משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

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

מדינת ישראל
State of Israel

תאריך: 20 יולי, 2009
כ"ח תמוז, תשס"ט
סימוכין: 015-99-2009-000789

לכב'
ועדת חוקה, חוק ומשפט
כנסת ישראל

לכב'
ועדת הכלכלה
כנסת ישראל

לכב'
ועדת המדע והטכנולוגיה
כנסת ישראל

לכב'
שר המשפטים פרופ יעקב נאמן
משרד המשפטים

נכבדיי,

הנדון: **<u>דין וחשבון על פעילות הרשות למשפט, טכנולוגיה ומידע בשנת 2008</u>**

1. הרשות למשפט, טכנולוגיה ומידע (להלן – **הרשות**) הוקמה מכח החלטת ממשלה 4660 מיום 29.1.2006 אשר החליטה על הקמת "רשות משפטית לטכנולוגיות מידע והגנה על הפרטיות" במשרד המשפטים. החלטת הממשלה הורתה על הכללתם של שלושה תפקידים על פי דין המסורים לנושאי תפקיד במשרד המשפטים במסגרת הפעילות של הרשות, ואלה הם:

   א. רשם מאגרי מידע הפועל מכוח חוק הגנת הפרטיות, התשמ"א-1981 (להלן בהתאמה – **רשם מאגרי מידע** ו**חוק הגנת הפרטיות**).

   ב. רשם גורמים מאשרים הפועל מכוח חוק חתימה אלקטרונית, התשס"א-2001 (להלן בהתאמה- **רשם גורמים מאשרים** ו**חוק חתימה אלקטרונית**).

   ג. רשם שירותי נתוני אשראי ומידע על עוסקים הפועל מכוח חוק שירות נתוני אשראי, התשס"ב-2002 (להלן בהתאמה– **רשם שירותי נתוני אשראי** ו**חוק נתוני אשראי**).

2. ב-1.9.2006 מוניתי לתפקיד והוטלה עלי המשימת להקים את הרשות. במסגרת זו, מינתה אותי הממשלה לקראת סוף שנת 2006 גם כרשם מאגרי מידע ושר המשפטים מינה אותי כרשם שירותי נתוני אשראי. את תפקיד רשם גורמים מאשרים ממלא עו"ד עמית אשכנזי, המשמש גם כראש המחלקה המשפטית של הרשות.

3. דין וחשבון זה מאגד, בפעם הראשונה בחיי הרשות, דיווח של שלושת הרשמים לכדי דו"ח מאוחד[1]. אף שלא קיימת לכך חובה בדין, הוסף על ידי הרשות ביוזמתה דו"ח אודות פעילות רשם שירותי נתוני אשראי באותם היבטים להם קבועה חובה לרשמים האחרים. ההגיון של מתן דו"ח מאוחד נובע מהיעד של הרשות לפעול כרשות הגנת מידע אישי המפעילה באופן מאוחד את מנגנוני הרגולציה של שלושת החוקים הנ"ל.

---

1. שניים מהחוקים המפורטים לעיל קובעים מסגרת של דין וחשבון שנתי לרשות המחוקקת:

   א. סעיף 10א לחוק הגנת הפרטיות קובע כי המועצה להגנת הפרטיות תעביר, לא יאוחר מאחד באפריל בכל שנה, דין וחשבון שיכין רשם מאגרי מידע אודות פעולות האכיפה והפיקוח שבוצעו אל ידו בשנה הקודמת להגשת הדו"ח. לדו"ח מצורפות הערות המועצה להגנת הפרטיות.

   ב. תקנה 16 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), תשס"ב–2001 קובעת כי רשם גורמים מאשרים יגיש לוועדה לענייני מחקר מדעי וטכנולוגי של הכנסת, לא יאוחר מ-1 באוקטובר של שנה, דין וחשבון על הפעלת סמכויותיו על פי התקנות.

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

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

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

4. הרשות תנקוט מהלך ייזום תיקון החוקים לצורך סנכרון מועד חובות הדיווח בין הרשמים השונים, וזאת כדי לאפשר הגשה של דו"ח מאוחד כאמור.

5. עיקרי מסמך זה מפרטים את פעילות הרשות בשנת 2008 בהפעלת הסמכויות הרגולטוריות המוקנות לרשמים השונים על פי דין. בנוסף, מתוארות פעילויות הקשורות בהגנת מידע אישי אשר נעשו במהלך השנה על ידי הרשות כמרכז הידע בנושא משפט וטכנולוגיה במשרד המשפטים.

בברכה,

יורם הכהן
ראש הרשות למשפט, טכנולוגיה ומידע

העתקים:
מר משה שילה- המנהל הכללי, משרד המשפטים;
מר מני מזוז- יועץ משפטי לממשלה, משרד המשפטים;
מר משה לדור- פרקליט המדינה, משרד המשפטים;
הגב' אורית קורן – המשנה ליועץ המשפטי לממשלה (חקיקה)
הגב' שרית דנה – המשנה ליועץ המשפטי לממשלה (אזרחי)

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

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

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

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

יולי 2009
תמוז, תשס״ט

תוכן עניינים

סטטוס הקמת הרשות	3
מבנה ארגוני	3
משימות עיקריות במהלך שנת 2008 בנושא הגנת מידע אישי	5
דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981 אודות פעולות הפיקוח והאכיפה בשנת 2008	8
מבוא	9
נתונים	9
פעולות פיקוח	9
רישום מאגרי מידע	11
קנס מנהלי	13
דין וחשבון של רשם גורמים מאשרים לפי חוק חתימה אלקטרונית, התשס"א-2001 לשנת תשס"ח-2008	14
מבוא	15
פיקוח	15
פעולות נוספות (שאינן פיקוח)	17
חקיקה והנחיות	17
עדכונים אודות חתימה אלקטרונית באירופה	18
נספח - אופן הפעלת סמכויות הפיקוח בחברת קומסיין	20
דין וחשבון של רשם שירותי נתוני אשראי ושירותי מידע על עוסקים לשנת תשס"ח-2008	25
מבוא	26
מתן רישיונות	26
פיקוח על בעלי הרישיונות	26
טיפול בתלונות	26
הנחיות הרשם	26

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

סטטוס הקמת הרשות

הרשות למשפט, טכנולוגיה ומידע נמצאת בשלבים מתקדמים של הקמה, אך טרם ניתן לקבוע כי הסתיים התהליך והיא נמצאת בשגרת פעולה ברוכה. הקמת הרשות כרוכה בראש ובראשונה בתהליכי תקנון וגיוס כח אדם, אשר במגזר הממשלתי אורכים זמן רב.

