות הכלולות בה, וכן לעניין דרכי אבטחת המידע כאמור, בין השאר בעניינים אלה:

(א) הגנה פיזית ולוגית על המאגר;

(ב) סדרי הניהול וכללי העבודה במאגר המידע ובקשר אליו, לרבות לעניין קביעה של הגבלות על גישה של מועסקים למידע.

(2) בתקנות לפי פסקה (1), יכול שייקבעו הוראות שונות לגבי מאגרים בעלי מאפיינים שונים.

(3) תקנות לפי פסקה (1) שיחולו על גופים המנויים בתוספת הראשונה, השנייה והרביעית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998, יותקנו בהתייעצות עם ראש הממשלה, ואולם תקנות כאמור לעניין גופים המנויים בפרטים 2 ו־3 לתוספת הראשונה של החוק האמור, יותקנו בהתייעצות עם שר הביטחון."

## דברי הסבר

**לפסקה (2)**

הסמכויות של מפקח לצורך מילוי תפקידיו לפי החוק, מעוגנות כיום בסעיף 10(ה1) לחוק. במסגרת הצעת החוק, סמכויות הפיקוח של הממונה ושל המפקחים מטעמו, מוגדרות ומאורגנות מחדש בפרק ד'1 המוצע. מאחר שבהתאם לסעיף 24א המוצע, פרקים ד'1 עד ד'3 המוצעים אינם חלים על רשות ביטחון כהגדרתה בסעיף 19(ג) לחוק ועל כל גוף אחר שקבע שר הביטחון, בצו, בהסכמת שר המשפטים, מוצע להגביל את תחולתו של סעיף 10(ה1) הקיים, כך שיחול רק לגבי רשות ביטחון כהגדרתה בסעיף 19(ג) וכל גוף אחר שנקבע בידי שר הביטחון כאמור בסעיף 24א המוצע. התוצאה היא שלגבי אותם גופים ימשיך לחול הדין הקיים טרם התיקון. תחולת סמכויות הפיקוח של הממונה ושל המפקחים מטעמו, ביחס לגופים במערכת הביטחון אשר אינם מוחרגים מתחולת פרק ד'1 המוצע כאמור לעיל, מוסדרת בסעיף נפרד בהצעת החוק – סעיף 23יד.

**לפסקה (3)**

סעיף 10(ז) לחוק קובע כיום כי "דין הרשם ודין מי שפועל מטעמו כדין עובד המדינה". ההוראה האמורה מתייתרת מאחר שהממונה הוא עובד המדינה, ולפי סעיף 10(ה) המוצע גם החוקרים והמפקחים שהממונה יכול להסמיך צריכים להיות עובדי המדינה. לפיכך מוצע לבטל את ההוראה האמורה.

**סעיף 4** סעיף 17 לחוק הגנת הפרטיות קובע כי בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע, אחראים לאבטחת המידע במאגר. אבטחת מידע מוגדרת בסעיף 7 לחוק כ"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין". אבטחת מידע היא מרכיב מהותי בהגנה מפני פגיעה בפרטיות מידע במאגר המידע, ולכן יש לה מקום מרכזי בהסדרה לפי פרק ב' לחוק. סעיף 36 לחוק קובע הסמכה לקבוע תקנות גם בנושא זה. מוצע להוסיף סעיף הסמכה ספציפי להתקנת תקנות בעניין האחריות לאבטחת מידע, כדי לאפשר הטלת סנקציה מינהלית על הפרת ההוראות.

5. בסעיף 17א(ב) לחוק העיקרי, במקום "הממונה על האבטחה" יבוא "האחראי על הגנת מידע". — תיקון סעיף 17א

6. בסעיף 17ב לחוק העיקרי – — תיקון סעיף 17ב

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

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

(3) בסעיפים קטנים (ב) ו־(ג), במקום "ממונה" יבוא "האחראי על הגנת מידע".

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

**"פרק ד'1: סמכויות פיקוח, בירור מינהלי ואכיפה**

**סימן א': הגדרות**

הגדרות

23ט. בפרק זה –

"חוק המחשבים" – חוק המחשבים, התשנ"ה–1995[1];

"חוק המעצרים" – חוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996[2];

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

"חפץ" – כהגדרתו בפקודת המעצר והחיפוש;

"מסמך" – לרבות פלט כהגדרתו בחוק המחשבים;

## דברי הסבר

עוד מוצע לקבוע כי ההוראות, לעניין אבטחת מידע, שיחולו על גופים המנויים בתוספת הראשונה, השנייה והרביעית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998, ייקבעו בהתייעצות עם ראש הממשלה או עם שר הביטחון, לפי העניין. גופים אלה כפופים להנחיות של שירות הביטחון הכללי בתחום הגנת מערכות מחשב קריטיות – הגופים המנויים בתוספת הרביעית לחוק, ובתחום אבטחת מידע – הגופים המנויים בתוספת הראשונה והשנייה לחוק האמור, למעט הגופים המנויים בפרטים 2 ו־3 לתוספת הראשונה של החוק האמור, אשר כפופים להנחיות הממונה על הביטחון במערכת הביטחון (להלן – המלמ"ב), בתחום זה. לכן, בקביעת תקנות לעניין אבטחת מידע שיחולו על גופים אלה, יש מקום להתייעצות עם ראש הממשלה שהוא השר הממונה על שירות הביטחון הכללי, או עם שר הביטחון, שהוא השר הממונה על המלמ"ב, לפי העניין, כדי למנוע סתירה או כפל הוראות בנושא זה.

**סעיפים 5 ו־6** סעיפים 17א ו־17ב לחוק מתייחסים לבעל התפקיד בגופים מסוימים שברשותם מאגרי מידע, שהוא אחראי על אבטחת המידע במאגרים. מוצע לתקן את הסעיפים האמורים ולהחליף את תוארו של בעל התפקיד כאמור מ"ממונה על אבטחת מידע" ל"אחראי על הגנת מידע", זאת כדי למנוע בלבול בינו לבין רשם מאגרי המידע אשר מוצע לשנות את תוארו לממונה על הגנת מידע (ר' דברי ההסבר לסעיפים 1 ו־2 להצעת החוק).

**סעיף 7 לפרק ד'1 המוצע**

פרק ד'1 המוצע קובע סמכויות פיקוח, בירור מינהלי ואכיפה. הסמכויות המפורטות בסימן ב' המוצע, נועדו לאפשר פיקוח שוטף על קיום הוראות החוק, בסמכויות הבירור המינהלי המפורטות בסימן ג' המוצע ייעשה שימוש במקרה שקיים יסוד סביר להניח כי בוצעה הפרה של הוראות החוק הנאכפות במישור המינהלי. בסמכויות האכיפה הפליליות המפורטות בסימן ד' המוצע, ייעשה שימוש במקרה שהתעורר חשד לביצוע עבירה על הוראות החוק.

**לסימנים א' ו־ב'**

סעיף 10(ה1) לחוק מפרט כיום את הסמכויות המיועדות לפיקוח שנרתי על קיום הוראות החוק, כאשר אין בהכרח חשד או יסוד להניח שהופרו אותן הוראות או שנעברו עבירות פליליות. לעתים מזומנות הפעלת סמכויות פיקוח שגרתיות אלה יכולה לעורר השערה כי אכן קיים חשד לביצוע עבירה או יסוד סביר להניח כי בוצעה הפרה, דבר שיקים את הבסיס להפעלת סמכויות הבירור המינהלי או סמכויות האכיפה בהתאמה.

[1] ס"ח התשנ"ה, עמ' 366.

[2] ס"ח התשנ"ו, עמ' 338.

"נתוני מערכת" – נתונים על אודות החזקה וניהול של מידע ושל מאגר מידע על אודות השימוש בהם, ובלבד שאינם כוללים מידע;

"פקודת המעצר והחיפוש" – פקודת סדר הדין הפלילי (מעצר וחיפוש)[נוסח חדש], התשכ"ט–1969[4].

**סימן ב': סמכויות פיקוח**

סמכויות מפקח

23. (א) לשם פיקוח על ביצוע ההוראות לפי פרקים ב', ד', ד'1 ו־ד'3, רשאי הממונה או מפקח שהוסמך על ידו:

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

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

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

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

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

## דברי הסבר

סעיף 23 המוצע מחליף את סעיף 10(ה1) לחוק. הסעיף מוסיף על סמכויות הפיקוח השגרתי על מאגרי המידע שהיו כלולות בסעיף 10(ה1) האמור, את הסמכות לדרוש הזדהות ואת הסמכות לדרוש הצגה או מסירה של עותק מחומר מחשב הכולל נתוני מערכת או מידע מדגמי. סמכויות החיפוש והתפיסה שהיו כלולות בסעיף 10(ה1) לחוק יחד עם סמכויות הפיקוח, מעוגנות במסגרת הצעת החוק בסימנים נפרדים, מאחר שסמכויות אלו הן סמכויות המופעלות בעת שקיים חשד לביצוע עבירה או יסוד סביר להניח שבוצעה הפרה.

כאמור לעיל, מוצע להסמיך את הממונה או המפקחים שהוסמכו על ידו, לדרוש הצגה או מסירה של עותק מחומר מחשב הכולל נתוני מערכת או מידע מדגמי. נתוני מערכת הם נתונים טכניים שאינם כוללים מידע אישי על אודות אדם, והם דרושים לבירור קיום הוראות החוק במאגר המידע הממוחשב, ביחס לאופן השימוש במידע. הדרך לבחון עמידה בהוראות החוק, תוך שמירה על פרטיות נושאי המידע במאגר, היא, בין השאר, באמצעות בדיקת הכללים המוגדרים במערכת המידע וסוג המידע השמור במערכת המידע, ובחינת פעולות העיבוד השונות המבוצעות במידע. ביחס לבחינת אבטחת המידע, יש צורך בבדיקה של אופן המימוש בפועל של עקרונות אבטחת המידע, למשל אופן הגדרת הרשאות הגישה למידע.

אשר למידע מדגמי – ככלל, הכוונה להצגה של עותק מחומר מחשב הכולל שדות אקראיים או למסירתו לצורך בדיקה מדגמית של המידע הנשמר במאגר או לצורך היבטים אחרים של הפיקוח על הניהול והשימוש במידע במאגר. כדי לצמצם למינימום את הפגיעה האפשרית בזכות לפרטיות של המפוקחים ושל נושאי המידע שבמאגרי המידע המפוקחים, מוצע כי מידע מדגמי ייאסף בהיקף הנדרש למימוש תכליות הפיקוח בלבד. כמו כן מוצע כי המידע המדגמי שנמסר או שנאסף יימחק, ככלל, ממאגרי המידע של הממונה כאשר אינו נדרש עוד באופן סביר להמשך הליכי הפיקוח.

[4] דיני מדינת ישראל, נוסח חדש 12, עמ' 284.

**סימן ג': סמכויות בבירור מינהלי**

צו לחיפוש ולחדירה לחומר מחשב

23יא. היה לממונה או לעובד המדינה שהוא הסמיך לכך בהודעה ברשומות, הכשיר לכהן כשופט של בית משפט מחוזי, יסוד סביר להניח כי ברוצעה הפרה של הוראה מההוראות לפי חוק זה, כאמור בסעיף 23טז, הוא רשאי לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעם בעצמו או באמצעות מפקח.

אופן ביצוע חדירה לחומר מחשב והעתקתו

23יב. על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סימן זה, יחולו הוראות סעיפים 23א, 24(א)(1) ו־(ב), 26 עד 28, 31 ו־45 וכן הוראות הפרק הרביעי לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות למפקח והסמכויות הנתונות לקצין יהיו נתונות לממונה ולעובד המדינה שהוא הסמיך כאמור בסעיף 23יא.

**סימן ד': סמכויות אכיפה**

סמכויות אכיפה

23יג. (א) היה לממונה או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ד'3, יהיו נתונות לממונה ולחוקר כל סמכויות הפיקוח לפי סימן ב' לפרק זה, וכן הם רשאים –

(1) לחקור כל אדם הקשור לעבירה כאמור או שעשויות להיות לו ידיעות הנוגעות לעבירה כאמור; על חקירה לפי פסקה זו יחולו הוראות סעיפים 2 ו־3 לפקודת הפרוצדורה הפלילית (עדות)[5], והוראות חוק סדר הדין הפלילי (חקירת חשודים), התשס"ב–2002[6], בשינויים המחויבים;

## דברי הסבר

**לסימן ג'**

בשנים האחרונות נדרן רבות הצורך במציאת מנגנוני אכיפה חלופיים להליך הפלילי, שיאפשרו תגובה מהירה, יעילה ומירתית להפרת הוראות החוק. ההתפתחויות בתחום השימוש במאגרי מידע מחייבות אף הן מתן כלים לאכיפה יעילה בידי הממונה.

המנגנון החלופי להליך הפלילי הוא מנגנון של הטלת סנקציות מינהליות. לשם כך, וכדי להבטיח כי הטלת הסנקציות תתבסס על תשתית ראייתית מתאימה ומספיקה, נדרש ליתן לממונה סמכויות שישמשו אותו לאיסוף תשתית ראייתית זו. כלי הפיקוח הקיימים לא תמיד נותנים מענה לכך, שכן לא מדובר בפיקוח שגרתי, אלא במקרים שבהם קיים יסוד סביר להניח שבוצעה הפרה של הוראות החוק, וכן לנוכח סוג הפעילות שעליה הממונה מפקח. לפיכך מוצע במסגרת הבירור המינהלי לתת לממונה או לעובד המדינה שהוא הסמיך לכך, הכשיר לכהן כשופט של בית משפט מחוזי, סמכויות רחבות יותר מהסמכויות הקבועות בסימן ב' לצורך הפיקוח השגרתי, ולהסמיך אותו לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת סדר הדין הפלילי (מעצר וחיפוש)[נוסח חדש], התשכ"ט–1969, ולבצעם בעצמו או באמצעות מפקח.

**לסימן ד'**

**לסעיף 23יג**

בחוק הגנת הפרטיות אין היום לרשם או למי מטעמו סמכויות חקירה פליליות. כיום מוקנות סמכויות אכיפה לכמה רשויות רגולטוריות בעלות התמחות ייחודית ומורכבת, ובהן רשות ניירות ערך, רשות ההגבלים עסקיים ורשות המסים.

בהתאם לכך מוצע להסמיך את הממונה והחוקרים מטעמו, בסמכויות חקירה, סמכות לתפיסת חפצים, סמכות עיכוב, סמכות לדרוש מאדם להתלוות אליו למשרדי

[5] חוקי א"י, כרך א', עמ' (ע) 439, (א) 467.

[6] ס"ח התשס"ב, עמ' 468; התשס"ח, עמ' 572.

(2) לתפוס כל חפץ שיש לו יסוד סביר להניח שהוא חפץ הקשור לעבירה כאמור;

(3) לבקש מבית המשפט צו חיפוש ותפיסה או צו חדירה לחומר מחשב לפי סעיפים 23 עד 24 לפקודת המעצר והחיפוש, ולבצעו.

(ב) על ביצוע חיפוש, תפיסת חפץ וחדירה לחומר מחשב או העתקתו לפי סעיף זה, יחולו סעיפים 23א, 24(א)(1) ו־(ב), 26 עד 28, 31 ו־45 וכן הוראות הפרק הרביעי, לפקודת המעצר והחיפוש, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין יהיו נתונות לממונה ולעובד המדינה שהוא הסמיך כאמור בסעיף 23יא.

(ג) היה לממונה או לחוקר יסוד סביר לחשד שאדם עבר עבירה לפי פרקים ב' או ד'3, הוא רשאי לעכבו כדי לברר את זהותו ואת מענו או כדי לחוקרו במקום הימצאו; היה הזיהוי בלתי מספיק או שלא ניתן לחקור את אותו אדם במקום הימצאו, רשאי הממונה או החוקר לדרוש מאותו אדם להתלוות אליו למשרדי הממונה או לזמנו למשרדי הממונה למועד אחר שיקבע; מי שזומן למשרדי הממונה, יתייצב במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 66, 67 ו־72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לממונה.

(ד) היה לממונה או לחוקר יסוד סביר לחשד שנעברה עבירה לפי פרקים ב' או ד'3, הוא רשאי לעכב אדם שיכול למסור לו מידע הנוגע לאותה עבירה, כדי לברר את זהותו ומענו וכדי לחקור אותו במקום הימצאו; וכן הוא רשאי לזמן אותו למשרדי הממונה למועד סביר אחר שיקבע לצורך ביצוע אותן פעולות; מי שזומן למשרדי הממונה, יתייצב במועד שזומן אליו; על עיכוב לפי סעיף קטן זה יחולו הוראות סעיפים 68 ו־72 עד 74 לחוק המעצרים, בשינויים המחויבים, ובשינויים אלה: הסמכויות הנתונות לשוטר יהיו נתונות לחוקר והסמכויות הנתונות לקצין הממונה יהיו נתונות לממונה.

## דברי הסבר

הממונה, סמכות לבקש צו שיפוטי לביצוע חיפוש ותפיסה וצו חדירה לחומר מחשב. הפעלת סמכויות אלה מותנית בתנאים המנויים בגוף סעיף ההסמכה.