על אף האמור לעיל, חלה בשנת 2008 התקדמות רבה בתהליך הקמת הרשות עם בחירתם של מנהלים לשלוש המחלקות ברשות ותחילת איוש הרשות בדרג זוטר יותר. עם זאת, היעד של איוש הרשות ב-20 אנשים במהלך שנת 2008 לא הושג, וגם היעד המתוקצב של 24 אנשים בשנת 2009 לא נראה, בשלב זה, בר השגה.

מבנה ארגוני

כזכור, המבנה הארגוני שאושר לרשות והסמכויות המצויות בידי הרשמים השונים מבסס אותה כרשות מסדירה לתחום של הגנת מידע אישי(personal data protection). מידע אישי הינה הגדרה רחבה, והיא כוללת בתוכה את ההגנה על מידע מוגן פרטיות, אך גם נושאים נוספים כגון זהותו האלקטרונית של האדם (נושא המטופל כיום באופן חלקי בחוק חתימה אלקטרונית) או מידע שהוא אישי, אך לא בהכרח מוגן פרטיות (כגון מספר כרטיס אשראי).

הרשות בנויה בחלוקה הבאה:

<u>מחלקת רישום ופיקוח</u> – עוסקת בשלוש משימות עיקריות, אשר נגזרות מעיקר הסמכויות הקיימות היום בידי הרשמים:

- ניהול מרשם מאגרי המידע לפי חוק הגנת הפרטיות, מתן רשיונות לשירותי נתוני אשראי ומידע על עוסקים ומתן רשיונות לגורמים מאשרים;
- הפעלת סמכויות הפיקוח המסורות לרשמים השונים (סעיף 10 לחוק הגנת הפרטיות; סעיפים 13-10 לחוק שירות נתוני אשראי; סעיף 17 לחוק חתימה אלקטרונית)
- חיבור הנחיות שוק בנושאים הנמצאים באחריות הרגולטורית של הרשות - קרי פרטיות במידע, נתוני אשראי וחתימה אלקטרונית;

לראשות המחלקה נבחרה בסוף 2008 עו"ד רבקי דב"ש, מי שעסקה בעבר בנושא הגנת פרטיות, חופש מידע וחוק הארכיונים במחלקת ייעוץ וחקיקה במשרד המשפטים ועברה לרשות במהלך שנת 2007.

<u>מחלקת אכיפה</u> – מחלקת האכיפה, הנמצאת בשלבי הקמה, אמורה לבצע שתי משימות עיקריות:

- חקירת עבירות על פגיעה בפרטיות במאגרי מידע על פי חוק הגנת הפרטיות וחוק שירותי נתוני אשראי;
- מתן סיוע לגופי אכיפת חוק אחרים בסוגיות המשפטיות והחקיקתיות העולות תוך חקירת מחשבים, בפרט בסוגיות של ראיות אלקטרוניות;

לראשות המחלקה נבחרה במהלך שנת 2008 עו"ד מילי בך, לשעבר ראש צוות חקירות ברשות להגבלים עסקיים.

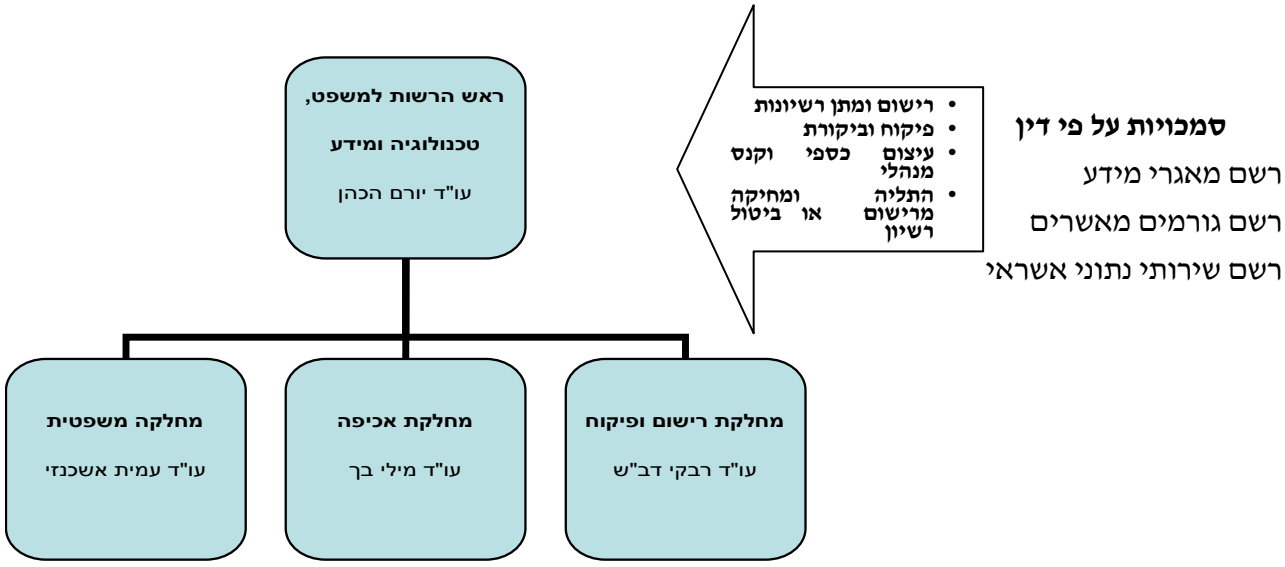
דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

<u>מחלקה משפטית</u> – למחלקה המשפטית של הרשות שלושה תפקידים עיקריים:

- מתן ייעוץ משפטי פנימי לפעילות הרשות כרשות רגולציה ואכיפת חוק;
- מוקד ידע פנימי של משרד המשפטים בסוגיות שונות של משפט וטכנולוגיה;
- מתן ייעוץ משפטי לפרויקטי טכנולוגית מידע משמעותיים בשירות הציבורי (ממשל זמין, תעודת זהות חכמה וכד') בהיבטים הייחודיים של משפט וטכנולוגיה;

לראשות המחלקה נבחר במהלך שנת 2008 עו"ד עמית אשכנזי, שהוא בעל ניסיון רב ממחלקת ייעוץ וחקיקה בנושאי טכנולוגיה ומשפט. עמית משמש גם כרשם גורמים מאשרים.

הסמכויות השונות המוקנות לרשמים על פי דין, מופעלות על ידי המחלקות השונות בהתאם לנושא.



משימות עיקריות במהלך שנת 2008 בנושא הגנת מידע אישי

מעבר למשימות הפיקוח, הרישוי והאכיפה המתוארות בדו"חות השונים להלן, הרשות עסקה במהלך שנת 2008 במספר נושאים מרכזיים הקשורים לתחומי עיסוקה כרשות העוסקת בהגנת מידע אישי. בפרק זה נתאר את עיקריהם. יצויין, כי מעבר לאמור כאן עסקה הרשות בנושאים נוספים הקשורים במשפט וטכנולוגיה, אך כיון שאינם קשורים בסוגיות של פרטיות או של חתימה אלקטרונית, הם אינם מפורטים בדו"ח זה.

<u>מימוש המלצות דו"ח שופמן</u>

דו"ח הצוות לבחינת החקיקה בתחום מאגרי המידע בראשות המשנה ליועץ המשפטי לממשלה (חקיקה) יהושע שופמן שהוגש בשנת 2007 (להלן – **דו"ח שופמן**) המליץ על שורה של שינויים בפרק ב' לחוק הגנת הפרטיות.

במהלך שנת 2008 נעשתה עבודה משותפת לרשות ולמחלקת ייעוץ וחקיקה במשרד המשפטים לקידום יישום המלצות דו"ח שופמן. הוחלט להפריד בין תהליך חיזוק סמכויות רשם מאגרי מידע והכלים הרגולטוריים העומדים לרשותו ובין תהליך גיבוש השינויים האחרים בחוק, זאת כדי לתת לרשם מאגרי מידע במהירה את הכלים המודרנים הנדרשים לצורך פעילותו.

במהלך שנת 2008 הושקע מאמץ ניכר לנסח את טיוטת תזכיר חוק המבסס את סמכויות האכיפה של רשם מאגרי מידע בפעולתו כגורם האוכף את חוק הגנת הפרטיות בהיבט של פרטיות במידע ממוחשב. תזכיר זה יוגש לכנסת במהלך שנת 2009, והוא מגדיר באופן מדויק את העבירות וההפרות הקשורות בפרטיות במידע, את סמכויות האכיפה של רשם מאגרי מידע של עבירות אלה ואת אמצעי האכיפה הנדרשים כדי לממש את הסמכויות.

במקביל, נמשך ברשות תהליך של ניתוח וניסוח יתר השינויים בחוק הגנת הפרטיות שהומלצו בדו"ח שופמן. אל שינויים אלה יתווספו המלצות לשינויים נוספים בחוק, העולות מהעיסוק היום-יומי ברשות בתחום הגנת המידע האישי.

הח"מ רואה בתהליך התאמת חוק הגנת הפרטיות, אשר נחקק בשנת 1981, לאתגרים שמציבה המציאות העכשווית והכיוונים אליהם חותרת טכנולוגיות המידע משימה עיקרית של הרשות אשר מחויבת מהשינויים הדרמטיים בפעולות עיבוד מידע ממוחשב.

<u>ליווי עבודת המטה להצעת חוק הכללת אמצעי זיהוי ביומטריים במסמכי זיהוי ובמאגרי מידע, התשס"ט-2008</u>

במהלך שנת 2008 השתתפה הרשות בתהליך המטה הממשלתי לגיבוש הצעת חוק הכללת אמצעי זיהוי ביומטריים במסמכי זיהוי ובמאגרי מידע, התשס"ט-2008.

מטרת הצעת חוק זו לאפשר נטילת אמצעי זיהוי ביומטריים מאזרחים על ידי משרד הפנים במסגרת הנפקתם של תעודות זהות ודרכונים הכוללים שבב מחשב, והמאפשרים אימות וזיהוי אלקטרוניים של נושא מסמך הזיהוי. בהצעת החוק מוצע להקים מאגר מידע המכיל נתונים ביומטריים של כל אזרחי מדינת ישראל.

במסגרת תהליך המטה הודגש והובהר על ידי הרשות פוטנציאל הסכנה לפרטיות כתוצאה משימוש לא הולם בטכנולוגיה הביומטרית, ובפרט באבטחת המידע הביומטרי במאגר המידע. חלק מהמלצות הרשות לעניין זה התקבלו ובאו לידי ביטוי בנוסח הצעת החוק.

במהלך שנת 2009 משתתפת הרשות בדיונים המתקיימים בכנסת בהצעת החוק.

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

תהליך הצטרפות ישראל ל-OECD

במהלך שנת 2008 רכזה הרשות את עבודת המטה הממשלתית מול ועדת מדיניות מחשבים, מידע ותקשורת (ICCP – Information, Computers and Communication Poclicy) של ארגון ה-OECD וזאת במסגרת תהליך הצטרפות ישראל לארגון.

לצורך קבלת ישראל ל-OECD על ישראל להוכיח כי היא עומדת במסמכי ההנחיה החלים על חברות הארגון. לועדת ה-ICCP מספר הנחיות העוסקות בסוגיות של פרטיות במידע(data protection), אבטחת מידע (data security), מדיניות פס רחב (broadband), הגנת תשתיות מידע קריטיות (Critical Information Infrastructure), הזדהות וחתימה אלקטרוניים (e-Authentication/e-Signature), הסדרת השימוש בהצפנה (Cryptography) ושימוש נוסף במידע ציבורי (re-use of Public Sector Information).