סמכות העיכוב שבסעיף 23יג(ג) ו־(ד) המוצע, מהווה כלי משלים לסמכות החקירה. סמכות העיכוב מוגבלת למטרות העיכוב הקבועות בחוק המעצרים: בירור זהותו ומענו של המעוכב או חקירת המעוכב במקום הימצאו. כמו כן מוצע להסמיך את הממונה או חוקר לזמן את המעוכב למשרדי הממונה למועד אחר, במקרים שבהם הזיהוי אינו מספיק או שלא היה ניתן לחקור אותו במקום הימצאו.

סעיפי העיכוב מבחינים בין עיכוב עד לעיכוב חשוד, מאחר שההצדקה להגבלת חירותו של עד שאינו חשוד פחותה. בהתאם להפיסה זו, ניתן לזמן עד למועד סביר אחר שייקבע, בדומה לסעיף 68 לחוק סדר הדין הפלילי (סמכויות אכיפה – מעצרים), התשנ"ו–1996 (להלן – חוק המעצרים). ככל שמדובר בחשוד ניתן לדרוש כי יתלווה

(ה) לעניין סעיפים קטנים (ג) ו־(ד), יראו את משרדי הממונה שהממונה הכריז עליהם בהודעה ברשומות כ"תחנת משטרה" לעניין הוראות חוק המעצרים.

תחולה על מערכת הביטחון

23יד. (א) על אף הוראות פרק זה, לא יעשה מפקח, חוקר, ממונה או עובד המדינה שהוא הסמיך כאמור בסעיף 23יא, שימוש בסמכויותיו לפי פרק זה כלפי מערכת הביטחון, אלא לאחר שעבר התאמה ביטחונית כמשמעותה בסעיף 15 לחוק שירות הביטחון הכללי, התשס"ב–2002[7].

(ב) השה, בהסכמת השר האחראי, יקבע בנהלים תנאים לשימוש בסמכויות לפי פרק זה כלפי מערכת הביטחון, בשים לב לטעמים של ביטחון המדינה, שלום הציבור וביטחונו; בהעדר הסכמה בין השרים, יקבע ראש הממשלה נהלים כאמור.

(ג) נהלים ראשונים לפי סעיף קטן (ב) ייקבעו בידי השה, בהסכמת השר האחראי, בתוך 90 ימים מיום תחילתו של חוק זה, ובהעדר הסכמה ביניהם – בידי ראש הממשלה, בתוך 30 ימים לאחר מכן.

(ד) בסעיף זה –

"מערכת הביטחון" – כל אחד מאלה, למעט רשות ביטחון וגוף אחר, שחלים עליהם הוראות סעיף 24א:

(1) משרד הביטחון ויחידות הסמך שלו;

(2) צבא ההגנה לישראל;

(3) יחידות ויחידות סמך של משרד ראש הממשלה, שעיקר פעילותן בתחום ביטחון המדינה;

(4) מפעלי מערכת הביטחון כמשמעותם בסעיף 20 לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998, שאינם יחידות או יחידות סמך כאמור בפסקה (3), ואשר שר הביטחון הודיע עליהם לשר;

(5) שירות בתי הסוהר;

## דברי הסבר

לחוקר למשרדי הממונה כדי לאפשר חקירה מיידית של העבירה וכן את התייצבותו במועד שנקבע, בדומה לסעיף 67 לחוק המעצרים. עוד מבהירה הצעת החוק כי מי שזומן לחקירה, בין אם הוא חשוד ובין אם הוא עד, מחויב להתייצב במועד שזומן אליו במשרדי הממונה.

**לסעיף 23יד**

מוצע לקבוע כי מפקח, חוקר, הממונה על הגנת המידע או עובד המדינה שהוא הסמיך כאמור בסעיף 23יא המוצע, לא יעשה שימוש בסמכויותיו לפי פרק ד' המוצע כלפי מערכת הביטחון, אלא לאחר שעבר התאמה ביטחונית, כמשמעותה בסעיף 15 לחוק שירות הביטחון הכללי, התשס"ב–2002. מערכת הביטחון, כהגדרתה בסעיף 23יד המוצע, אינה כוללת רשות ביטחון כהגדרתה בסעיף 19(ג) לחוק וגוף אחר כאמור בסעיף 24א המוצע, אשר הוראות פרק זה כלל לא חלות לגביהם.

עוד מוצע לקבוע כי שר המשפטים, בהסכמת השר האחראי, כהגדרתו בסעיף המוצע, יקבע בנהלים תנאים

[7] ס"ח התשס"ב, עמ' 179.

"השר האחראי" – כמפורט להלן, לפי העניין:

(1) לעניין הגופים המנויים בפסקאות (1), (2) ו־(4) להגדרה "מערכת הביטחון" – שר הביטחון;

(2) לעניין גופים המנויים בפסקה (3) להגדרה "מערכת הביטחון" – ראש הממשלה;

(3) לעניין שירות בתי הסוהר – השר לביטחון הפנים.

סודיות

23טו. אדם שהגיע אליו מידע בתוקף תפקידו לפי פרק זה, ישמרנו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לפי הוראות חוק זה או לפי צו בית משפט.

**פרק ד'2: אמצעי אביפה מינהליים**

**סימן א': הטלת עיצום כספי**

עיצום כספי

23טז. (א) בסעיף זה –

"מידע בעל רגישות מיוחדת" –

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

(2) מידע רפואי או מידע על מצבו הנפשי של אדם;

(3) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א–2000[8];

## דברי הסבר

לשימוש בסמכויות לפי פרק ד'1 כלפי מערכת הביטחון. תנאים אלה יאפשרו הפעלת הסמכויות האמורות בהתחשב בהיבטים הייחודיים של מערכת הביטחון. נהלים ראשונים כאמור ייקבעו בידי שר המשפטים, בהסכמת השר האחראי, בתוך 90 ימים מיום תחילתו של התיקון המוצע, ובהעדר הסכמה בין הזשרים – בידי ראש הממשלה, בתוך 30 ימים לאחר מכן.

**לסעיף 23טו**

לאור רגישותו האפשרית של המידע שיימסר או שייאסף במסגרת הפעלת הסמכויות לפי פרק זה, מוצע לקבוע חובת סודיות מפורשת ביחס למידע באמור. הפרת חובת הסודיות יכול שתעלה כדי ביצוע עבירה פלילית לפי סעיף 5 לחוק הגנת הפרטיות או לפי סעיף 117 לחוק העונשין, התשל"ז–1977 (להלן – חוק העונשין).

**לפרק ד'2 המוצע**

כפי שפורט בדברי ההסבר לפרק ד'1 המוצע, האביפה במישור הפלילי לבדה אינה מספקת פתרון מלא לאביפת הוראות חוק הגנת הפרטיות הנוגעות למאגרי מידע. מורכבותם של ההליכים הפליליים מביאה לסרבול ועיכוב בתגובה הנאותה למעשי העבירה. כמו כן, לעתים התגובה ההולמת את נסיבות ביצוע ההפרה אינה מצדיקה את האכיפה במישור הפלילי דווקא שאמור להיות מופעל במקרים חמורים.

בהתאם למגמה העולמית בתחום הגנת הפרטיות במאגרי מידע, ובהתאם למגמה בתחום האכיפה החלופית בידי רשויות פיקוח בישראל, מוצע לקבוע בחוק סמכות לממונה להטיל סנקציה מינהלית בשל הפרת חלק מהוראות החוק, המתאימות לאכיפה בדרך זו. בכך תינתן לממונה סמכות יעילה ומידתית שמאפשרת לטפל במקרים של אי־ציות לחוק באופן מדורג שהולם את סוגי ההפרות השונות ואת נסיבות הביצוע השונות שלהן.

סמכות זו, המאפשרת אכיפה באמצעים מינהליים, כפופה לכללי המשפט המינהלי, בין השאר בכל הנוגע לדיות הראיות הנדרשות להטלת הסנקציה המינהלית, לזכות השימוע בטרם הטלתה, ולזכות לעתור נגד ההחלטה המינהלית לאחר קבלתה.

**לסימן א'**

**לסעיף 23טז**

סעיף 23טז המוצע מסמיך את הממונה להטיל עיצום כספי בשל הפרת הוראות החוק המנויות בסעיף. תכליתו של העיצום הכספי איננה ענישה, אלא כפיית ציות וההחזרת מפוקה למשטר ציות להוראות החוק. העיצום הכספי מהווה תחליף למנגנונים פליליים דוגמת עבירות מינהליות ועבירות אחריות קפידה. האכיפה המינהלית

[8] ס"ח התשס"א, עמ' 62.

(4) מידע על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם;

(5) מידע על אודות עברו הפלילי של אדם;

(6) נתוני מנוי ונתוני מיקום כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007[9];

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

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

(9) מידע נוסף שקבע שר המשפטים, בצו, באישור ועדת החוקה חוק ומשפט של הכנסת;

"מידע רגיל" – מידע שאינו מידע בעל רגישות מיוחדת;

"הסכום הבסיסי" – סכום כמפורט להלן, לפי העניין:

(1) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים שאינו עולה על 1,000, שיש בו רק מידע רגיל – 5,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 50,000 ש"ח;

(2) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים העולה על 1,000 ואינו עולה על 10,000, שיש בו רק מידע רגיל – 10,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 100,000 ש"ח;

(3) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים העולה על 10,000 ואינו עולה על 100,00, שיש בו רק מידע רגיל – 20,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 200,000 ש"ח;

(4) לעניין הפרה בקשר למאגר מידע הכולל מידע על מספר אנשים העולה על 100,000 ואינו עולה על 1,000,000, שיש בו רק מידע רגיל – 40,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 400,000 ש"ח;

(5) לעניין הפרה בקשר למאגר מידע שיש בו מידע על מספר אנשים העולה על 1,000,000, שיש בו רק מידע רגיל – 80,000 ש"ח; ואם יש בו גם מידע בעל רגישות מיוחדת – 800,000 ש"ח.

(ב) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בסכום הבסיסי:

## דברי הסבר

מכוונת להוראות שבירורן העובדתי פשוט, הן בתחום מומחיותו של הרגולטור ולפיכך ההכרעה בדבר ביצוע ההפרה תיעשה במהירות ויעילות.

ההפרות המנויות בסעיף 23טז המוצע, מחולקות לשלוש קבוצות לפי דרגת חומרה עולה. ההוראות המנויות בסעיף 23טז(ד) הן ההפרות החמורות ביותר – ולכן הפרתן

[9] ס"ח התשס"ח, עמ' 72.

(1) ניהל או החזיק מאגר מידע החייב ברישום שלא בהתאם להוראות סעיף 8(א);

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

(3) לא הודיע לממונה על שינוי בפרט מהפרטים המפורטים בסעיף 9(ב) או לפי סעיף 9(ג), בניגוד להוראות סעיף 9(ד);

(4) החזיק ברשותו חמישה מאגרי מידע לפחות, החייבים ברישום לפי סעיף 8, ולא קיים את חובת הדיווח השנתי בהתאם להוראות סעיף 17א(ב);

(5) ניהל או החזיק מאגר מידע המשמש לשירותי דיוור ישיר, בלי שיש בידו רישום המציין את המקור שממנו קיבל כל אוסף נתונים המשמש לצורך מאגר המידע ומועד קבלתו וכן למי מסר כל אוסף נתונים כאמור, בניגוד להוראות סעיף 17ה;

(6) לא פירט על דרישת מידע כי הוא מוסר דרך קבע מידע בהתאם לסעיף 23ג, בניגוד להוראות סעיף 23ד(א);

(7) לא קיים רישום של המידע שמסר בהתאם לסעיף 23ג, בניגוד להוראות סעיף 23ד(ב);

(8) לא הודיע לממונה כי הוא מקבל מידע דרך קבע בהתאם לסעיף 23ג והמידע נאגר במאגר מידע, בניגוד להוראות סעיף 23ד(ג);

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

(ג) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בשיעור של כפל הסכום הבסיסי:

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

(2) סירב לאפשר לאדם שמידע עליו מוחזק במאגר מידע לעיין במידע שעליו, בניגוד להוראות לפי סעיף 13;

(3) ביצע שינוי במידע שברשותו בלי שהודיע עליו לכל מי שקיבל את המידע, בניגוד להוראות לפי סעיף 14(ב);

## דברי הסבר

יכולה להביא להטלת העיצום הכספי שבמרגר החומרה הגבוה ביותר.

קביעת סכום העיצום הכספי ביחס להפרות המנויות בסעיף 23טז המוצע, מבוססת על נוסחה אשר בבסיסה סכום בסיסי, שני פרמטרים משפיעים על סכום העיצום הכספי שהממונה רשאי להטיל: מספר האנשים שעל אודותיהם יש מידע במאגר (ככל שהמספר גדול יותר – סכום העיצום הכספי גדל) ורגישות המידע (הפרות ביחס למידע בעל

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

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

(6) הפר הוראה מההוראות שנקבעו לפי סעיף 17(ב);

(7) החזיק במאגרי מידע של בעלים שונים בלי שהבטיח כי אפשרות הגישה לכל מאגר תהיה נתונה רק למי שהורשו לכך במפורש בהסכם בכתב בינו לבין בעליו של אותו מאגר, בניגוד להוראות סעיף 17א(א);

(8) לא מינה אחראי על הגנת מידע, בניגוד להוראות סעיף 17ב(א);

(9) ניהל או החזיק מאגר מידע המשמש לשירותי דיוור ישיר, בלא שהמאגר היה רשום במרשם ובלא שאחת ממטרותיו הרשומות של המאגר היא שירותי דיוור ישיר, בניגוד להוראות סעיף 17ד;

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

(11) לא נענה לדרישתו של אדם בהתאם לסעיף 17ו(ב), שמידע המתייחס אליו יימחק ממאגר מידע המשמש לדיוור ישיר, בניגוד להוראות סעיף 17ו(ד);

(12) לא נענה לדרישתו של אדם בהתאם לסעיף 17ו(ג), כי מידע המתייחס אליו, לא יימסר לאדם, לסוג בני אדם או לאנשים מסוימים, בניגוד להוראות סעיף 17ו(ד).

(ד) הפר אדם הוראה מההוראות לפי חוק זה, כמפורט להלן, רשאי הממונה להטיל עליו עיצום כספי בשיעור של פי ארבעה מהסכום הבסיסי:

(1) השתמש במידע ממאגר המידע שלא למטרה שלשמה נמסר, בניגוד לסעיף 23מ;

(2) השתמש במידע ממאגר מידע בלא הרשאה של בעל מאגר המידע, או תוך חריגה מהרשאה כאמור, בניגוד לסעיף 23מא; לעניין זה, מי שברשותו עותק של מאגר מידע, או חלק מהותי ממנו – יראו אותו כמי שמשתמש במידע ממאגר המידע, אלא אם כן הוכיח אחרת.

## דברי הסבר

רגישות מיוחדת יגררו הגדלת העיצום הכספי). גם מידת חומרתה של ההפרה משפיעה על גובה העיצום הכספי (מתבטא במכפלות של פי 2 ופי 4 מהסכום הבסיסי).

לצד ההסמכה של הממונה להטיל עיצום כספי, מוצע גם להגביל ולהבנות את שיקול דעתו ולכן הנוסחה שלפיה מחושב סכום העיצום הכספי הסופי, קבועה בחוק.

הודעה על כוונת חיוב

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

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

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

(2) סכום העיצום הכספי והתקופה לתשלומו;

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

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

זכות טיעון

23יח. מפר שנמסרה לו הודעה על כוונת חיוב רשאי לטעון את טענותיו, בכתב, לפני הממונה, לעניין הכוונה להטיל עליו עיצום כספי ולעניין סכומו, בתוך 30 ימים מיום מסירת ההודעה.

החלטת הממונה ודרישת תשלום

23יט. (א) הממונה יחליט, לאחר ששקל את הטענות שנטענו לפי סעיף 23יח, אם להטיל על המפר עיצום כספי, והוא רשאי להפחית את סכום העיצום הכספי לפי הוראות סעיף 23כב.

(ב) החליט הממונה לפי סעיף קטן (א) –

(1) להטיל על המפר עיצום כספי, ימסור לו דרישה לשלם את העיצום הכספי (בפרק זה – דרישת תשלום), שבה יציין, בין השאר, את סכום העיצום הכספי המעודכן, ואת התקופה לתשלומו;

(2) שלא להטיל על המפר עיצום כספי, ימסור לו הודעה על כך בכתב.

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

## דברי הסבר

**לסעיפים 23יז עד 23יט**

כאשר הממונה סבור כי אדם הפר את הוראות החוק ובכוונתו להטיל עליו עיצום כספי, עליו למסור למפר קודם לכן הודעה על כוונה להטיל עיצום כספי. אדם שנמסרה לו הודעה כאמור, רשאי לטעון את טענותיו בכתב לפני הממונה הן לעניין הכוונה להטיל עליו עיצום כספי והן לגבי סכומו, בתוך 30 ימים מיום מסירת ההודעה. לאחר מכן, יחליט הממונה, לאחר ששקל את הטענות שנטענו, אם להטיל על המפר עיצום כספי וכן הוא רשאי להפחית את הסכום לפי הוראות סעיף 23כב המוצע. החליט הממונה להטיל עיצום כספי, ישלח למפר דרישת תשלום ובה יציין את סכום העיצום הכספי המעודכן. החליט הממונה שלא להטיל עיצום כספי, ימסור הודעה על כך למפר בכתב.

הפרה נמשכת והפרה חוזרת

23כב. (א) בהפרה נמשכת ייווסף על העיצום הכספי הקבוע לאותה הפרה, החלק החמישים שלו לכל יום שבו נמשכת ההפרה.

(ב) בהפרה חוזרת ייווסף על העיצום הכספי הקבוע לאותה הפרה, סכום השווה לעיצום הכספי כאמור; לעניין זה, "הפרה חוזרת" – הפרת הוראה מההוראות לפי חוק זה, כאמור בסעיף 23עז, בתוך שנתיים מהפרה קודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע.

הפרה לפי חוק זה וחוק אחר

23כא. על מעשה אחד המהווה הפרה של הוראה מההוראות לפי חוק זה המנויות בפרק ד'2 ושל הוראה מההוראות לפי חוק אחר לא יוטל יותר מעיצום כספי אחד.

סכומים מופחתים

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

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

סכום מעודכן של העיצום הכספי

23כג. (א) העיצום הכספי יהיה לפי סכומו המעודכן ביום מסירת דרישת התשלום, ולגבי מפר שלא טען את טענותיו לפני הממונה כאמור בסעיף 23יט(ג) – ביום מסירת ההודעה על כוונת חיוב; הוגשה עתירה לבית המשפט לעניינים מינהליים על הטלת עיצום כספי ועוכב תשלומו של העיצום הכספי לפי הוראות סעיף 23לד(א), יהיה העיצום הכספי לפי סכומו המעודכן ביום ההחלטה בעתירה.

## דברי הסבר

**לסעיף 23כ**

מוצע לקבוע שכאשר הפרה היא הפרה נמשכת, ייווסף על העיצום הכספי הקבוע לאותה הפרה, החלק החמישים שלו לכל יום שבו נמשכת ההפרה. ערך מוצע לקבוע שכאשר הפרה היא הפרה חוזרת, ייווסף על סכום העיצום הכספי שהיה ניתן להטיל בשל אותה הפרה אילו היתה הפרה ראשונה, סכום השווה לעיצום הכספי כאמור. הפרה חוזרת היא הפרת הוראה מהוראות החוק בתוך שנתיים מההפרה הקודמת של אותה הוראה שבשלה הוטל על המפר עיצום כספי או שבשלה הורשע.

**לסעיף 23כא**

מוצע לקבוע כי במצב שבו בוצע מעשה שמהווה הפרה של הוראה מההוראות לפי חוק זה המנויות בפרק ד'2 שבשלהן ניתן להטיל עיצום כספי ושל הוראה מההוראות לפי חוק אחר – לא יוטל יותר מעיצום כספי אחד. הסדר דומה קבוע בסעיף 48(ז) לחוק איסור מימון טרור, התשס"ה–2005.

**לסעיף 23כב**

הממונה אינו רשאי להטיל עיצום בסכום הנמוך מסכום העיצום הכספי שהחוק קובע לאותה הפרה (כמפורט לעיל), סכום העיצום הספציפי נקבע על יסוד הסכום הבסיסי ובהתחשב בקיומם של פרמטרים שונים בהתאם לנוסחה הקבועה בסעיף 23עז המוצע). עם זאת, כדי לאפשר גמישות והתחשבות, בין השאר במצבים שבהם מדובר במפוקה צייתן שמשתף פעולה עם הממונה, מוצע להסמיך את שר המשפטים לקבוע בתקנות רשימה של מקרים, נסיבות ושיקולים שבשלהם יהיה הממונה רשאי להטיל עיצום כספי בסכומים נמוכים יותר מהקבוע בחוק, ובשיעורים שיקבע שר המשפטים בתקנות.

**לסעיף 23כג**

לסעיף קטן (א) מוצע לקבוע כי העיצום הכספי יהיה לפי סכומו המעודכן במועד מסירת דרישת התשלום, ולגבי מפר שבחר שלא לטענן את טענותיו לפני הממונה כאמור בסעיף 23יט(ג) – הסכום המעודכן ביום מסירת ההודעה על כוונת חיוב. כמו כן, הוגשה עתירה לבית המשפט לעניינים

(ב) הסכום הבסיסי יתעדכן ב־1 בינואר בכל שנה (בסעיף קטן זה – יום העדכון), בהתאם לשיעור שינוי המדד הידוע ביום העדכון לעומת המדד שהיה ידוע ביום כ"ז בשבט התשע"א (1 בפברואר 2011); הסכום האמור יעוגל לסכום הקרוב שהוא מכפלה של 10 שקלים חדשים; לעניין זה, "מדד" – מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה.

(ג) הממונה יפרסם ברשומות הודעה על הסכום הבסיסי המעודכן לפי סעיף קטן (ב).

המועד לתשלום העיצום הכספי

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

הפרשי הצמדה וריבית

23כה. לא שולם עיצום כספי במועד, ייווספו עליו לתקופת הפיגור הפרשי הצמדה וריבית כהגדרתם בחוק פסיקת ריבית והצמדה, התשכ"א–1961[10] (בפרק זה – הפרשי הצמדה וריבית), עד לתשלומו.

גבייה

23כו. עיצום כספי ייגבה לאוצר המדינה, ועל גבייתו תחול פקודת המסים (גבייה)[11].

**סימן ב': התראה מינהלית**

התראה מינהלית

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

## דברי הסבר

מינהליים על הטלת העיצום הכספי, ועוכב תשלומו של העיצום הכספי כאמור בסעיף 23לד(א), יהיה סכום העיצום הכספי – הסכום המעודכן ביום ההחלטה בעתירה.

**לסעיפים קטנים (ב) ו־(ג)**

מוצע לקבוע מנגנון אוטומטי לעדכון סכומי העיצום הכספי, ב־1 בינואר בכל שנה (להלן – יום העדכון), בהתאם לשיעור שינוי מדד המחירים לצרכן שמפרסמת הלשכה המרכזית לסטטיסטיקה, הידוע ביום העדכון, לעומת המדד שהיה ידוע ביום כ"ז בשבט התשע"א (1 בפברואר 2011). עוד מוצע לקבוע כי הממונה יפרסם ברשומות הודעה על סכומי העיצום הכספי המעודכנים כאמור.

**לסעיפים 23כד עד 23כו**

מוצע לקבוע כי העיצום הכספי ישולם בתוך 30 ימים מיום מסירת דרישת התשלום כאמור בסעיף 23יט המוצע, וכי אם לא שולם עיצום כספי במועד, ייווספו עליו לתקופת הפיגור הפרשי הצמדה וריבית עד לתשלומו. עוד מוצע כי עיצום כספי ייגבה לאוצר המדינה ועל גבייתו תחול פקודת המסים (גבייה).

**לסימן ב'**
**לסעיפים 23כז ו־23כט**

בסעיף זה מוצע כלי מינהלי נוסף, חלופי להטלת העיצום הכספי, ההתראה המינהלית. כלי אכיפה זה הוא כלי המיועד לעודד ציות של המפוקחים ולאפשר התמודדות עם הפרות עתידיות, על ידי מתן תמריץ שלילי לביצוען ותמריץ חיובי לציות.

מטרתו של כלי אכיפה זה להביא לשינוי התנהגות, תוך הבהרת חובותיו של המפוקח והחזרתו למשטר של ציות. ההתראה המינהלית תופעל ביחס להפרות שלממונה יש סמכות להטיל בשלהן עיצום כספי.

בעצם משלוח ההתראה יש קביעה של הממונה כי בוצעה על ידי המפוקח הפרה, אך לא יוטל בשלה עיצום כספי, לפיכך, הפעלת ההתראה מחייבת קיומה של תשתית

[10] ס"ח התשכ"א, עמ' 192.

[11] חוקי א"י, כרך ב', עמ' (ע) 1374, (א) 1399.

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

בקשה לביטול התראה מינהלית

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

(1) הוא לא ביצע את ההפרה;

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

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

## דברי הסבר

ראייתית לביצועה של ההפרה, שהיתה מספיקה לצורך הטלת העיצום הכספי. אם המפוקח לא יחזור למשטר הציות, וישוב לבצע הפרות נוספות בעתיד או שימשיך בביצועה של ההפרה שבשלה נשלחה לו ההתראה, יימצא מפר הפרה חוזרת או נמשכת, בהתאמה, ויוטל עליו עיצום כספי בהתאם.

עיקר תכליתה של ההתראה הוא הבהרה ביחס להוראות החוק או לפיו שאינן חד־משמעיות, ולפיכך קיימת אפשרות שהן אינן ברורות דיין למפוקח בגלל עמימות ניסוחן. גם הוראות שטרם הוטמעו בקרב ציבור המפוקחים ונדרשת היערכות ביחס ליכולת לקיימן הן הוראות שראוי ליתן בשלהן התראה טרם אכיפתן באמצעות הטלת סנקציה ישירה. על מצבים אלה חולש התנאי שההפרות המדוברות אינן הפרות שיש בהן חומרה יתרה.

הפרות חמורות מחייבות הפנמת מדיניות רגולציה תקיפה ולכן בכלל לא יהיה ניתן להסתפק בהתראה. גם במצב שבו המפר מפר את ההוראה שלא בפעם הראשונה, לא מתאים השימוש בכלי אכיפה זה. במצב דברים כזה ספק אם ניתן לייחס למפר את חוסר ההבנה שניתן לייחס במצבים מסוימים למפר שזו לו הפעם הראשונה שהוא מפר את הוראות החוק.

כדי להבטיח שקיפות ושוויוניות באכיפה ולהגביר את הוודאות, מוצע לענן את המקרים המתאימים למשלוח התראה, בנהלים שיקבע הממונה באישור היועץ המשפטי לממשלה או משנה ליועץ המשפטי לממשלה שהוא הסמיך לכך.

**לסעיף 23כח**

אף על פי שמשלוח ההתראה אינו מלווה בסנקציה מיידית דוגמת הטלת העיצום הכספי, לנוכח העובדה שיש בה קביעה בדבר ביצועה של הפרה ומשמעויות עתידיות לגבי הפרות נוספות, מוצע לאפשר למפוקח לבקש את ביטולה. לפיכך מוצע לקבוע כי מפר שנמסרה לו התראה מינהלית, רשאי לפנות לממונה, בכתב בתוך 30 ימים, בבקשה לבטל את ההתראה, מהטעמים האלה בלבד: המפר לא ביצע את ההפרה או שהמעשה שביצע המפר, המפורט בהתראה, אינו מהווה הפרה. הממונה רשאי לבטל את ההתראה או לדחות את הבקשה ולהותיר את ההתראה על כנה. החלטת הממונה תינתן למפר בכתב בצירוף נימוקי ההחלטה.

**לסימן ג'**

כלי אכיפה נוסף שמוצע לתת בידי הממונה, אף הוא חלופי להטלת עיצום כספי, הוא התחייבות להימנע מהפרה. ההתחייבות היא מעין "עיצום כספי על תנאי", היא מיועדת לשימוש כלפי מפרים שביצוע הפרות אינו מאפיין אותם ברגיל.

משמעות ההתחייבות היא כי על אף שקיימת תשתית להוכחת ביצוע הפרה, העיצום הכספי נדחה לתקופה שבמסגרתה נדרש המפוקח לקיים את הוראות החוק, ואף תנאים נוספים נלווים שלדעת הממונה יש בהם כדי להביא לצמצום הנזק שנגרם, לתיקון הליקויים שנמצאו ולהבטחת הציות של המפוקח. על המפר למלאם בתוך פרק זמן שיפורט אף הוא בהתחייבות.

השוני בין ההתחייבות וההתראה המינהלית נעוץ, בין השאר, בצורך לקבל את הסכמת המפר לתנאי ההתחייבות, ובכלל זה את הסכמתו לצעדים שעליו לבצע וללוח הזמנים

הפרה נמשכת והפרה חוזרת לאחר התראה

23בט. (א) נמסרה למפר התראה מינהלית לפי הוראות סימן זה והמפר המשיך להפר את ההוראה שבשלה נשלחה לו ההתראה, ימסור לו הממונה דרישת תשלום בשל הפרה נמשכת כאמור בסעיף 23כ(א).

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

**סימן ג': התחייבות להימנע מהפרה**

התחייבות להימנע מהפרה

23ל. (א) היה לממונה יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי חוק זה, כאמור בסעיף 23ט1, והתקיימו נסיבות שקבע הממונה, בנהלים, באישור היועץ המשפטי לממשלה, רשאי הוא להמציא למפר, במקום הודעה על כוונת חיוב, הודעה שלפיה באפשרותו להגיש לממונה כתב התחייבות ועירבון לפי הוראות סימן זה, במקום שיוטל עליו עיצום כספי לפי הוראות סימן א'; בסעיף קטן זה, "היועץ המשפטי לממשלה" – לרבות משנה ליועץ המשפטי לממשלה שהוא הסמיכו לעניין זה.

(ב) בכתב ההתחייבות יתחייב המפר להפסיק את הפרת ההוראה כאמור בסעיף קטן (א), ולהימנע מהפרה נוספת של אותה הוראה, בתוך תקופה שיקבע הממונה, ושתחילתה ביום מסירת ההודעה כאמור באותו סעיף קטן ובלבד שהתקופה האמורה לא תעלה על שנתיים (בסימן זה – תקופת ההתחייבות).

(ג) הממונה רשאי לדרוש כי המפר יכלול בכתב ההתחייבות תנאים נוספים שעליו לעמוד בהם במהלך תקופת ההתחייבות לשם הקטנת הנזק שנגרם מההפרה או מניעת הישנותה.

(ד) נוסף על כתב ההתחייבות יפקיד המפר בידי הממונה עירבון בסכום העיצום הכספי שהממונה היה רשאי להטיל על המפר בשל אותה הפרה, בהתחשב בקיומם של מקרים, נסיבות ושיקולים שנקבעו לפי סעיף 23כב(ב).

## דברי הסבר

שבו עליו לעמוד. בדומה להתראה המינהלית, גם לצורך הצעת התחייבות למפר חלף הטלת עיצום כספי, נדרשת תשתית ראייתית שמספיקה להטלת עיצום כספי. זאת במיוחד באשר אי־הסכמה של המפר להתחייבות תוביל להטלה של עיצום כספי עליו.

**לסעיף 23ל**

מוצע לקבוע כי אם היה לממונה יסוד סביר להניח כי אדם הפר הוראה מההוראות לפי החוק, שניתן להטיל בשלה עיצום כספי, והתקיימו נסיבות המנויות בנהלים שקבע הממונה, באישור היועץ המשפטי לממשלה או משנה ליועץ המשפטי לממשלה שהוא הסמיך לכך, הוא רשאי, במקום להמציא למפר הודעה על כוונת חיוב ולהטיל עליו עיצום כספי, להמציא לו הודעה שיש באפשרותו להגיש לממונה כתב התחייבות ועירבון במקום שיוטל עליו עיצום כספי. בכתב ההתחייבות המפר יתחייב להפסיק את ההפרה ולהימנע מהפרה נוספת של אותה הוראה בתוך תקופה שיקבע הממונה ושתחילתה ביום מסירת ההודעה, ובלבד שהתקופה האמורה לא תעלה על שנתיים.

הממונה רשאי לקבוע בכתב ההתחייבות תנאים נוספים שעל המפר להתחייב ולעמוד בהם בתקופת ההתחייבות, במטרה להקטין את הנזק שנגרם מההפרה או למנוע את הישנותה.

תרצאות הגשת כתב התחייבות ועירבון או אי־הגשתם

23לא. הגיש המפר לממונה כתב התחייבות ועירבון לפי סימן זה, בתוך 30 ימים מיום מסירת ההודעה כאמור בסעיף 23ל(א), לא יוטל עליו עיצום כספי בשל אותה הפרה; לא הגיש המפר לממונה כתב התחייבות ועירבון בתוך התקופה האמורה, ימציא לו הממונה הודעה על כוונת חיוב בשל אותה הפרה, לפי סעיף 23יז.

הפרת התחייבות

23לב. (א) הגיש המפר כתב התחייבות ועירבון לפי סימן זה והפר תנאי מתנאי ההתחייבות, כמפורט בפסקאות שלהלן, יחולו ההוראות המפורטות באותן פסקאות, לפי העניין:

(1) המשיך המפר, במהלך תקופת ההתחייבות, להפר את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – יחלט הממונה את העירבון וימציא למפר דרישת תשלום בשל ההפרה הנמשכת כאמור בסעיף 23ב(א);

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

(3) הפר המפר תנאי מהתנאים הנוספים שנקבעו בכתב ההתחייבות כאמור בסעיף 23ל(ג) – יחלט הממונה את העירבון.

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

## דברי הסבר

העירבון שיופקד נוסף על כתב ההתחייבות, יהיה בגובה העיצום הכספי שהממונה היה רשאי להטיל על המפר בשל אותה הפרה, בהתחשב בקיומן של נסיבות הפחתה לפי החוק.