הרשות נהלה את התהליך מול ועדת ה-ICCP, ורכזה את המענה של מדינת ישראל בנושא אשר כלל התייחסות של משרד ראש הממשלה, ומשרדי האוצר, הבטחון והתקשורת. תהליך זה אמור להסתיים בשנת 2009 עם אישור עמידת ישראל בהנחיות הארגון בהבטים אלה.

לעניין זה יש להדגיש כי קיומה של הרשות עזר באופן משמעותי לתהליך האישור של ישראל בנושאי הליבה של ה-ICCP, שכן סוגיות הקשורות בהגנת מידע אישי הן מרכזיות בעיסוק הועדה בנושא.

בקשת הכרת הנציבות האירופית בהתאמת ישראל לדירקטיבה האירופית להגנת מידע אישי

בסעיף 26 לדו"ח רשם מאגרי מידע משנת 2007 דווח על הגשת בקשה של ישראל להכרה כי משטר הגנת הפרטיות במידע בישראל מקיים רמה מקבילה לזו הקיימת בדירקטיבה האירופית להגנת מידע אישי, ועל כן ניתן להכיר בישראל כמקיימת "רמה הולמת" של הגנת מידע על פי סעיף 25(6) לדירקטיבה.

במהלך שנת 2008 התקבל דו"ח בדיקה שבוצע על ידי הנציבות האירופית בנושא ולגבי מספר נקודות בו נדרשה התייחסות מפורשת. הרשות גבשה את המענה בנושא, ונמצאת בהמשך תהליך בחינת הבקשה על ידי הנציבות האירופית.

גם לעניין זה ראוי לציין כי קיומה של הרשות, בדומה לרשויות הגנת מידע אירופאיות, ותפקודה בפועל, הינו נדבך חשוב וקריטי בתהליך ההכרה בישראל כתואמת את הנדרש בדין האירופי.

ליווי גיבוש טיוטת תזכיר להפצת מידע מרשם החברות

במהלך שנת 2008 בוצעה על ידי הרשות, במשותף עם רשות התאגידים במשרד המשפטים עבודת מטה לבחינת ההסדר הקיים להפצת מידע מרשם החברות. תהליך זה נדרש עקב כשלים שהתגלו בתהליך הקיים של הפצת המידע מרשם החברות באמצעות זכיינים.

לצורך הגנה על הפרטיות מחד גיסא ובחינת הצרכים הכלכליים מאידך גיסא נעשה על ידי הרשות ורשות התאגידים תהליך מטה מסודר אשר בחן את התכליות הראויות להסדרה בעניין זה, ואת המסגרת הנכונה לשם פיקוח על תהליך הפצת המידע מרשם החברות למטרות הלגיטימיות.

בסופו של התהליך הופץ תזכיר לתגובת הציבור, המציע מסגרת של מערכת רשיונות להפצת המידע האמור, באופן שיתקיים האיזון האמור עיל.

תזכיר חוק זה אמור להיות מובא בפני הכנסת במהלך שנת 2009.

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

<u>גיבוש תוכנית twinning בנושא הגנת מידע אישי עם הנציבות האירופית</u>

במהלך שנת 2008 גובש המכרז לקיום תוכנית twinning עם הנציבות האירופית בנושא של "חיזוק הגנת מידע אישי בישראל" בתקציב של כ-1,000,000 אירו. Twinning היא תוכנית הממומנת על ידי הנציבות האירופית, במסגרתה מתבצע שיתוף פעולה בין רשות מדינתית אירופית לרשות מקומית.

המכרז שגובש פרט מסגרת לתוכנית בת 18 חודשים שתעסוק בהבטים שונים של הגנת מידע אישי, וזאת כדי לשפר את היכולות של הרשות בקיום תפקידיה כרשות הגנת מידע אישי, כמו גם לגרום להעלאת מודעות בציבור בנושא זה.

בתהליך המכרזי שנערך בין מדינות אירופאיות שונות נבחרה רשות הגנת המידע האישי של ספרד Agencia Española de Protección de Datos (AEPD) שהיא רשות הגנת מידע אישי מובילה, ואשר הצעתה כללה שליחת מומחים מרחבי אירופה במסגרת התוכנית.

במסגרת התוכנית, אשר צפויה להתחיל במחצית שנת 2009 יתבצע מספר רב של פעילויות שיועברו על ידי מומחי בנושא הגנת מידע אישי מאירופה. בין היתר, יתקיימו סדנאות פנימיות לעובדי הרשות, ימי עיון לציבור הרחב ולסקטורים מוגדרים, סיורים ברשויות הגנת מידע אישי מקבילות באירופה וייצור מסמכי הנחיה והעלאת מודעות בנושא של פרטיות במידע.

הרשות מייחסת חשיבות רבה לתוכנית זו, אשר עשויה לספק ידע ייחודי בנושא ממקורות אירופאיים מגוונים, חשיפת אנשי הרשות למתודות פיקוח ואכיפה ברשות מקבילות והעלאת המודעות לנושא בקרב בעלי מאגרי מידע ובציבור הרחב.

דין וחשבון של רשם מאגרי מידע לפי חוק הגנת הפרטיות, התשמ"א-1981
אודות פעולות הפיקוח והאכיפה בשנת 2008

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

מבוא

במהלך שנת 2008 סבלה פעילות הפיקוח של רשם מאגרי מידע מתהליך החלפת כוח האדם, שהוא חלק מתהליך הקמת הרשות ואודותיו כבר דווח בדין וחשבון לשנת 2007[2]. פעולות הפיקוח שנעשו היו מצומצמות יחסית, ועיקר המאמץ הפיקוחי התמקד בבירור תלונות שהתקבלו מאזרחים.

במחצית שנת 2008 נבחרה עו"ד מילי בך לעמוד בראש מחלקת האכיפה של הרשות. לקראת סוף שנת 2008 נבחרה עו"ד רבקי דב"ש לעמוד בראש מחלקת רישום ופיקוח ועו"ד לימור שמרלינג-מגנזיק כסגניתה והממונה על הפיקוח.

מינויים אלה סללו את הדרך לתחילת תפקודן של המחלקות בחלוקת התפקידים המיועדת להן, לפיהן מחלקת רישום ופיקוח עוסקת בתהליך רישום ורישוי ופיקוח עקב תלונות אודות הפרות של חוק הגנת הפרטיות, בעוד שמחלקת האכיפה מטפלת במקרים קשים יותר, העשויים לעלות עד כדי עבירה פלילית על הוראות חוק הגנת הפרטיות. לעניין זה יש להבהיר כי בשלב זה לא קיימות בידי הרשות סמכויות חקירה פליליות, ועל כן מופעלות הסמכויות המצויות בפרק ב' לחוק הגנת הפרטיות.

בשל המצב המתואר לעניין מצבת כח האדם לאורך רוב השנה כמעט ולא התקיימה פעולה יזומה של פיקוחי רוחב, החיוניים כדי לזהות תופעות בתחום הגנת הפרטיות במידע.

נתונים

בשנת 2008 נפתחו 122 תיקי פיקוח, מתוכם 111 תיקים אשר מקורם בתלונה (זאת לעומת 90 תיקי פיקוח אשר נפתחו בשנת 2007). הטיפול ב- 85 תיקים (כ- 70%) הסתיים באותה שנה.

בחינת תוכן התלונה ומיהות הנילונים מעלה כי מרבית התלונות נגעו לפגיעה בפרטיות כתוצאה מפעולות שיווקיות[3] (15 תלונות – כ-33% מסך התלונות). בנוסף, פעילות המגזר הפיננסי הטרידה את המתלוננים (7 תלונות – כ– 15%) ותחום התקשורת ופעילותם של גופים ציבוריים (5 תלונות כ"א כ-11% לכל סקטור).

מרבית התלונות הגיעו לרשות דרך אתר האינטרנט של הרשות (18 תלונות) או בדואר האלקטרוני (14 תלונות).

פעולות פיקוח

מדיניות רשם מאגרי מידע היא כי הדיווח על פיקוחים מתבצע רק לאחר סיום תהליך הפיקוח, וזאת כדי לא לפגוע בתהליך הפיקוח. על כן, מפורטות להלן מספר פעולות פיקוח אשר לגביהן ניתן למסור מידע, שכן תהליך הפיקוח הסתיים או שניתן לפרסם את תוכן הפיקוח מבלי לפגוע בתהליך.

<u>גופים ציבוריים</u>

<u>משרד הבטחון</u>

בדו"ח השנתי לשנת 2007, דווח על התליית רישומו של מאגר מידע בשירות אגף השיקום במשרד הבטחון עקב מציאת כשלים בשמירה על הוראות אבטחת מידע בתהליכי העברת מידע מהאגף לגורמים חיצוניים כמיקור חוץ[4]. בתהליך המשך לפיקוח, נערכה פגישה בין נציגי משרד הבטחון לרשם מאגרי המידע, בעקבותיה התקבל מהמשרד מידע נוסף אודות תהליכי השמירה על הפרטיות במשרד הבטחון.

---

[2] ראו סעיפים 9 , 10, 17 ו-18 לדו"ח רשם מאגרי מידע משנת 2007.

[3] בכללן כמחצית נגעו לסעיף 30א לחוק התקשורת (העוסק בפניות בלתי מוזמנות באמצעים אוטומטיים) – 7 במספר

[4] ראו סעיף 19 לדו"ח רשם מאגרי מידע משנת 2007.

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

בחינת החומר העלתה כי עדיין ישנם ליקויים באופן טיפולו של משרד הבטחון בנושא הגנת הפרטיות במידע האגור במאגרי מידע המצויים בניהולו, ובפרט ככל הקשור בתהליכי העברת מידע לגורמים חיצוניים במסגרת מיקור חוץ.

רשם מאגרי המידע הורה למשרד לתקן את הליקויים שנמצאו לאלתר. בכוונת הרשם לערוך פיקוח חוזר בסוגיה זו בהמשך שנת העבודה 2009.

<u>המפקח הארצי על הבחירות והפצת פנקס הבוחרים</u>

לקראת בחירות לכנסת, נמסר לרשימות או מפלגות המתמודדות בבחירות תקליטור ובו רשימת הבוחרים ממרשם האוכלוסין (להלן – הפנקס) בהתאם להוראות סעיף 39 לחוק הבחירות לכנסת [נוסח משולב], תשכ"ט – 1969 (להלן – חוק הבחירות). המידע הכלול בתקליטור כולל שם משפחה ושם פרטי, מספר תעודת זהות, וכתובת מדויקת והוא מכיל את כל בעלי זכות הצבעה בבחירות הארציות.

לפי חוק הבחירות השימוש בפנקס מותר רק לצורך התמודדות בבחירות לכנסת ולצורך קשר עם ציבור הבוחרים ; אין לעשות במידע שימוש אחר <u>לרבות העברתו לצד שלישי</u>.

במערכות בחירות קודמות, עלה חשש שרשימות הבוחרים שנמסרו לנציגי המפלגות לצורך מערכת הבחירות, דלפו שלא כדין לגורמים פרטיים שונים, תוך פגיעה בפרטיות ציבור הבוחרים ועבירה של הוראות החוק.

לפיכך, הוחלט לערוך פיקוח רוחבי בתחום זה על מנת ללמוד את פעילות המפקח על הבחירות, משרד הפנים, המפלגות וגופים נוספים, לבחון את הכשלים וליתן המלצות לשינוי התהליך על מנת לצמצם את אפשרות הפגיעה בפרטיות. תהליך הפיקוח החל בשלהי שנת 2008, וצפוי להסתיים בשנת 2009.

עם סיום הפיקוח, יועברו ממצאיו בדו"ח נפרד.

<u>כשל אבטחת מידע בבית חולים איכילוב</u>

בעקבות ידיעה עיתונאית על כשל אבטחת מידע באתר האינטרנט של בית החולים איכילוב, בוצע פיקוח לבחינת מהות הכשל ואופן התנהלות ביה"ח והחברה המפעילה את האתר עבור ביה"ח.

הבדיקה העלתה כי כשל אבטחת המידע, אפשר למי שאינו מורשה לעיין בפרטי הזמנת תורים למרפאות חוץ של בית החולים על ידי הכנסת מספר תעודת הזהות של המזמין לפקודת ה-http של דפדפן האינטרנט.