**לסעיף 23לא**

אם הגיש המפר לממונה כתב התחייבות ועירבון כאמור, בתוך 30 ימים מיום שנמסרה לו הודעת הממונה כאמור בסעיף 23בט(א), לא יוטל עליו עיצום כספי בשל אותה הפרה. אם לא הגיש המפר לממונה כתב התחייבות ועירבון בתוך 30 ימים כאמור, הממונה ימציא לו הודעה על כוונת חיוב בשל אותה הפרה, לפי סעיף 23יז.

**לסעיף 23לב**

מוצע לקבוע שאם המפר הפר תנאי מתנאי ההתחייבות, יהיה ניתן לפעול כדלקמן:

(1) אם המפר המשיך להפר, במהלך תקופת ההתחייבות, את ההוראה שבשל הפרתה נתן כתב התחייבות – הממונה יחלט את העירבון וימציא למפר דרישת תשלום בשל ההפרה הנמשכת;

(2) אם המפר חזר והפר במהלך תקופת ההתחייבות את ההוראה שבשל הפרתה נתן את כתב ההתחייבות – הממונה יחלט את העירבון וימציא למפר הודעה על כוונת חיוב בשל ההפרה החוזרת;

(3) אם המפר הפר תנאי מהתנאים הנוספים שקבע הממונה בכתב ההתחייבות – הממונה יחלט את העירבון.

עוד מוצע לקבוע כי יראו חילוט של העירבון לפי סעיף זה, כהטלת עיצום כספי על המפר בשל ההפרה שלגביה ניתן העירבון.

כמו כן מוצע לקבוע כי אם הופר תנאי מתנאי ההתחייבות, והמפר הפר פעם נוספת את ההוראה שבשל הפרתה נתן את כתב ההתחייבות, לא יאפשר הממונה למפר להגיש כתב התחייבות נוסף בשל ההפרה הנוספת.

(ג) הופר תנאי מתנאי ההתחייבות כאמור בסעיף זה, והפר המפר פעם נוספת את ההוראה שבשל הפרתה נתן את כתב ההתחייבות, לא יאפשר לו הממונה להגיש כתב התחייבות נוסף לפי הוראות סימן זה, בשל אותה הפרה.

השבת העירבון

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

**סימן ד': שונות**

עיכוב תשלום העיצום הכספי והחזרתו

23לה. (א) אין בהגשת עתירה לפי חוק בתי משפט לעניינים מינהליים, התש"ס–2000[12], על הטלת עיצום כספי, כדי לעכב את תשלום העיצום הכספי, אלא אם כן הסכים לכך הממונה או שבית משפט הורה על כך.

(ב) החליט בית המשפט לקבל עתירה כאמור בסעיף קטן (א), לאחר ששולם העיצום הכספי לפי הוראות פרק זה, יוחזר העיצום הכספי או כל חלק ממנו אשר הופחת בידי בית המשפט, בתוספת הפרשי הצמדה וריבית מיום תשלומו עד יום החזרתו.

פרסום

23לה. (א) הטיל הממונה עיצום כספי לפי פרק זה, יפרסם הממונה את הפרטים שלהלן, בדרך שתבטיח שקיפות לגבי הפעלת שיקול דעתו בקבלת ההחלטה להטיל עיצום כספי:

(1) דבר הטלת העיצום הכספי;

(2) מהות ההפרה שבשלה הוטל העיצום הכספי ונסיבות ההפרה;

(3) סכום העיצום הכספי שהוטל;

## דברי הסבר

**לסעיף 23לג**

מוצע לקבוע כי אם עמד המפר בתנאי כתב ההתחייבות, יוחזר לו, בתום תקופת ההתחייבות, העירבון שהפקיד בתוספת הפרשי הצמדה וריבית מיום הפקדתו עד יום החזרתו.

**לסימן ד' לסעיף 23לד**

מוצע לקבוע ברירת מחדל ולפיה אין בהגשת עתירה לפי חוק בתי משפט לעניינים מינהליים, התש"ס–2000, על הטלת עיצום כספי, כדי לעכב את תשלום העיצום הכספי אלא אם כן הסכים לכך הממונה או שבית המשפט הורה על כך.

עוד מוצע לקבוע כי אם החליט בית משפט לקבל עתירה על הטלת עיצום כספי, לאחר ששולם העיצום הכספי, יוחזר העיצום הכספי או כל חלק ממנו אשר הופחת בידי בית המשפט, בתוספת הפרשי הצמדה וריבית מיום תשלומו עד יום החזרתו.

**לסעיף 23לה**

מוצע לחייב את הממונה לפרסם את החלטותיו בדבר הטלת העיצום הכספי. פרסום החלטות הממונה הוא כלי שתכליתו היא הבטחת שקיפות ביחס להפעלת שיקול הדעת של הממונה בהטלת העיצום הכספי, בידיו של הממונה מסור כלי רב עוצמה, מבחינת היקף הסנקציות שהוא יכול להטיל. לפיכך, וכדי להבטיח כי השימוש באותו כלי נעשה באופן שוויוני ועניני, מוצע לחייב את הממונה לפרסם את החלטותיו בדבר הטלת העיצומים הכספיים, סכומיהם ושיעורי ההפחתה, אם הופחת סכום העיצום הכספי. פרטי הפרסום יהיו כאלה שיאפשרו לציבור לבחון ולבקר את החלטות הממונה. עוד מוצע לקבוע כי אם הוגשה עתירה על הטלת עיצום כספי, יפרסם הממונה את דבר הגשת העתירה ואת תוצאותיה.

הפרסום, ככלל לא יכלול את שמות המפרים, ככל שהם יחידים, אלא אם כן הדבר נחוץ כדי להזהיר את הציבור מפניהם. כן יימנע הממונה מפרסום פרטים שנאסר פרסומם לפי הוראות סעיף 9(א) לחוק חופש המידע,

[12] ס"ח התש"ס, עמ' 190.

(4) אם הופחת העיצום הכספי – הנסיבות שבשלהן הופחת סכום העיצום ושיעורי ההפחתה;

(5) פרטים על אודות המפר;

(6) שמו של המפר – ככל שהמפר הוא תאגיד.

(ב) הוגשה עתירה על הטלת עיצום כספי, יפרסם הממונה את דבר הגשת העתירה ואת תוצאותיה.

(ג) על אף הוראות סעיף קטן (א)(6), רשאי הממונה לפרסם את שמו של מפר שהוא יחיד, אם סבר שהדבר נחוץ לצורך אזהרת הציבור, וכבל שהמפר מחזיק או מנהל מאגר מידע.

(ד) על אף האמור בסעיף זה, לא יפרסם הממונה פרטים שהם בגדר מידע שרשות ציבורית מנועה מלמסור לפי סעיף 9(א) לחוק חופש המידע, התשנ"ח–1998[13], וכן הוא רשאי שלא לפרסם פרטים לפי סעיף זה, שהם בגדר מידע שרשות ציבורית אינה חייבת למסור לפי סעיף 9(ב) לחוק האמור.

שמירת אחריות פלילית

23לו. (א) תשלום עיצום כספי, המצאת התראה מינהלית או מתן כתב התחייבות ועירבון, לפי פרק זה, לא יגרעו מאחריותו הפלילית של אדם בשל הפרת הוראה מההוראות לפי חוק זה, המהווה עבירה.

(ב) הוגש נגד אדם כתב אישום בשל הפרה המהווה עבירה לפי חוק זה, לא ינקוט נגדו הממונה הליכים לפי פרק זה בשל אותה הפרה, ואם שילם המפר עיצום כספי או הפקיד עירבון כאמור בסעיף 23לא(א) – יוחזר לו הסכום ששולם או העירבון שהופקד, לפי העניין, בתוספת הפרשי הצמדה וריבית מיום תשלום הסכום או יום הפקדת העירבון, עד יום החזרתו.

**פרק ד'3: עבירות**

הפרעה לממונה במילוי תפקידו

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

## דברי הסבר

התשנ"ח–1998, והוא רשאי שלא לפרסם פרטים מהטעמים המנויים בסעיף 9(ב) לאותו חוק.

**לסעיף 23לו**

ישנן הוראות בחוק שאכיפתן יכולה להתבצע הן במישור המינהלי והן במישור הפלילי. אף על פי שאין המדובר בסיכון כפול, הטלת סנקציות בשני המישורים היא אמצעי העולה על הנדרש. לפיכך הסעיף המוצע מבהיר כי אף על פי שננקט הליך מינהלי לפי פרק ד'2 המוצע, אין בכך כדי לגרוע מאחריותו הפלילית של המפר. עם זאת, אם הוגש נגד מפר כתב אישום בשל הפרת הוראה מהוראות החוק שהיא גם עבירה, לא ינקוט נגדו הממונה הליכים לפי פרק זה ואם המפר שילם עיצום כספי או הפקיד עירבון, יוחזר לו הסכום ששילם או העירבון שהופקד, בתוספת הפרשי הצמדה וריבית מיום תשלומו או הפקדתו עד יום החזרתו.

**לפרק ד'3 המוצע**

מוצע להתאים את חלק העונשין בחוק בנוגע למאגרי מידע, להסדרה המפורטת שבהצעת חוק זו. על חלק מהפרות החוק מוצע לקבוע סנקציה מינהלית, ועל אלה שיש בהן מידה של חומרה יתרה, הנלמדת, בין השאר, מהיסוד הנפשי המלווה אותם או מפוטנציאל הנזק לציבור הגלום בהן – מוצע כי יוגדרו כעבירות פליליות בחלק העונשין של החוק וייאכפו במישור הפלילי.

**לסעיף 23לז**

מוצע לקבוע כי מי שמפריע לממונה, או לחוקר או למפקח מטעמו, במילוי תפקידו לפי החוק, דינו – מאסר שישה חודשים. התנהגות זו היא התנהגות שראוי להגדירה כעבירה פלילית המלווה באפשרות להטיל סנקציה פלילית נאותה.

[13] ס"ח התשנ"ח, עמ' 226.

הפרה בכוונה להטעות

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

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

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

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

אי־מסירת הודעה בכוונה להטעות

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

שימוש במידע ממאגר מידע בניגוד למטרה שלשמה נמסר

23מ. בעל מאגר מידע או מחזיק בו, המשתמש במידע ממאגר המידע שלא למטרה שלשמה נמסר, או המתיר זאת לאחר, דינו כדין הפוגע במזיד בפרטיות זולתו לפי סעיף 5.

שימוש במידע ממאגר מידע בלא הרשאה

23מא. (א) לא ישתמש אדם במידע ממאגר מידע בלא הרשאה של בעל מאגר המידע, או בחריגה מהרשאה כאמור; לעניין זה, מי שברשותו עותק של מאגר מידע, או חלק מהותי ממנו – יראו אותו כמי שמשתמש במידע ממאגר המידע, אלא אם כן הוכיח אחרת.

## דברי הסבר

**לסעיף 23לח**

מוצע לקבוע בעבירות פליליות שדינן מאסר שלוש שנים, כמה התנהגויות המבוצעות בכוונה להטעות את הממונה או מפקח מטעמו, שיש להן קשר ישיר להפעלת הפיקוח על ניהול מאגרי המידע: כתיבת פרטים לא נכונים בבקשה לרישום מאגר מידע, אי־הודעה לממונה על שינוי בפרטים על אודות המאגר בניגוד לחובה הקבועה בחוק, מסירת פרטים לא נכונים במענה לדרישה של הממונה או של מפקח. התנהגויות אלה הן התנהגויות שראוי להגדירן בעבירה פלילית המלווה באפשרות להטיל סנקציה פלילית נאותה.

**לסעיף 23לט**

סעיף זה עוסק בפגיעה חמורה בנושא המידע עצמו. ההימנעות ממסירת ההודעה לפי סעיף 11 לחוק (הודעה המבהירה לנושא המידע אם חלה עליו חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו ובהסכמתו, מה המטרה שלשמה מבוקש המידע ולמי יימסר המידע ומטרות המסירה), מתוך כוונה לקבל את המידע במרמה, מפירה את זכותו הבסיסית של נושא המידע שלא תיפגע פרטיותו בלא הסכמתו מדעת (סעיף 1 לחוק), בלא קבלת הודעה הכוללת את הפרטים האמורים אין לנושא המידע יכולת לגבש הסכמה מדעת למסירת המידע, וגם אין אפשרות מעשית לבחון אם נעשה במידע שימוש שלא למטרה לשמה נמסר. מוצע לקבוע לעבירה לפי סעיף זה, עונש מאסר של שלוש שנים.

**לסעיף 23מ**

מוצע לקבוע עבירה ספציפית לגבי מאגרי מידע, המבוססת על שימוש במידע שבמאגר שלא למטרה שלשמה נמסר המידע. עיקרון זה הוא אחד מהעקרונות היסודיים בדיני הפרטיות במידע והוא מנוי בסעיפים 2(9) ו־8(ב) לחוק. הפרתו מממשת את פוטנציאל הסיכון הגלום בעיבוד מידע ממוחשב. הענישה בשל עבירה זו נגזרת מהוראת הקבוע בסעיף 5 לחוק.

**לסעיף 23מא**

מוצע לקבוע כעבירה שדינה מאסר שלוש שנים, שימוש במידע ממאגר מידע בלא הרשאה מבעל המאגר בהתנהגות זו יש פגיעה בפרטיות נושאי המידע, באשר יש בה שימוש במידע שלא למטרה שלשמה נאסף ובלא הסכמתו של נושא המידע.

(ב) המשתמש במידע ממאגר מידע בלא הרשאה או בחריגה מהרשאה, כאמור בסעיף קטן (א), דינו – מאסר שלוש שנים.

מסירת מידע מגוף ציבורי

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

תחולה על ידיעות על ענייניו הפרטיים של אדם

23מג. הוראות סעיפים 23מ עד 23מב יחולו על ידיעות על ענייניו הפרטיים של אדם, אף שאינן בגדר מידע, כשם שהן חלות על מידע.

אחריות נושא משרה בתאגיד

23מד (א) נושא משרה בתאגיד חייב לפקח ולעשות כל שניתן למניעת עבירות לפי סעיפים 16 ו־23מ עד 23מב בידי התאגיד או בידי עובד מעובדיו; המפר את חובתו האמורה, דינו – קנס כאמור בסעיף 61(א)(4) לחוק העונשין.

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

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

## דברי הסבר

**לסעיף 23מב**

גופים ציבוריים אוספים מידע אישי במאגרי מידע ומקבלים מידע מגופים ציבוריים אחרים, והדבר יוצר סיכונים לפרטיותם של נושאי המידע. לכן מוצע לקבוע בסעיף זה, כי מי שמוסר מידע מגוף ציבורי בניגוד להוראות פרק ד' לחוק הגנת הפרטיות מבצע עבירה פלילית, ודינו – מאסר שלוש שנים.

**לסעיף 23מג**

מוצע כי סעיפים 23מ, 23מא ו־23מב, יחולו גם על ידיעות על ענייניו הפרטיים של אדם שאינן "מידע" כהגדרתו בסעיף 7 לחוק.

**לסעיף 23מד**

מוצע להטיל חובת פיקוח על נושא משרה בתאגיד, ולפיה עליו לפקח ולעשות כל שניתן למניעת עבירות לפי סעיפים 16 ו־23מ עד 23מב לחוק, בידי התאגיד ועובדיו. חובה זו של נושא המשרה היא נדבך חשוב בתמרוץ התאגיד לציית להוראות החוק. ככל שנושא המשרה יימצא מפר את חובת הפיקוח הזו, תוטל עליו אחריות פלילית. עוד קובע הסעיף כי אם בוצעה עבירה על הוראות הסעיפים האמורים בידי התאגיד או אחד מעובדיו, חזקה היא , הניתנת לסתירה, שנושא המשרה הפר את חובת הפיקוח.

הנחת הבסיס בסעיף זה היא כי חלק מתפקידו של נושא משרה בתאגיד הוא ליצור הליכי עבודה ונהלים שתכליתם הטמעה של הוראות הרגולציה המחייבות ביחס למאגרי המידע שיש לתאגיד, וכן שמתפקידו לפקח ולהבטיח כי הוראות אלה מקוימות בידי התאגיד ועובדיו. העבירות המקימות את החזקה שנושא המשרה לא קיים את חובת הפיקוח שלו, הוגבלו לעבירות שמשקפות מצב שבו הוראות רגולציה שעל התאגיד לקיים – הופרו, שכן ההנחה היא שפעילות הטמעה של הוראות אלה היתה יכולה למנוע זאת.

סתירת החזקה האמורה יכולה להיעשות על ידי הוכחה של נושא המשרה כי עשה כל שניתן כדי למלא את חובתו. פעילות הדרכה והטמעת הוראות הקשורות ביישום החובות לפי החוק בקרב העובדים, פעולות ביקורת ובקרה, ופעולה של נושא המשרה להפסקת ההפרה ומניעת הישנותה יכולים לשמש לסתירת החזקה האמורה.