הכשל תוקן מיידית על ידי החברה המפעילה את האתר, אך בבדיקה נתגלו ממצאים מדאיגים בנוגע למדיניות אבטחת המידע בבית החולים, אשר תוצאתה באה לידי ביטוי גם בכשל המתואר לעיל.

בעקבות דרישה של הרשם, הכין ביה"ח תוכנית עבודה לטיפול בליקויים, לרבות ביצוע סקר סיכונים מקיף. תוכנית עבודה זו אמורה להיות מיושמת על ידי בית החולים במהלך שנת 2009, ובכוונת הרשם לבדוק את התקדמות המפוקח לפי תוכנית העבודה ותיקון הליקויים כנדרש.

<u>מגזר פרטי</u>

<u>חברת ישרכארט – חשיפת מידע עודף בהליך משפטי</u>

התקבלה תלונה כנגד חברת ישרכארט בטענה שהחברה העבירה מידע המצוי במאגריה, לגורם שלישי מעבר לנדרש.

עניינה של התלונה היה תביעה שהוגשה על ידי צד ג' כנגד המתלונן וחברת ישראכרט בגין עסקה שביצע המתלונן. במסגרת כתב ההגנה מטעמה הגישה ישראכרט תדפיסי פירוט פעולות של המתלונן לגבי מספר חודשים. בכל אחד מהתדפיסים הופיעו נתונים כגון מס' החשבון, פירוט עסקאות שביצע המתלונן באותו חודש, עסקאות תשלומים שביצע במועדים אחרים, נתוני מסגרת האשראי ונתונים נוספים.

לאחר בירור מול החברה נמסרה הודעה לחברה כי על פניו המידע שנמסר על ידם במסגרת ההליך המשפטי מהווה פגיעה לכאורה בפרטיות לפי סעיף 2 לחוק, שכן המידע שנמסר בהליך המשפטי אינו נדרש באותו עניין ולא היה צורך בחשיפתו במסגרת ההליך אשר עסק בעסקה מסוימת עם בית עסק אחד. החברה נתבקשה ליידע את הרשם בדבר הפעולות שבכוונתו לנקוט על מנת להבטיח כי מקרים כאלו לא יישנו.

<u>שימוש בעותקים בלתי חוקיים של מרשם האוכלוסין</u>

בדו"ח רשם מאגרי מידע משנת 2007, דווח על התופעה של זליגת מידע ממרשם האוכלוסין למאגר מידע המופץ ברשת האינטרנט[5] והטיפול באירוע על ידי משרד הפנים. במהלך שנת 2008 התקבלו מספר תלונות, שבדיקתן העלתה כי קיים ביניהן מכנה משותף והוא שימוש על ידי גופים מסחריים במאגר המידע הבלתי חוקי הנ"ל.

השימושים הבלתי חוקיים במאגר מסתברים להיות מהטיפוסים הבאים:

- שימוש במידע למטרת פעילות מפולחת של דיוור ישיר
- שימוש במידע לאיתור אנשים בהליכי גביית חוב
- שימוש במידע למטרות של גניבת זהות[6] או וידוא פרטי הזהות

תהליכי הבדיקה של התלונות הנ"ל נמצאים עדיין בשלבי בירור, אך לדעתנו היקף השימוש במידע מתוך מאגר המידע הנ"ל במגזר הפרטי, ולעיתים גם על ידי ספקי שירות של מגזר ציבורי, היא גדולה ומדובר בתופעה חמורה.

לעניין זה יחידת רשם מאגרי מידע פועלת לצמצום התופעה במסגרת הסמכויות המוקנות לה כיום, אך לאור מקרים מסוג זה בולט חסרונן של סמכויות מקיפות יותר לרשם, אשר תאפשרנה התמודדות יותר אפקטיבית עם אירועים מסוג זה.

<u>בנק לאומי – שימוש במידע שלא למטרה שהתקבל</u>

אצל רשם מאגרי מידע התקבלה תלונה כי בסניף של בנק לאומי בחיפה נעשה שימוש במידע שמנוהל על ידי הבנק כמתפעל של קרן השתלמות למטרות שיווקיות, החורגות במפורש מהשימוש הלגיטימי שהותר לו לעשות במידע. פיקוח במקום אימת את החשד להפרה, והתברר כי לא מדובר במעידה חד-פעמית אלא שיטת הפעולה של פקידי הסניף. עוד הסתבר כי הפעולה נעשתה בניגוד להנחיות כלליות שנתנו בבנק לעניין ולהתחייבות מפורשת שנתן הבנק לרשם מאגרי מידע בעת אישור הסכמי התפעול של הבנק במסגרת מימוש רפורמת בכר[7]. הבנק אישר למתלונן את עיקרי התלונה, והתחייב לרענן את הנהלים ולאכוף אותם.

מקרה זה הינו דוגמה למגבלות האכיפה במסגרת הסמכויות הקיימות לרשם מאגרי מידע היום. על פניו מדובר בעבירה פלילית לכאורה[8] והפרה של התחייבות שנתנה לרגולטור. אמצעי האכיפה הקיימים היום

---

[5] ראו דו"ח רשם מאגרי מידע לשנת 2007, סעיף 19.ב.2.ב.

[6] על כך לא התקבלה תלונה ישירה ברשות.

[7] לעניין ההנחיות הרגולטוריות בעניין זה ראו סעיף 11 לדו"ח רשם מאגרי מידע משנת 2007.

[8] הפרה של הוראות סעיף 2(9) לחוק הגנת הפרטיות, עבירה שבצידה עונש של חמש שנות מאסר.

לרשם מאגרי מידע מוגבלים ומתמצים באפשרות להתלות או למחוק מאגר מידע מפנקס מאגרי מידע[9] או בהטלה של קנס מנהלי, אשר ניתן להפעלה על עבירות אחריות קפידה שאינן הולמות מקרה זה. התמריץ הקיים להפר את החוק הוא כלכלי בעיקרו (שימוש במידע למטרות שיווקיות), ועל כן חשוב שתהיה סנקציה אשר תמזער את הכדאיות הכלכלית של ההפרה, דוגמת האפשרות להטיל עיצום כספי על ידי הרשם.

רישום מאגרי מידע

<u>נתונים</u>

בשנת 2008 הוגשו 472 בקשות חדשות לרישום מאגרי מידע - עליה קלה מול שנת 2007 בה הוגשו 442 בקשות אך במסגרת המגמה הטבעית של גידול שנתי מתון של בקשות הרישום הנובע מהתרחבות המשק הישראלי.

כפי שצויין בדו"ח רשם מאגרי מידע לשנת 2006, הליך הרישום מתבצע ברובו במיקור חוץ מול רשות הדואר, על הבעיות הנגזרות מכך – כפי שצויין שם[10]. נוסף על כך, מערכת המידע שמעמידה רשות הדואר לניהול פנקס מאגרי המידע, אינה נותנת מענה מתאים לצרכי יחידת הרשם.

לאור האמור לעיל הוחלט לשנות את אופן פעילות היחידה מול רשות הדואר, כאשר בשלב ראשון טופל תהליך רישום מאגרי מידע חדשים. מטרת השינוי נועדה להוביל לתוצאות הבאות –

- הגברת היעילות בטיפול בבקשות הרישום לאור כח האדם המצומצם אשר ניתן להקצות למשימה;
- עמידה ביעד של מתן אישור רישום למאגרי מידע תוך 90 יום. לצורך כך נקבע יעד של מתן אישורי רישום תוך 90 יום ל-70% מהמאגרים שהגישו בקשות חדשות;
- יישור קו לגבי מאגרי המידע אשר הגישו בקשות רישום בעבר וטרם קיבלו אישור כאמור למרות חלוף 90 הימים (כ-1500 מאגרים). מטרת מהלך זה לצמצם את מספר מאגרי המידע הממתינים לאישור רשם בשליש, וצמצום מספר מאגרי המידע הממתינים לאישור רשם לעשרות ספורות בסוף שנת 2010.

<u>צמצום חובת רישום מאגרי מידע</u>

בעקבות המלצות דו"ח שופמן, ולאור המידע שנאסף מיום כניסתו של רשם מאגרי מידע הנוכחי, הוחלט לקדם, בשיתוף עם מחלקת ייעוץ וחקיקה במשרד המשפטים, הצעה לצמצום חובת רישום מאגרי המידע או לבחינת חלופות לחובה זו. בימים אלו מתגבשת טיוטת תזכיר אשר תכלול, בין היתר, הצעות לשינוי בתחום זה תוך כוונה שזו תשולב בטיוטת תזכיר סמכויות האכיפה האמור.

לעניין זה, יש לדעת כי המשאבים המוקדשים כיום על ידי יחידת רשם מאגרי מידע למכלול ההבטים של הרישום (בדיקת בקשות רישום, בקשות לשינוי פרטי רישום, תהליך גביית אגרות רישום ואגרות שנתיות), יחסית לגודלה של הרשות, הם רבים.

בעבודה הקשורה ברישום מאגרי מידע עוסקים היום שני עובדים באופן שוטף. בנוסף עוסקים בכך באופן חלקי, בפרט בתקופת הפצת האגרה השנתית, עובדים נוספים במחלקת רישום ופיקוח אשר עונים על פניות הציבור בנושא. מוחזקת מערכת מידע ייעודית בחברת הדואר לניהול פנקס מאגרי המידע, וחלק מהעבודת הרישום נעשה במיקור חוץ על ידי עובדת חברת הדואר. כדי להקל על העומס בתקופה של תשלום האגרות מופעל זה שנתיים מוקד ייעודי במיקור חוץ המעסיק שני אנשים.

התועלת להגנת הפרטיות במידע של האזרחים מהליך רישום מאגרי מידע מוטל בספק. מי משמעבד מידע פרטי פוגש את הרשות המסדירה, רשם מאגרי מידע, בעיקר בהבטים של רישום ותשלום אגרות ופחות בהיבטים של קיום החובות המהותיות על פי חוק הגנת הפרטיות – שימוש במידע למטרה שנמסר, שמירה על סודיות המידע ואבטחתו, מתן זכות עיון ותיקון במידע לנושאי המידע וכד'.

---

[9] שתהפוך כל פעילות עיבוד מידע במאגר לבלתי חוקית.
[10] ראו סעיף 11 לדו"ח רשם מאגרי מידע לשנת 2006.

העקרון של רישום מאגרי מידע מקורו בשנות ה-80, בו כמות מאגרי המידע במדינה הייתה בסדר גודל של מאות. כיום, קיימים בישראל עשרות מליוני מחשבים[11] שכל אחד מהם עשוי להכיל מאגר מידע אחד או יותר.

להליך של רישום מאגרי מידע יכול להיות תועלת חיובית, וזו גם הודגמה בתהליך שתואר בדו"ח הרשם לשנת 2007 בהקשר של קופות הגמל[12]. אך העמדה המקצועית של הרשות, לאור הנסיון המצטבר בנושא היא שניתן למצוא הסדרים חלופיים לתועלות המתקבלות מתהליך רישום, ולצמצם באופן משמעותי את החובה הבריוקרטית המוטלת כיום תוך שיפור מצב ההגנה על הפרטיות במידע בכל היבט.

יצויין, כי ככל שמדובר בגופים ציבוריים האוספים מידע אודות אנשים מכח חוק (ולא על בסיס הסכמה כנדרש בחוק הגנת הפרטיות) ומי שעוסק בסחר במידע[13] עמדת הרשות היא כי יש להמשיך בקיום חובת רישום כאמור מהטעם שהשימוש במידע לא נעשה על בסיס הסכמת האנשים או ידיעתם.

<u>דחיית בקשת רישום בשל חשד לרישום למטרה בלתי חוקית</u>

במהלך שנת 2008 התקבלה אצל רשם מאגרי מידע בקשה לרישום מאגר מידע לשירות נתוני אשראי לפי חוק שירות נתוני אשראי. נסיבות הבקשה ומיהות המבקש העלו חשד כי עצם רישום מאגר המידע ישמש לפעילות בלתי חוקית או כמסווה להם.

לאחר בדיקה החליט רשם מאגרי מידע, מכוח הסמכות המוקנית לו בסעיף 10(א)(1)[14] לחוק הגנת הפרטיות לסרב לבקשה. למבקש נתנה שהות כקבוע בסעיף 10(א)(3) לחוק הגנת הפרטיות להשמיע את טענותיו. המבקש בחר שלא לטעון כנגד ההחלטה, ובקשת רישום מאגר המידע נמחקה.