התראה לעובד רשות ציבורית

23מה. (א) בוצע מעשה או מחדל שניתן להטיל בשלו עיצום כספי לפי הוראות סעיף 23טז(ב), (ג) או (ד) (בסעיף זה – ההפרה), בידי רשות ציבורית, או נעברה עבירה לפי סעיפים 16 או 23לח עד 23מב בידי רשות ציבורית, רשאי הממונה לשלוח התראה לעובד אחראי ברשות הציבורית (בסעיף זה – ההתראה), שלפיה עליו לפקח על כך שהרשות הציבורית תנקוט אמצעים כמפורט להלן, לפי העניין, במהלך התקופה הנקובה בהתראה, וכי אם לא יעשה כן יהיה צפוי לקנס כאמור בסעיף קטן (ב) –

(1) אמצעים להפסקת ההפרה או העבירה המפורטת בהתראה;

(2) אמצעים למניעת הישנות ההפרה או העבירה.

(ב) לא ביצעה רשות ציבורית את האמור בהתראה, יראו את העובד האחראי ברשות הציבורית כאילו הפר את חובתו האמורה בסעיף קטן (א), אלא אם כן הוכיח כי עשה כל שניתן בנסיבות העניין כדי למלא את חובתו האמורה, ודינו – קנס כאמור בסעיף 61(א)(2) לחוק העונשין.

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

(ד) בסעיף זה –

"רשות ציבורית" – משרד ממשלתי ויחידת סמך של משרד ממשלתי;

"עובד אחראי" – מנהל רשות ציבורית."

הוספת סעיף 24א

8. אחרי סעיף 24 לחוק העיקרי יבוא:

"אי־תחולה על רשות ביטחון ועל גוף אחר

24א. (א) הוראות פרקים ד'1 עד ד'3 לא יחולו על רשות ביטחון כהגדרתה בסעיף 19(ג) ועל כל גוף אחר שקבע שר הביטחון, בצו, בהסכמת שר המשפטים.

## דברי הסבר

**לסעיף 23מה**

סעיף זה קובע מנגנון שתכליתו הגברת הציות להוראות החוק ברשויות ציבוריות. לפי הסעיף המוצע במקרה שבו נמצא שרשות ציבורית הפרה הוראה מהוראות החוק שניתן להטיל בשלה עיצום כספי או עברה עבירה לפי סעיפים 16 או 23לח עד 23מב, רשאי הממונה לשלוח התראה לעובד אחראי ברשות הציבורית (המוגדר כבעל התפקיד הבכיר באותה רשות – המנהל), בהתראה יידרש העובד האחראי לפקח על כך שהרשות תנקוט אמצעים להפסקת ביצוע ההפרה או העבירה, או למניעת הישנותה, וכי אם לא יעשה כן יהיה צפוי לקנס כאמור בסעיף 61(א)(2) לחוק העונשין.

אם הרשות הציבורית לא ביצעה את האמור בהתראה, קמה חזקה ולפיה לא קיים העובד האחראי את חובתו לפקח על נקיטת האמצעים כאמור אלא אם כן הוכיח שעשה כל שניתן בנסיבות העניין לקיום חובתו האמורה.

לנוכח ההכרה ביכולת השליטה המוגבלת של הקצאת המשאבים בגוף ציבורי, שנדרשים לעתים לשם קיום הדרישות המנויות בהתראה שנשלחה לעובד האחראי, מטיל הסעיף המוצע כמה מגבלות:

ראשית, הסעיף מכוון לבעל התפקיד הבכיר בהיררכיה הניהולית, מתוך הנחה שיש לו יכולת השפעה מרבית על התנהלות הרשות ועל תקציבה.

שנית, הגשת כתב אישום נגד העובד האחראי טעונה אישור של היועץ המשפטי לממשלה. במסגרת זו תיבחן השאלה אם עשה העובד האחראי כל שניתן כדי להניע את הרשות הציבורית לבצע את שנדרש בהתראה. שיקול לגיטימי בהקשר זה יכול שיהיה המניעה התקציבית שבשלה לא בוצעו הצעדים המנויים בהתראה.

**סעיף 8** מוצע לקבוע בסעיף 24א המוצע, כי הוראות פרקים ד'1 עד ד'3 לחוק לא יחולו על רשות

(ב) שר הביטחון, בהסכמת שר המשפטים, רשאי שלא לכלול בפרסום ברשומות של צו כאמור בסעיף קטן (א), את שמו של גוף שלגביו הוצא הצו האמור, מטעמים של שמירה על ביטחון המדינה, ואולם הנוסח המלא של הצו, הכולל את שמו של הגוף האמור, יופקד אצל שר המשפטים."

תיקון סעיף 31א

9. בסעיף 31א לחוק העיקרי, אחרי סעיף קטן (ב) יבוא:

"(ג) הוראות סעיף זה יחולו רק על רשות ביטחון ועל גוף אחר שחלים עליהם הוראות סעיף 24א."

תיקון חוק הרשויות המקומיות (בחירות)

10. בחוק הרשויות המקומיות (בחירות), התשכ"ה–1965[14], בסעיף 16(ה), במקום "לרשם מאגרי המידע כהגדרתו בחוק" יבוא "לממונה על הגנת מידע כהגדרתו בסעיף 7 לחוק".

תיקון חוק הבחירות לכנסת

11. בחוק הבחירות לכנסת [נוסח משולב], התשכ"ט–1969[15], בסעיף 39(ה), במקום "לרשם מאגרי המידע כהגדרתו בחוק" יבוא "לממונה על הגנת מידע כהגדרתו בסעיף 7 לחוק".

תיקון חוק סדר הדין הפלילי

12. בחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב–1982, בתוספת השלישית, בפרט (5), בטור ב' יבוא:

"ב. סעיף 23מה לחוק הגנת הפרטיות, התשמ"א–1981."

תיקון חוק בתי משפט לעניינים מינהליים

13. בחוק בתי משפט לעניינים מינהליים, התש"ס–2000, בתוספת הראשונה, בפרט 28, במקום "הרשם" יבוא "הממונה".

תיקון חוק הפיקוח על שירותים פיננסיים (עיסוק בייעוץ פנסיוני ובשיווק פנסיוני)

14. בחוק הפיקוח על שירותים פיננסיים (עיסוק בייעוץ פנסיוני ובשיווק פנסיוני), התשס"ה–2005[16] –

(1) בסעיף 231(א)(6), במקום "הרשם" יבוא "הממונה על הגנת מידע" ובמקום "רשם מאגרי המידע" יבוא "הממונה על הגנת מידע";

## דברי הסבר

ביטחון כהגדרתה בסעיף 19(ג) לחוק ועל כל גוף אחר שקבע שר הביטחון, בצו, בהסכמת שר המשפטים. עוד מוצע כי שר הביטחון, בהסכמת שר המשפטים, רשאי שלא לכלול בפרסום ברשומות של צו כאמור, את שמו של גוף שלגביו הוצא הצו, מטעמים של שמירה על ביטחון המדינה, ואולם הנוסח המלא של הצו, הכולל את שמו של הגוף האמור, יופקד אצל שר המשפטים.

על הגופים שיוחרגו מתחולת פרקים ד' עד ד'3 כאמור – ימשיך לחול הדין הקיים (התיקונים הנדרשים לעניין זה מופיעים בסעיפים 3 ו-9 להצעת החוק) וההסדרים החדשים לא יחולו, וזאת עד שתושלם הבחינה באשר לדרך המתאימה לפיקוח על מילוי הוראות החוק הנוגעות למאגרי המידע של גופים אלה.

**סעיף 9** בפרקים ד'2 ו-ד'3 המוצעים נקבעו הוראות לעניין הפרות ועבירות במאגרי מידע, שנועדו להחליף את האמור בסעיף 31א לחוק. מאחר שבהתאם למוצע בסעיף 8 להצעת החוק, הוראות פרקים ד'2 ו-ד'3 לחוק לא יחולו על רשות ביטחון כהגדרתה בסעיף 19(ג) לחוק ועל כל גוף אחר שנקבע בידי שר הביטחון כאמור בסעיף 24א לחוק, מוצע להגביל את תחולתו של סעיף 31א לחוק רק לרשות ביטחון ולגוף אחר כאמור.

**סעיף 12** מוצע לתקן את התוספת השלישית לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב–1982, כדי לאפשר אצילה של סמכות היועץ המשפטי לממשלה לאשר הגשת כתב אישום לפי סעיף 23מה לחוק הגנת הפרטיות, לפרקליט המדינה ולמשנה לפרקליט המדינה.

**סעיפים 10, 11 ו-13 עד 16** בהתאמה לשינוי המונחים המוצע בסעיף 1 להצעת החוק, מוצע לתקן את החוקים המפורטים להלן, ולהחליף בהם את המונח "הרשם" או "רשם מאגרי המידע" במונח "הממונה" או "הממונה על הגנת מידע":

1. חוק הרשויות המקומיות (בחירות), התשכ"ה–1965;
2. חוק הבחירות לכנסת [נוסח משולב], התשכ"ט–1969;

[14] ס"ח התשכ"ה, עמ' 248; התשס"ט, עמ' 94.
[15] ס"ח התשכ"ט, עמ' 103; התש"ע, עמ' 620.
[16] ס"ח התשס"ה, עמ' 918; התשע"א, עמ' 366.

(2) בסעיף 31ט1(ב)(1), במקום "רשם מאגרי המידע" יבוא "הממונה על הגנת מידע".

תיקון חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע

15. בחוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009[17] –

(1) בסעיף 2, במקום ההגדרה "רשם מאגרי המידע" יבוא:

""הממונה על הגנת מידע" – כהגדרתו בסעיף 7 לחוק הגנת הפרטיות;";

(2) בסעיף 20(ב), במקום "ולרשם מאגרי המידע" יבוא "ולממונה על הגנת מידע";

(3) בסעיף 33 –

(א) בסעיף קטן (א), במקום "לרשם מאגרי המידע" יבוא "לממונה על הגנת מידע";

(ב) בסעיף קטן (ה), במקום "ולרשם מאגרי המידע" יבוא "ולממונה על הגנת מידע".

תיקון חוק מרשם תורמי מוח עצם

16. בחוק מרשם תורמי מוח עצם, התשע"א–2011[18], בסעיף 10(ג), במקום "הרשם" יבוא "הממונה".

## דברי הסבר

3. חוק בתי משפט לעניינים מינהליים, התש"ס–2000;

4. חוק הפיקוח על שירותים פיננסיים (ייעוץ בייעוץ פנסיוני ובשיווק פנסיוני), התשס"ה–2005;

5. חוק הכללת אמצעי זיהוי ביומטריים ונתוני זיהוי ביומטריים במסמכי זיהוי ובמאגר מידע, התש"ע–2009;

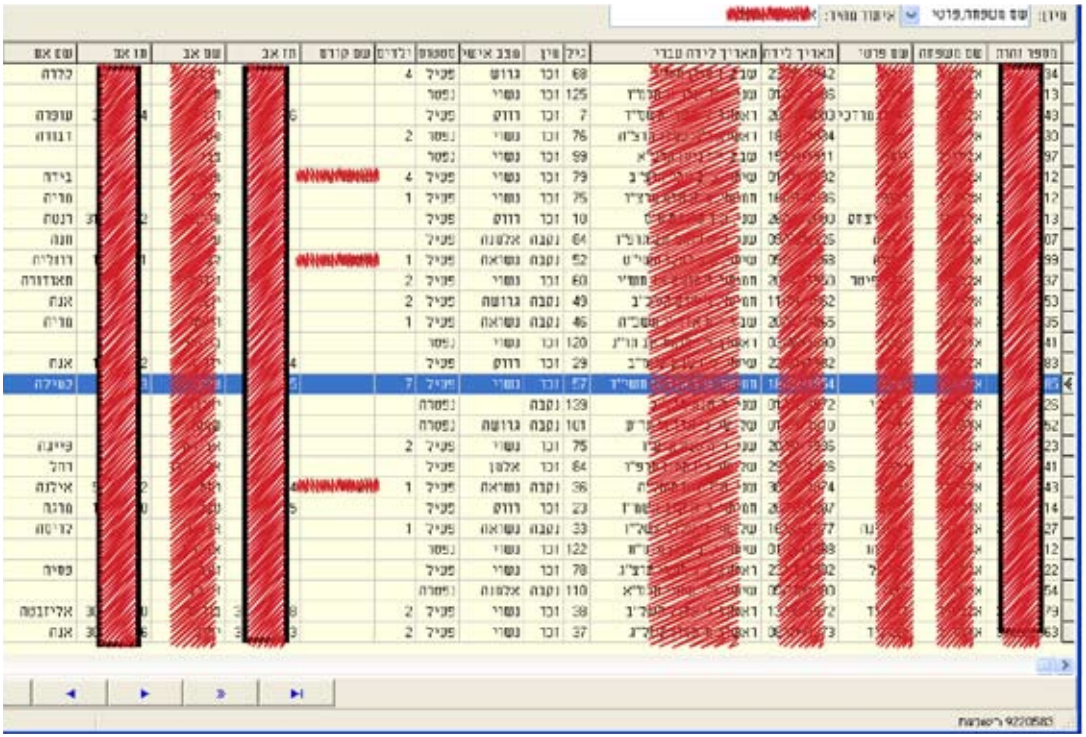
6. חוק מרשם תורמי מוח עצם, התשע"א–2011.

[17] ס"ח התש"ע, עמ' 256.

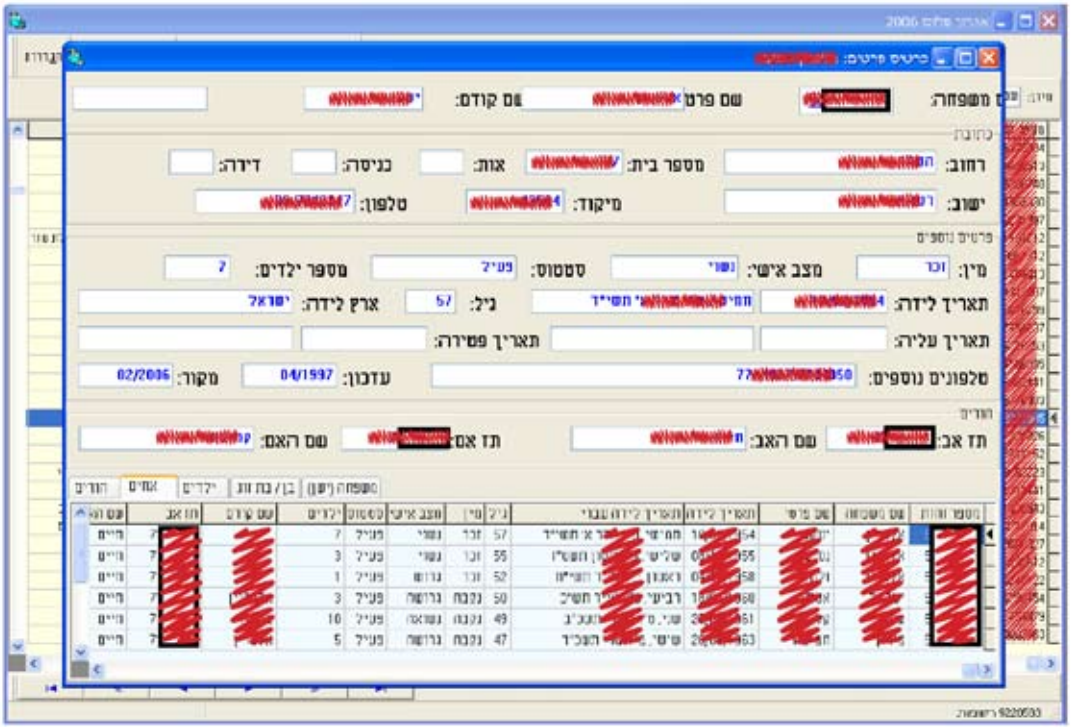
[18] ס"ח התשע"א, עמ' 382.

# נספח ב׳

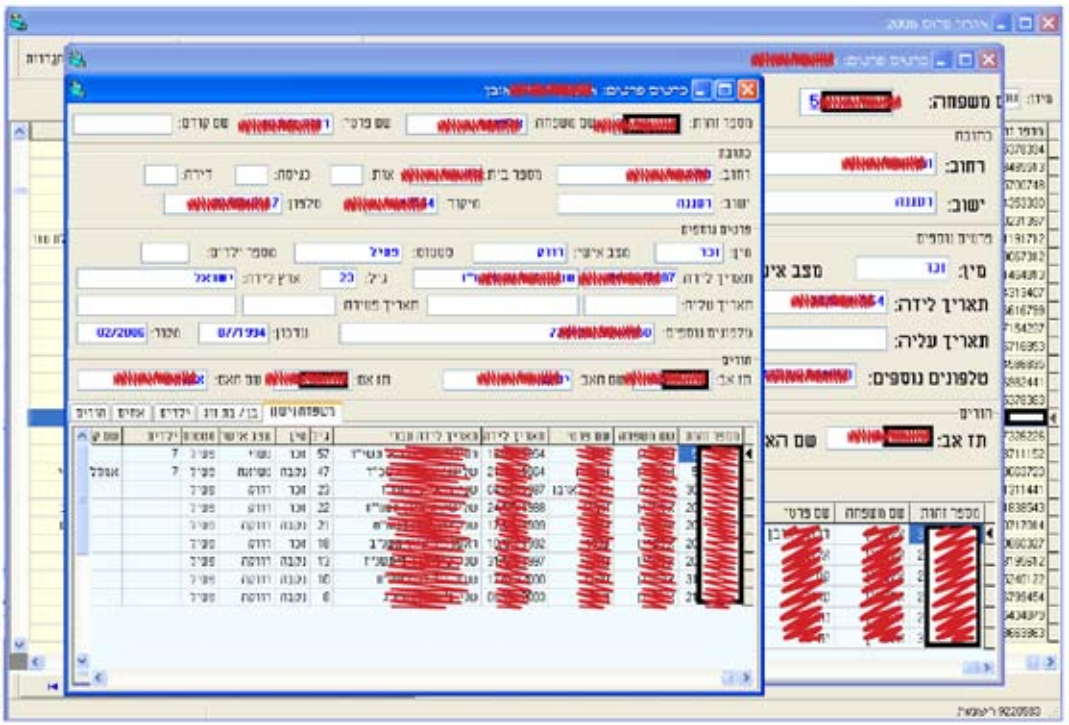
## מסכים של תוכנת אגרון



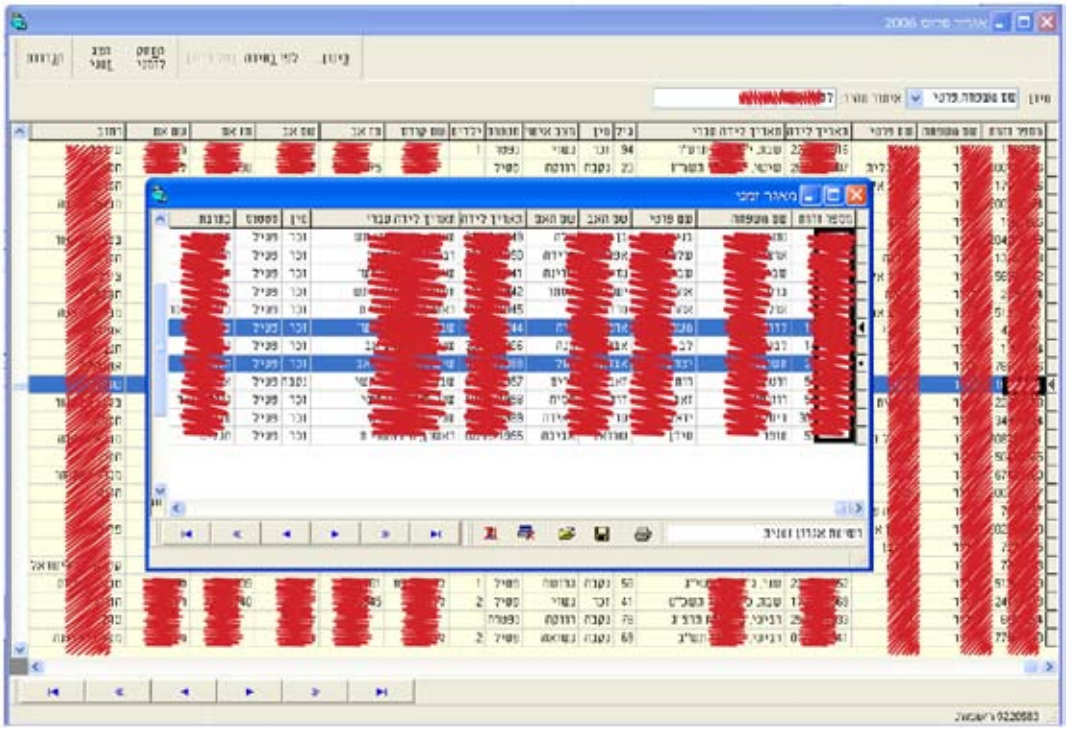
המסך הראשי של התוכנה – ניתן לעיין ולדפדף בפרטי 9.2 מליון האזרחים המתועדים במאגר ולצפות, לגבי כל אדם, במספר זהותו, שם משפחתו, שמו הפרטי, תאריך לידתו (הלועזי והעברי), גילו, מינו, מצבו האישי, מספר ילדיו, שמו הקודם, שמות הוריו ומספרי זהותם.



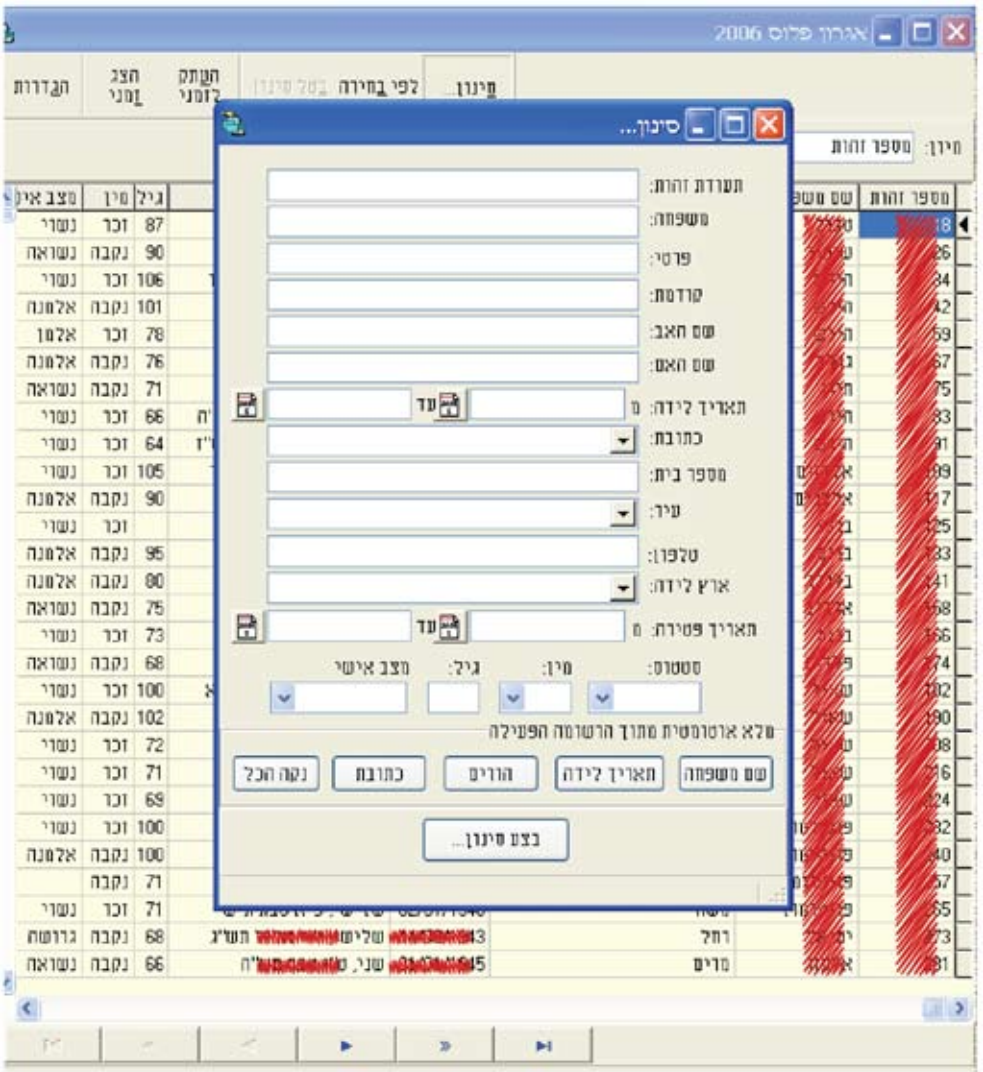
לגבי כל אדם המתועד ב"אגרון" ניתן לפתוח מסך מידע אישי המפרט את פרטי המידע הבאים: מספר זהותו, שם משפחתו, שמו הפרטי, שמו הקודם, כתובתו המדוייקת, מיקוד, טלפון ראשי וטלפונים נוספים, מינו, מצבו האישי, מספר ילדיו, תאריך לידתו (עברי ולועזי) וגילו, ארץ לידתו, תאריך עלייתו לישראל (אם עלה), תאריך פטירתו (אם נפטר), תאריך עדכון פרטיו במרשם, שמות הוריו ומספרי זהותם ואת הפרטים המנויים בדוגמה הקודמת לילדיו, הוריו, אחיו ואחיותיו.



ניתן לנווט מכל קרוב משפחה של אדם (בן זוג, ילד, אח, הורה) אל אותם פרטים על אודות קרוב המשפחה בהקשה כפולה (Double-Click) על הרשומה שלו.



ניתן ללקט פרטי אישיים של אישים שונים ל"מאגר זמני" ללא מגבלה.




זהו מסך איתור המידע העיקרי של "אגרון" המאפשר לחתוך מתוך בסיס הנתונים רשומות לפי הפרמטרים המפורטים לעיל (וכל שילוב שלהם), כגון: "כל הנערות בנות הגילאים 15–11 הגרות ברחוב מסוים בעיר מסוימת" או "כל הדיירים בכתובת מסויימת" או "כל מי שנולד בארץ מסוימת, והוא בגיל 50–40 והוא נשוי" וכד'.

# נספח ג'

## הנחית 2/2011 של רשם מאגרי מידע - שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

# הנחית רשם מאגרי מידע מס' 2/2011

# שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי

## 1. מטרה

1.1. העזרות בשירותי מיקור חוץ (outsourcing) מהווה מרכיב משמעותי בפעילותם של ארגונים במשק מודרני. במקרים רבים, שירותי מיקור החוץ כרוכים בניהול מידע אישי המעובד בארגון באופן ממוחשב.

1.2. מטרת הנחיה זו היא להבהיר את עמדתו של רשם מאגרי המידע בדבר הפעולות הראויות לקיום חובותיהם של בעל מאגר המידע, מנהל מאגר המידע והמחזיק בו לגבי עיבוד מידע אישי אגב מיקור חוץ מכוח הוראות חוק הגנת הפרטיות, התשמ"א–1981 (להלן – **החוק**) והתקנות לפיו[4].

1.3. יובהר, כי נוסף על הנחיה זו, בעת שימוש בשירות מיקור החוץ הכולל גם העברת מידע אישי אל מחוץ לגבולות ישראל, יש לוודא קיום הוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א–2001[5].

## 2. רקע

2.1. השימוש בשירותי מיקור חוץ משמעו הוצאה מחוץ לארגון, או ביצוע על ידי מי שאינם עובדי ארגון, של פעולות ותהליכים המבוצעים בדרך כלל על ידי הארגון, במטרה לקדם יעילות, להוזיל עלויות ולהתמקד בליבת העיסוק של הארגון.

4 במחלקת יעוץ וחקיקה במשרד המשפטים נמצאת בשלבים מתקדמים הכנה של הנחיית יועץ משפטי לממשלה בנושא מיקור חוץ בידי גופים ציבורים. ככל שיידרש, הנחייה זו תתוקן לאחר פרסום הנחיית היועץ.

5 בכוונת הרשם לפרסם הנחיה אשר תעסוק בנושא השימוש בשירותי "מחשוב ענן" (cloud computing), שתהיה משלימה 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

2.2. כתוצאה מכך נדרשת הסדרה משפטית וארגונית כדי להבטיח מימוש יעדי הארגון בביצוע השירות, שלא באמצעות עובדיו. במסגרת זו נדרשת מניעת הסיכונים הנובעים מכך שהשירות מבוצע במיקור חוץ.[6]

2.3. חוק הגנת הפרטיות ובפרט העקרונות הקבועים בפרק ב' בו, מסדיר את השימוש החוקי במידע אודות אדם כהגדרתו בחוק וקובע את מסגרות ההגנה כנגד שימוש לרעה באותו מידע. על מנת להשיג תכלית זו, מטיל פרק ב' בחוק אחריות למניעת שימוש לרעה במידע, דליפה או גניבה של המידע על מי שאוסף ומעבד מידע עבור עצמו ועל מי שמספק לו שירותים.

2.4. בשירותי מיקור חוץ יש חשיבות רבה לרמת רגישות המידע המוצא למיקור חוץ. בחינת רמת הרגישות של המידע נגזרת הן מפרמטרים כמותיים (כגון מספר נושאי המידע, היקף המידע, מספר בעלי הרשאת הגישה למידע), והן מפרמטרים מהותיים (כגון סוג המידע).

2.5. בעת השימוש בשירותי מיקור חוץ החובות והאחריות המוטלים מכוח החוק על בעל מאגר מידע, מנהל מאגר מידע והמחזיק בו ממשיכים לחול על כל אחד מהם כאילו הוא מבצע את הפעילות בעצמו, כולל, בין היתר, עקרון "הגבלת המטרה" לפי הוראות פרקים ב' ו–ד' לחוק הגנת הפרטיות, ובמיוחד בסעיפים 2(9) ו– 8(ב) לחוק, חובת אבטחת המידע והבטחת מימוש זכויות נושא המידע.

## 3. הנחיה

3.1. לאור האמור לעיל, עמדת רשם מאגרי המידע בדבר הפעולות הראויות לקיום חובותיהם של בעל מאגר המידע, מנהל מאגר המידע והמחזיק בו לגבי עיבוד מידע אישי אגב מיקור חוץ מכוח הוראות החוק והתקנות שמכוחו הינה כדלקמן:

3.1.1. <u>הוצאת פעילות למיקור חוץ – בדיקה מקדמית, היקף ומודל אספקת שירות</u>

6 בגוף ציבורי נדרשת בחינה של עצם ההחלטה על שימוש במיקור חוץ, בשים לב למספר היבטים ייחודיים לגופים אלה: הדינים החלים על הגוף הציבורי, היקף המידע המוחזק על ידו והיות איסוף המידע מכוח סמכות חוקית לעומת על בסיס הסכמה של האזרח נושא המידע.

3.1.1.1. על ארגון המבקש להוציא פעילות למיקור חוץ (להלן – **המזמין**) לבחון **האם הוא רשאי להוציא את המידע שהוא מבקש לעבד במיקור חוץ אל מחוץ לשליטתו בתהליך של מיקור חוץ**, שכן עשויות להיות מגבלות חוקיות או אתיות, אשר מונעות העברה כאמור. אף אם אין מגבלה פורמלית כאמור, מומלץ לקיים הליך בחינה האם ראוי, לאור אופי המידע האישי שהשירות יתבקש לגביו ורגישותו, להעביר את המידע או את העיבוד שלו למיקור חוץ.

3.1.1.2. על המזמין **להגדיר בפירוט מהו סוג השירות המבוקש על ידו, וכפועל יוצא מכך – מהו היקף המידע האישי הנדרש לצורך אספקת השירות על ידי נותן שירות מיקור החוץ (להלן – הקבלן)**. הגדרה זאת ראוי שתיכלל במסגרת אפיון כולל של השירות המבוקש המוצג בשלב ההזמנה להציע הצעות או כנספח למכרז או לחוזה. לעניין זה קיימים שלושה מודלים:

3.1.1.2.1. שירות המחייב טיפול במידע אישי החל משלב איסוף המידע מנושאי המידע בשם המזמין ועיבוד המידע על ידי הקבלן, לרבות ההקמה מאגר המידע;

3.1.1.2.2. שירות המחייב העברה או העתקה של מאגר מידע שלם, או חלק מהותי ממנו, מהמזמין לקבלן;

3.1.1.2.3. שירות המחייב טיפול במידע אישי בדרך של מתן הרשאות גישה או עדכון למידע במאגר המידע אצל המזמין, בהיקף הנדרש לצורך מתן שירות ספציפי, ללא העברת מאגר המידע במלואו.

**כנקודת מוצא יש להעדיף את חלופה 3.1.1.2.3 לעיל**, שכן העברת עותק שלם של מאגר מידע לקבלן או מתן גישה בלתי–מוגבלת למערכות המזמין, מציבים סיכון ממשי של העברת מידע עודף, שאינו דרוש במישרין למילוי תפקידו החוזי של הקבלן. בנוסף, בחלופות 3.1.1.2.1 ו–3.1.1.2.2 מאבד המזמין את יכולת השליטה בשימוש במאגר המידע. למעלה מכך, הניסיון מלמד כי הרשאות גישה נדיבות מדי מזמנות סיכוני אבטחת מידע שניתן להימנע מהם. **בחירה בחלופה 3.1.1.2.3 לעיל, יחד עם שימוש באמצעים אשר יבטיחו הגבלה של מתן הרשאות גישה למידע ובקרה על שימושים חריגים בהרשאות, יצמצמו במידה ניכרת את הסיכונים הנובעים מעיבוד מידע. כתוצאה מכך ניתן יהיה להקל בדרישות הקשורות בהסדרת נושא**

**זה במסגרת התפעול והפיקוח השוטפים**. ככל שנבחרת חלופה אחרת, יש לתעד את ההצדקה לבחירה בחלופה זו נוכח הנאמר לעיל.

3.1.2. <u>בחירת הקבלן</u>

**3.1.2.1. בבחירת הקבלן המבצע את מיקור החוץ על המזמין לבחון את ההיבטים הבאים:**

3.1.2.1.1. ניסיון קודם של הקבלן בעיבוד מידע אישי;

3.1.2.1.2. רקע ומוניטין של הקבלן;

3.1.2.1.3. קיום חשש לניגוד עניינים מובנה או סיכון אחר לשימוש פסול במידע על ידי הקבלן או מי מטעמו.

3.1.2.2. ככל שהמידע המועבר לקבלן הוא רגיש יותר, כך יש לנקוט במשנה זהירות בבחירת הקבלן.

3.1.3. <u>ניסוח חוזה ההתקשרות</u>

**3.1.3.1. צמידות מטרה** – על המזמין **להגדיר מפורשות את המטרות המותרות לשימוש ואת סוג בעלי התפקידים המועסקים על ידי הקבלן שיהיו מורשים בגישה אל המידע, וזאת על מנת להקפיד שהקבלן** ישתמש במידע אך ורק לשם ביצוע המטרה המקורית של הפעילות שביצועה הועבר אליו. יש לוודא שהחוזה מנוסח בבהירות הן בהגדרת המטרה והן בדרכים למימוש מטרה זו. יש לדרוש כי הקבלן ידריך את עובדיו במטרות השימוש במידע, ויוכיח את קיום ההדרכות למזמין.

**3.1.3.2. במקרה בו הקבלן אוסף מידע ישירות מנושא המידע, על המזמין לוודא כי הקבלן יקיים ויקפיד הקפדה יתירה על קיום חובת ההודעה הקבועה בסעיף 11 לחוק.** נוסח ההודעה ואופן קיומה צריכים להיקבע על ידי המזמין, או להיות מאושרים על ידו.

**3.1.3.3. על המזמין לאסור במפורש על הקבלן לאסוף מידע בדרכים בלתי-חוקיות, או לעשות שימוש במאגרי מידע בלתי-חוקיים.**

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

**3.1.3.4. על חוזה ההתקשרות עם הקבלן להכיל בטוחות, לרבות חיוב עריכת ביטוח אחריות מקצועית, סעדים וכלי בקרה אפקטיביים שיאפשרו תגובה מהירה ויעילה של המזמין להפרות של הוראות החוק והחוזה.** יצוין, כי ככל שהגדרת מטרות השימוש המותרות במידע ודרישות אבטחת המידע ברורות (כמפורט להלן), כך יקל להפעיל סעדים אפקטיביים.

3.1.3.5. במקרים המתאימים, על המזמין לדרוש **ייחוד עיסוק של הקבלן, הפרדה תאגידית בין הקבלן לגופים אחרים העוסקים במידע או הפרדה מבנית בתוך התאגיד הקבלן**, על מנת לצמצם ככל הניתן סיכון לשימוש במידע ממאגר המידע של המזמין לצרכים אחרים של הקבלן או לקוחותיו.

3.1.4. <u>אבטחת מידע ובקרה על פעילות במיקור חוץ</u>

3.1.4.1. קיום חובת אבטחת המידע חייבת להיות תנאי יסודי בכל התקשרות לצורך ביצוע שירות מיקור חוץ.

**3.1.4.2. במסגרת אפיון השירות, עוד בטרם התקשרות, על המזמין לבחון ולהגדיר את האיומים והסיכונים הנובעים מסוג המידע המועבר לקבלן, ולקבוע את אמצעי אבטחת המידע להתמודדות עימם.** ככל שרמת רגישות המידע גבוהה יותר והנזק הצפוי להיגרם לנושא המידע עם חשיפתו יהיה גדול יותר, יש ליישם אמצעי אבטחת מידע יותר קפדניים.

**3.1.4.3. בהתאם לכך על המזמין להגדיר מסמך אבטחה מחייב**, שיתייחס לכל הנושאים המפורטים ב<u>**נספח א'**</u> להנחיה זו. **מסמך זה יהיה חלק בלתי נפרד מתנאי ההתקשרות עם הקבלן, ובמקרים המתאימים אף יהיה תנאי סף להתקשרות.** לעניין זה ניתן להיעזר בת"י ISO 27001 וכן בנייר העמדה שפרסמה רמו"ט בנושא אבטחת מידע

לצורך הגנת הפרטיות[7]. **בעיבוד מידע בעל רגישות גבוהה יותר, מוצע לדרוש מהקבלן עמידה בתקן האמור** או בתקן חלופי הולם.

**3.1.4.4. על המזמין לוודא הסדרה ברורה של מימוש חובת הסודיות המפורטת בסעיף 16 לחוק לגבי מורשי הגישה למידע מטעמו של הקבלן.**

**3.1.4.5. על המזמין לאסור על הקבלן להעביר לצד שלישי כלשהו מידע שקיבל במסגרת ההתקשרות, או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה ישירות לביצוע ההתקשרות.**

**3.1.4.6. יש לוודא, כי קבלן המספק שירותים למספר רב של מזמינים, מקיים את חובותיו מכוח סעיף 17א לחוק.** לעניין זה, חובה לוודא קיום הדרישה בחוק כי הקבלן יפריד את הפעילות המתבצעת עבור המזמין מפעילויות עיבוד אחרות המבוצעות על ידו.

3.1.4.7. מומלץ, כי בכל שירות מיקור חוץ ימונה ממונה אבטחת מידע כאמור בסעיף 17ב לחוק, הן אצל הקבלן והן אצל המזמין. בהתאם לקבוע בחוק, אם הקבלן משמש מחזיק עבור יותר מחמישה מזמינים, חובה עליו לקיים זאת.

3.1.4.8. על המזמין לבצע מעקב ובקרה שוטפים על קיום הוראות החוק והוראות החוזה בידי הקבלן. ככל הניתן, יש ליישם אמצעים טכנולוגיים מקובלים, כגון מערכות ניטור ובקרה, כדי לאפשר פיקוח על פעילות הקבלן ועובדיו.

3.1.4.9. על המזמין לדרוש מהקבלן דיווחים שוטפים בכל הנוגע לאופן ניהול מאגר המידע ועיבוד המידע. כמו כן, על המזמין לדרוש לקבל דיווח מידי בכל מקרה של חשש לדליפת מידע מהמאגר או שימוש החורג מההרשאה שניתנה.

---

7 http://www.justice.gov.il/NR/rdonlyres/8D081CC2-225B-4269-95F7-BF6860654DA4/18194/tyutat_takanot_avtachat_meida_100112.pdf
במסגרת נייר העמדה יש הסדר מוצע לעניין היבטי אבטחת המידע במיקור חוץ לפיו, מסמך האבטחה, שמומלץ שיהיה חלק נפרד מחוזה ההתקשרות, יכלול הוראות לעניין נהלי סיווג והרשאה של עובדי הקבלן ומערכותיו, כללי הפרדת מערכות בין המערכות המקבלות גישה למידע, לבין מערכות אחרות בשימושו של הקבלן במהלך עסקיו, הוראות לעניין אבטחה פיזית ולוגית של המידע, הוראות לעניין מדיניות השבתה של מדיה מגנטית לרבות כוננים קשיחים וחתימה על הסכמי שמירת סודיות ע"י עובדי הקבלן.

3.1.4.10. על המזמין לשמור לעצמו את זכויות הפיקוח הדרושות, בהתאם לרגישות המידע וטיב פעילותו של הקבלן, לערוך ביקורות באתר הקבלן, במיוחד כשעולות תלונות נגד הקבלן או לקראת סיום ההתקשרות עמו. על המזמין לוודא כי לקבלן ברורות גם חובותיו כלפי הרשם, לרבות סמכויות הפיקוח של הרשם אצל הקבלן בהקשר של פעילות מיקור החוץ שלו עבור המזמין.

3.1.4.11. במקרים המתאימים, ובהתאם לרגישות המידע, יש לוודא כי ממונה אבטחת המידע מטעם המזמין יוסמך לבצע ביקורת, לרבות ביקורת פתע, על אופן התנהלות הקבלן בסוגיות של השימוש במידע ואבטחתו. לשם הקלה על הפיקוח, מומלץ לקבל מהקבלן הסכמה מראש כי נציגים מוסמכים של הגוף המזמין יוכלו לחדור לחומר המחשב שבשליטתו או באחזקתו, ככל הנדרש לצורכי פיקוח ובקרה על פעולותיו. אפשרות אחרת היא להסתמך על ביצוע ביקורות מסוג זה בידי צד שלישי בלתי תלוי המקובל על הקבלן והמזמין כאחד.

3.1.5. זכויות נושא המידע – **על המזמין לקבוע מראש הוראות ונהלים ביחס למימוש זכויות העיון והתיקון על ידי נושא המידע, כולל התייחסות לעניין זמני תגובה, עלויות**, והכל בשים לב לסעיפים 13 ו–14 לחוק ותקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ"א–1981.

3.1.6. הפעלה שוטפת של שירות מיקור החוץ

3.1.6.1. על המזמין לקבוע מנגנוני הטמעה והדרכה של הוראות החוזה אצל עובדי הקבלן, על מנת לוודא שעקרונות הגנת המידע האישי יופנמו בכל רובדי ארגונו של הקבלן הרלבנטיים לביצוע השירות.

3.1.6.2. יש לקבוע איש קשר מטעם הקבלן, אשר יעמוד בקשר עם מקביל לו מטעם המזמין. אנשי הקשר יתאמו ביניהם את כל הטעון בירור בקשר להדרכה והטמעה של השירות, תוך הסבר מפורש על אודות השימוש המותר במידע.

3.1.7. משך שמירת המידע, ביעור המידע

3.1.7.1. יש להתיר לקבלן לשמור מידע שהתקבל מהמזמין, או מידע שהקבלן צבר בעצמו אגב מתן השירות, רק למשך פרק הזמן הנדרש במישרין לביצוע תפקידו לפי החוזה.

3.1.7.2. עם סיום ההתקשרות עם הקבלן, על המזמין לוודא כי כל המידע שהגיע לקבלן במסגרת שירות מיקור החוץ נמחק מכל אמצעי המדיה שברשותו, לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחרת. ככל שקיימת הוראה בדין המחייבת שמירת המידע אצל הקבלן, יש לוודא כי אמצעי האבטחה והבקרה שהוגדרו בחוזה עם המזמין יישארו אפקטיביים לכל אורך תקופת השמירה.

3.1.7.3. ככל שנדרשת על ידי הקבלן זכות גישה למידע לאחר סיום ההתקשרות לצורך התגוננות בפני תביעות בקשר עם תפקידיו לפי החוזה, ניתן לשמור עותק של המידע באמצעי גיבוי מקובל אצל צד ג' נאמן אשר יהיה רשאי להתיר את הגישה למידע רק למטרות הנ"ל.

3.1.7.4. על המזמין לדרוש מן הקבלן תצהיר המאמת ביצוע פעולות מחיקה, ביעור והשמדה של כל המידע שהגיע אליו במסגרת ההתקשרות עמו.

3.1.8. תיעוד – מומלץ כי לתהליך קבלת ההחלטות לגבי כל האמור לעיל ייערך תיעוד מסודר על מנת לאפשר לרשם או לצדדים שלישים אחרים לבחון את האופן בו מתבצע מיקור החוץ.

3.2. כלי עזר ליישום האמור בהנחיה זו מצוי ב**נספח ב'**.

3.3. הנחיה זו אינה גורעת מהוראות חוק הגנת הפרטיות והתקנות שמכוחו, או מכוחם של חיקוקים, הוראות והנחיות רגולטורים אחרים. לעניין גופים הנתונים לפיקוח של המפקח על הבנקים בבנק ישראל או של הממונה על שוק ההון במשרד האוצר, ראו **נספח ג'**.

3.4. הנחיה זו תיכנס לתוקף ביום 19/5/12. לאחר מועד זה יפעיל רשם מאגרי מידע את מכלול הסמכויות הקבועות לו בדין על פי העמדה המפורטת בהנחיה 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

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

## נספח א' – נושאים להתייחסות במסמך האבטחה של מזמין שירות מיקור חוץ

1. אבטחה פיסית – קיום הגנה פיסית על מערכת המידע ועל התשתית שלה לרבות מבנה, אמצעי תקשורת, מסופים ותשתית חשמלית, מפני סיכונים סביבתיים ופגיעות התואמים את רגישות המידע שיעובד;
2. אבטחה לוגית – נקיטת אמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין המזמין לקבלן;
3. הפרדת מאגרי מידע – כללי הפרדת מערכות בין המערכות המקבלות גישה למידע, לבין מערכות אחרות בשימושו של הקבלן במהלך עסקיו;
4. מדיניות הוצאה משירות של מדיה מגנטית ואופטית לרבות כוננים קשיחים, אמצעי אחסון ניידים או נתיקים, מצעי גיבוי וכד';
5. נהלים – קביעת סדרי ניהול של מאגר מידע, סיווג והרשאות גישה למידע, והוראות לאיסוף, לסימון, לאימות, לעיבוד ולהפצה של המידע, בהתאם להוראות החוק והתקנות שמכוחו;
6. ניהול הרשאות:
   1.1. קביעת אופן מתן הרשאת גישה למאגר המידע והטלת הגבלות על מורשי הגישה;
   1.2. עריכת רישום מעודכן של מורשי הגישה למאגר המידע לפי הרשאות הכניסה השונות.
7. תפעול – קיום הוראות תפעול של המערכת תוך אבטחת המידע ושמירה על שלמות המידע;
8. סודיות – החתמת מורשי הגישה על התחייבות לשמירה על סודיות ועל ההוראות שנקבעו לפי הנהלים ומסמך האבטחה;
9. בקרה – קביעת סדרי בקרה לגילוי פגיעות בשלימות המידע ותיקון ליקויים.
10. קבלת עובדים – קביעת תנאים לגבי אמינות עובדים ועבר של עבירות הקשורות בשימוש במידע בהתאם לרגישות המידע.

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

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

## נספח ב' – רשימת בדיקה לקיום הוראות ההנחיה בהתקשרות לשירותי מיקור חוץ

| נושא | סעיף בהנחיה | תוכן הבדיקה | הערות |
|---|---|---|---|
| בדיקה ראשונית | 3.1.1.1 | האם רשאי וראוי להוציא את הפעילות למיקור חוץ | |
| | 3.1.1.2 | הגדרת סוג השירות והיקף המידע הנדרשים במסגרת ההתקשרות ובחירת החלופה המועדפת לאספקת השירות | |
| בחירת קבלן | 3.1.2 | בחירת הקבלן על פי עמידה בפרמטרים שונים | |
| תנאי התקשרות | 3.1.3.1 | הגדרה ברורה של מטרות שימוש מותרות על ידי הקבלן ומורשי גישה למידע מטעם הקבלן | |
| | 3.1.3.2 | וידוא של קיום חובת ההודעה מצד הקבלן לפי סעיף 11 לחוק | |
| | 3.1.3.3 | קביעת איסור על הקבלן לאיסוף או שימוש במידע לא חוקי | |
| | 3.1.3.4 | קביעת בטוחות, סעדים וכלי בקרה אפקטיביים שישמשו את המזמין בעת הפרת החוק או החוזה על ידי הקבלן | |
| | 3.1.3.5 | דרישת ייחוד עיסוק של הקבלן ו/או הפרדה תאגידית/ מבנית אצל הקבלן, במקרים המתאימים | |

| נושא | סעיף בהנחיה | תוכן הבדיקה | הערות |
|---|---|---|---|
| אבטחת מידע ובקרה | 3.1.4.1 | קביעת חובת אבטחת המידע כתנאי יסוד להתקשרות | |
| | 3.1.4.2 | הגדרת האיומים והסיכונים הנובעים מסוג המידע המועבר לקבלן, ואמצעי אבטחת המידע להתמודדות עימם | |
| | 3.1.4.3 | הגדרת מסמך אבטחה מחייב, כחלק בלתי נפרד וכתנאי סף בהתקשרות עם הקבלן | בעיבוד מידע ברמת רגישות גבוהה, יש לחייב את הקבלן לעמוד בת"י ISO27001 |
| | 3.1.4.4 | וידוא הסדרה ברורה של מימוש חובת הסודיות על ידי מורשי גישה מטעם הקבלן | |
| | 3.1.4.5 | קביעת איסור על הקבלן להעביר מידע שקיבל בהתקשרות לצד ג' או להשתמש במידע למטרה שלא קשורה בביצוע ההתקשרות | |
| | 3.1.4.6 | וידוא קיום חובות קבלן המספק שירותים למספר מזמינים רב מכוח סעיף 17א לחוק | במיוחד, יש לוודא כי הקבלן מפריד בין הפעילות עבור המזמין לבין פעילות עבור מזמינים אחרים או עבור עצמו |
| | 3.1.4.7 | בחינת אפשרות מינוי ממונה אבטחת מידע הן אצל הקבלן והן אצל המזמין | אצל קבלן המספק שירותים לחמישה מזמינים ומעלה זוהי חובה, לפי סעיף 17ב לחוק |
| | 3.1.4.8 | ביצוע מעקב ובקרה שוטפים אחר פעילות הקבלן לפי החוק והחוזה | רצוי לעשות שימוש גם באמצעים טכנולוגיים |
| | 3.1.4.9 | דרישת דיווחים שוטפים מהקבלן על ניהול מאגר המידע ועיבוד המידע, ודרישת דיווח מידי במקרה של חשש לדליפת מידע | |
| | 3.1.4.10 | שמירה על זכויות המזמין לבצע ביקורת באתר הקבלן ולפקח על פעילות, כולל סמכויות הפיקוח של הרשם | |
| | 3.1.4.11 | הסדרה מראש של אפשרות ממונה אבטחת המידע או צד ג' מטעם המזמין לבצע ביקורת פתע אצל הקבלן, כולל הסכמה מראש של הקבלן לחדירה על ידו לחומר מחשב | במקרים המתאימים, בהתאם לרמת רגישות המידע |

| נושא | סעיף בהנחיה | תוכן הבדיקה | הערות |
|---|---|---|---|
| זכויות נושא המידע | 3.1.5 | קביעה מראש של הוראות ונהלים ביחס למימוש זכויות העיון והתיקון שיוגדרו בהתאם לרמת הזיקה של הקבלן למידע | כולל התייחסות לזמני תגובה, עלויות |
| הפעלה שוטפת | 3.1.6.1 | קביעת מנגנוני הטמעה והדרכה של הוראות החוזה אצל עובדי הקבלן | |
| | 3.1.6.2 | קביעת איש קשר מטעם הקבלן ומקביל לו מטעם המזמין לתיאום הפעילות על פי החוזה | |
| משך שמירת המידע וביעורו | 3.1.7.1 | קביעת פרק הזמן המותר לקבלן לשמור את המידע | יש להגביל את פרק הזמן לתקופה הנדרשת לביצוע ההתקשרות בלבד |
| | 3.1.7.2 | וידוא מחיקת כל המידע אצל הקבלן, על כל אמצעי מדיה שברשותו | ככל שיש הוראה אחרת בדין, יש לוודא המשך קיום אמצעים האבטחה והבקרה שבחוזה |
| | 3.1.7.3 | העברת עותק של המידע לנאמן צד ג' לצורך התגוננות עתידית מתביעות | במידת הצורך |
| | 3.1.7.4 | קבלת תצהיר מהקבלן על ביצוע פעולות מחיקת, ביעור והשמדת כל המידע | |
| תיעוד | 3.1.8 | עריכת תיעוד מסודר של קבלת ההחלטות ביחס לביצוע מיקור חוץ שניתן יהיה להציג לרשם ולצדדים שלישיים | |

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

## נספח ג' – תחולת ההנחיה על גופים הנתונים לפיקוח של המפקח על הבנקים או של הממונה על שוק ההון

1. מטרת נספח זה היא לקבוע את אופן התחולה של ההנחיה בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי (להלן – **ההנחיה**), על רקע האמור בסעיפים 1 ו–2 להנחיה, לגבי גורמים המפוקחים על ידי המפקח על הבנקים בבנק ישראל (להלן – **המפקח על הבנקים**) ועל ידי הממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר (להלן – **הממונה על שוק ההון**) (להלן ביחד – **הגורמים**).

2. לפי ידיעת הרשם, על הגורמים חלות ההוראות הבאות (להלן ביחד – **ההוראות**):

2.1. על המפוקחים על ידי המפקח על הבנקים חלה הוראת ניהול בנקאי תקין מספר 357;

2.2. על גופים המפוקחים על ידי הממונה על שוק ההון חלים חוזר גופים מוסדיים 2006–9–6, הוראה לניהול סיכוני אבטחת מידע של הגופים המוסדיים וחוזר גופים מוסדיים 2010–9–4, ניהול טכנולוגיות מידע בגופים מוסדיים.

3. בהתאם לכך, יראה הרשם את דרישות המינימום המפורטות בהנחיה כמתקיימות לעניין הגורמים בתנאי שבידיהם הוכחות שהם עומדים בהוראות החלות עליהם, ביישום השינויים והתוספות המפורטים להלן:

3.1. על הגורמים לקיים את ההוראות באופן שהן חלות באופן מלא גם על מידע אישי.

3.2. על הגורמים לקיים את ההוראות, תוך יישום קונקרטי, במסגרת דרישות ההוראות, של הנושאים הספציפיים המממשים את עקרונות החוק המפורטים בסעיפים הבאים:

3.2.1. הוראות בעניין הגבלת מטרה, כמפורט בסעיף 3.1.3 להנחיה.

3.2.2. הוראות בעניין זכויות נושא המידע, כמפורט בסעיף 3.1.5 להנחיה.

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

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

3.2.3. הוראות בעניין משך שמירת המידע, כמפורט בסעיף 3.1.7 להנחיה.

3.3. על הגורמים להתייחס באופן מתועד, במסגרת הפעלת שיקול דעת בהתאם לעקרונות ההוראות, לעקרונות הקונקרטיים המפורטים מטה:

3.3.1. מודל שירות כפונקציה של הסיכון, כמפורט בסעיפים להנחיה.

3.3.2. בחינת העדר חשש לניגוד עניינים של הקבלן לעניין מידע אישי כמפורט בסעיפים 3.1.2.1.3 ו– 3.1.3.5 להנחיה.

4. במקרה של ספק או אי בהירות מוצע להתייעץ עם הרשם.

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

State of Israel Ministry of Justice
ILITA The Israeli Law, Information and Technology Authority

מדינת ישראל משרד המשפטים
רמו"ט הרשות למשפט, טכנולוגיה ומידע

## מידע לגבי ההנחיה

1. **מס' ההנחיה:** 2/2011
2. **נושא ההנחיה:** שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי
3. **תאריך פרסום:** 21/11/11
4. **בתוקף מתאריך:** 19/5/12
5. **חוקים שאוזכרו:**
   א. חוק הגנת הפרטיות, התשמ×א–1981.
   ב. תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס×א–2001.
   ג. תקנות הגנת הפרטיות (תנאים לעיון במידע וסדרי הדין בערעור על סירוב לבקשת עיון), התשמ×א–1981.
6. **פסקי דין שאוזכרו:** אין.
7. **מאמרים שאוזכרו:** אין.
8. **הנחיות היועץ המשפטי לממשלה שאוזכרו:** אין.
9. **הנחיות רשם מאגרי מידע שאוזכרו:** אין.
10. **מילות מפתח:** אבטחת מידע, בעל מאגר מידע, בקרה, דליפת מידע, הדרכה, הטמעה, המפקח על הבנקים, הפרדה תאגידית, הרשאות, מזמין, מחזיק מאגר מידע, מיקור חוץ, ממונה שוק ההון, ביטוח וחסכון, מנהל מאגר מידע, ניגוד עניינים, סעדים, ערבות, קבלן, Outsourcing.
11. **עדכונים**

| גרסה | פרטים | תאריך |
|---|---|---|
| 1.1 | תיקון טעות סופר בסעיפים 3.2.2 ו– 3.3.2 לנספח ג' | 07.06.12 |
| | | |
| | | |
| | | |

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

In the credit data field, one of the licenses to operate an information service about business was canceled at the request of the operator Lev Emun Entrepreneurs Ltd. ILITA urged the Bank of Israel to cease to have files containing the list of persons and bank accounts limited due to checks over drafting freely available online and in collaboration with the Bank of Israel formulated an arrangement in order to limit and regulate the distribution of these files.

ILITA managed in 2011 another criminal investigative file, which also concerns trade of personal data from illegal sources. This case was managed at its beginning as an administrative supervision case, for which administrative fines were imposed, but the defendant chose to be tried for the offenses made, and therefore the case became a criminal investigation proceeding case that was submitted for prosecution.

In 2011 ILITA continued publishing guidelines related to privacy protection, in order to clarify the law regarding specific issues. Guidelines were distributed on the following topics: the public transport smart card project; outsourcing of personal data processing; draft guideline in the context of privacy and protection of personal data in contracts of cell phone operators; draft guideline regarding the application of the provisions of the Protection of Privacy Law on HR screening services; prohibition of the use of data regarding the imposition of a lien by a third party; draft guideline regarding the use of surveillance cameras and their databases.

During 2011, the Databases Registrar approved Google's Street View service operation in Israel, after stipulating several terms related to the way the photographs are collected for this service, transparency and informing citizens about the photographs, jurisdiction of Israeli courts for violations of the law if occur, and how information is presented to the service users.

In the field of electronic signature, the registration of Personnel ID Ltd as a qualified certification authority for the issuance of electronic signature certifications in accordance with the Electronic Signature Law, 2001 was approved in 2011, after thorough examination by the Certification Authorities Registrar licensing team. During the year ILITA was submitted with an application to register Certification Authority under the "e-government" project of the Ministry of Finance, intended to allow certified electronic signature for every citizen in the smart ID card project. Also, two financial sanctions of 71,600 NIS were imposed on the Certificate Authority ComSign Ltd. for various violations of the law and the instructions by the Registrar.

In 2011 the actual application of Certification Authorities Registrar' Guideline no. 2-2010 had begun. This guideline governs the technological, administrative and security requirements of the certificate authority management system for electronic signature. In addition, the Certification Authorities Registrar approved, for the first time a hardware component, smart card of Athena ltd, as consistent with the requirements of the law to store secure electronic signature.

mechanisms to avoid double regulation, with parallel information-related regulators in Israel, such as the banks supervisor in the Bank of Israel and the Capital Markets department in the Ministry of Finance.

In the International arena, ILITA continued in 2011 to participate and influence the international debate on personal data protection. The final decision by the European Union and European Parliament stating that data protection framework in Israel is adequate according to article 25(6) of the European Directive 95/46/EC was published in January 2011, and is in force since May 2011. ILITA continued to represent Israel in ICCP (Information, Communication and Computers Policy) Committee of the OECD and its Working Party on Information Security and Privacy (WPISP). As founding member in the Global Privacy Enforcement Network (GPEN), ILITA continued to participate in GPEN activities. The twinning program with the Spanish Data Protection Agency AEPD ended at the beginning of the year.

In the area of personal data protection, ILITA continued the process of improving its supervision of data controllers. Common issues that arose in these operations were infringing purpose limitation, complying with the direct marketing chapter and with the data security obligations in the law. The report includes Database Registrar inspection cases in the public sector (Ministry of Defense, Enforcement and Collection Authority, the Ministry of Transportation (Licensing Authority), Securities Authority, the city of Ashkelon) and in the private and third sector, in different areas (internet, burial services, direct marketing, human resources services, medicine, insurance, private investigators, communications). In some of the cases that ended in 2011 administrative fines were imposed.

The main event of 2011 in ILITA's activities was cracking the Agron case, the theft and online dissemination of the full population registry of the State of Israel. Investigation of the case began in 2010, when ILITA's Investigations Department received its criminal investigative powers. After an intensive, complicated and complex investigation, evidence were achieved against six people, who joined for the theft of the full population registry of 9.2 million Israeli citizens (living and deceased), the trading of it, the development of software to use it and its dissemination online, as well as other crimes. The Agron case caused great damage, primarily to the privacy of Israeli citizens, but also to other values, and there is a significance importance to its cracking for the purposes for which ILITA was established.

# SUMMARY OF THE REPORT

This report reviews the activities of ILITA in 2011. During this year ILITA continued to be built, but have not yet reached the extent of personnel power and resources as planned. During the year ILITA started developing a dedicated information system to support its various regulatory activities.

Towards the end of the year, the Knesset approved first reading of the Protection of Privacy Law (Amendment No. 12) (Enforcement Powers), which is intended to modernize the data protection enforcement powers of ILITA, and to institute the Data Protection Commissioner in ILITA.

ILITA Continued to promote a complementary amendment to the Protection of Privacy Law, which will significantly reduce database registration duties and instate duties of proper management of personal data.

In its public policy roles, ILITA continued in 2011 to be involved and influence various law and technology matters, such as: the "right to oblivion" in publishing personal information in court cases (Engelhard Commission); the biometric database part of the smart ID card project; The pension information clearinghouse initiative aimed to improve pension consulting to the citizens of Israel; using electronic signature to sign medical prescriptions; advancing data security regulation to allow access to medical information by pharmacists in a reform to improve service for the chronically ill; privacy issues arising in establishing smart grid to charge electric vehicles; expert committee that examines reform that will tax vehicles according to actual use as part of environment and transportation policies; formulating national policies for the state Archivist regarding preservation of electronic records; publication of limited customers and accounts electronic information by the Bank of Israel.

During this year ILITA started to build collaborative regulation and to establish joint

recommendation to prosecute the suspects to the Tel Aviv District Attorney's Office. During May 2012 the suspects were charged with offenses against the Protection of Privacy Law, the Computers Law and the Penal Law. The damages caused by the Agron case to Israel and its citizens are numerous and severe, and the report lists them one by one.

Another enforcement leap forward in 2011 is the first reading by the Israeli Parliament, the Knesset, of the Protection of Privacy Law (Amendment No. 12) (Enforcement Powers). This bill, formulated by ILITA in cooperation with the Division of Counseling and Legislation in the Ministry of Justice, is expected to promote the enforcement capabilities of the norms set in the Protection of Privacy Act Law 1981 to the challenges of our time.

Considering the ever-limited resources, as head of ILITA I believe that private enforcement of the law by individuals, through civil law mechanisms such as class actions, is very important. These private enforcement means should not be limited to private sector controllers, and in appropriate cases should be applied to public sector bodies as controller or processor of personal data. Accordingly, ILITA will continue to be transparent to the public and publish investigation and inspection findings, as well as guidelines directing the public regarding its rights.

I would like to thank the dedicated and excellent employees of ILITA for their wonderful daily work throughout the year. The product of their efforts is specified in this report.



Yoram Hacohen

Head of ILITA

Administrative enforcement was the bread and butter of ILITA since its establishment. It is done by exercising the supervision powers and imposing sanctions according to the laws ILITA operates by - Protection of Privacy Law, Credit Data Services Law and Electronic Signature Law. Exercising those powers has been improved dramatically during the past years and data controllers are exposed to such actions by ILITA.

I believe that Criminal enforcement by a data protection authority is particularly important, and ILITA has been a world pioneer in this. The complexity of data protection related offences require in-depth knowledge of information technologies by the investigators, as well as of electronic evidence and privacy protection. The exceptional ease of violating personal data protection obliges effective enforcement that affects all players. It must ensure that controllers and processors internalize the negative outcomes that they may suffer from the violation, and should produce sufficient deterrence of offenders. It must also result in raising awareness of the general public in Israel to its rights under the Protection of Privacy Law.

Technological infrastructure of personal data processing is getting increasingly complex, as well as the economic and business models that drive them. It requires that the investigator have deep understanding of technology, information and economics. In addition to track the criminal activity by traditional tools of inquiry and questioning, modern privacy protection enforcement agency must gain complementary capabilities that will expose criminals hiding behind technological masks.

2011 stands out for ILITA's successful efforts in criminal enforcement of personal data protection, arising from building a specialized criminal investigations department according to the above mentioned concepts. Described in detail in this report is the story of "Agron Case" - the theft and online dissemination of Israel's full population registry, which containing broad, complete and sensitive information about the whole population of Israel.

ILITA's criminal investigation department cracked this crime and concluded the investigation after an intensive investigation that began in 2009 and passed a

# INTRODUCTORY REMARKS BY HEAD OF ILITA
## (THE ISRAELI LAW, INFORMATION AND TECHNOLOGY AUTHORITY)

2011 Annual Report on ILITA's activities focus on the importance of enforcement of personal data protection principles and the promotion of public policy, in view of significant events that took place this past year.

During 2011 ILITA used a variety of regulatory tools to achieve its goals as the regulator of personal data protection in Israel, among those are inspections and investigations to enforce the Privacy law; initiating legislative processes; promoting privacy related public policy; general public education; issuing and advertising guidelines; cooperation with fellow regulators in Israel; cooperation with data protection regulators and other stakeholders in the international arena.

Data protection laws regulate the use of individuals' personal data that is stored and processed in information systems in order to prevent misuse of such data both by persons who are duly authorized or have no permission to access the data. Data use is governed by the principle of purpose limitation, which restricts the use of data for purposes for which it was initially collected, as well as additional requirements imposed on data controllers and processors. Data protection laws grant additional rights to data subjects, particularly with respect to transparency of information collection, the nature of information stored, its accuracy and use in practice.

Enforcement – criminal, administrative - is an essential element in any regulatory toolkit of supervisory authority. The importance of privacy, which is a basic constitutional right in Israel, intensifies the significance of enforcement by ILITA of data protection rules. Moreover, regulatory enforcement of data protection laws is needed, as usually the damage can hardly be repaired and it is difficult (but not impossible) to quantify and compensate for it.







**THE ISRAELI LAW, INFORMATION AND TECHNOLOGY AUTHORITY (ILITA)**

**MINISTRY OF JUSTICE**

The Government Campus
125 Begin Rd., 9th floor
P.O.Box 7360
Tel Aviv 61072, Israel
Tel.: +972-3-7634094
Fax: +972-2-6467490
ilita@justice.gov.il
ilita.justice.gov.il/en

ISBN 978-965-92053-0-1

An electronic copy of this report is available at ilita.justice.gov.il



# THE ISRAELI **LAW, INFORMATION AND TECHNOLOGY** AUTHORITY (ILITA)

# 2011 REPORT

November 2011



**STATE OF ISRAEL**
MINISTRY OF JUSTICE



# THE ISRAELI **LAW, INFORMATION AND TECHNOLOGY** AUTHORITY (ILITA)

# 2011 REPORT



**STATE OF ISRAEL**
MINISTRY OF JUSTICE