הפעלת סמכות זו של רשם מאגרי מידע היא נדירה, ובפרט במקרה המתואר לעיל.

קנס מנהלי

לקראת סוף שנת 2008 הסתיים תהליך הפעלת אפשרות מתן קנס מנהלי על ידי רשם מאגרי מידע בדרך של המרת עבירות פליליות של אחריות קפידה על פי סעיף 31א לחוק הגנת הפרטיות לקנס. אודות האפשרות שיוטל קנס מנהלי פורסמה הודעה לציבור.

במהלך שנת 2009 יופעל הקנס במקרים הראויים לכך, מקום שיהיו בידי רשם מאגרי מידע ראיות להפרת סעיף 31א לחוק.

לעניין זה נבקש לציין כי בתזכיר סמכויות האכיפה האמור, מגובש מנגנון חלופי של עיצומים כספיים, אשר מתאים טוב יותר, לדעת רשם מאגרי מידע, לסוג ההפרות של חוק הגנת הפרטיות אשר רבות מהן נובעות משיקולים כלכליים.

---

[11] לעניין זה יש להבין כי כל טלפון סלולרי הוא מחשב, כהגדרתו בחוק המחשבים, התשנ"ה-1995 ומחזיק, במקרים רבים, מידע אישי רב.

[12] ראו סעיף 14 לדו"ח רשם מאגרי מידע משנת 2007.

[13] כלומר מי שמוכר מידע שאסף אודות אנשים לאחרים למטרות כגון דיוור ישיר, טיוב מידע, שיווק וכד'.

[14] "הוגשה בקשה לרישום מאגר מידע —
(1) ירשום אותו הרשם בפנקס, תוך 90 ימים מיום שהוגשה לו הבקשה, זולת אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין"

דין וחשבון של רשם גורמים מאשרים לפי חוק חתימה אלקטרונית, התשס"א-2001 לשנת תשס"ח-2008

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

מבוא

חוק חתימה אלקטרונית התשס"א - 2001 (להלן בפרק זה – **החוק**) והתקנות שהותקנו מכוחו, נועדו להגביר את הוודאות לגבי פעולות המתבצעות באופן אלקטרוני ע"י הסדרת תוקפה המשפטי ומעמדה הראיתי של החתימה האלקטרונית בישראל.

על פי החוק מונה רשם גורמים מאשרים, הפועל כיום במסגרת הרשות למשפט, טכנולוגיה ומידע במשרד המשפטים. תפקיד הרשם לרשום את הגורמים המאשרים במרשם הגורמים המאשרים, וזאת לאחר תהליך בדיקה קפדני בדבר עמידתם בתנאים המקדמיים הקבועים בחוק. לאחר רישום גורם מאשר, מפקח הרשם על פעילותם של הגורמים המאשרים, על מנת להבטיח כי הם עומדים בדרישות החוק ותקנותיו.

הרשם מפעיל סמכויות בהתאם לחוק וכן בהתבסס על שני קובצי תקנות מקיפים בנושא זה, שהנם תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 (להלן – **תקנות חומרה ותוכנה**), ותקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001 (להלן – **תקנות רישום גורם מאשר**).

הרשם הנוכחי, עו"ד עמית אשכנזי, מונה לתפקידו ב- 10.01.07.

לרקע כללי בדבר הפעלת החוק, מוזמן הקורא לעיין בסעיף 2 לדוח השנתי לשנת תשס"ז-2007.[15]

פיקוח

עיקר תפקידי הרשם אמורים להשתלב במסגרות סמכויות מחלקת הרישום והפיקוח של הרשות, ובכך לנצל את בצורה יעילה יותר את כוח האדם הפיקוחי ואת הנסיון בנושא זה. לקראת סוף שנת 2008 החל מהלך ארגוני זה להתבצע אולם טרם הושלם.

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

במרשם הגורמים המאשרים רשום כיום גורם מאשר אחד, חברת קומסיין בע"מ (להלן – **קומסיין**). במהלך שנת 2008 בוצעו מספר פיקוחים בקומסיין, וזאת לאחר שבפיקוחים שבוצעו בשנת 2007 נמצאו ליקויים ברמת אבטחת המידע של מערך הגורם המאשר בחברה, אשר אינם תואמים את הרמה הנדרשת מניהול מערך רגיש שכזה.

בהתאם לדרישת הרשם החלה חברת קומסיין בפעילות מתקנת על-מנת להביא את רמת אבטחת המידע לרף הנדרש ולתקן את יתר הליקויים שנתגלו בתהליכי העבודה. תהליכי תיקון הליקויים בחברת קומסיין לא בוצעו בקצב הנדרש[16]. הרשם ממשיך לקיים פיקוח שוטף על השלמת תיקון כל הליקויים כנדרש.

---

[15] הדוח ניתן לעיון באתר האינטרנט של הרשם: בכתובת
http://www.justice.gov.il/NR/rdonlyres/E75A70A5-EE75-4E32-A3A0-F0B83BBAF380/10394/DochRasham2007.pdf

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

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

הצגת מסמך כוזב לכאורה במהלך פיקוח

בספטמבר 2007, במהלך פיקוח שוטף הוצג בפני הרשם מסמך, אשר נחזה להיות פרוטוקול חתום אלקטרונית על ידי ששה מעובדי קומסיין, ובו תיעוד, לכאורה, על השתתפותם בתהליך חילול אמצעי חתימה של הגורם המאשר מספר שבועות לפני כן. בבדיקה של תיעוד ויזואלי הקיים בגורם המאשר אודות המועד שבו בוצע התהליך, הסתבר כי התהליך בוצע על ידי שני עובדי קומסיין בלבד.

לפי נהלי חברת קומסיין, כפי שהוגשו לרשם ואשר בהתבסס עליהן קיבלה החברה את האישור ונרשמה במרשם, הטיפול במפתח החתימה, המאפשר הנפקת תעודות, מחייב ביצוע פרוצדורה קבועה ונוקשה אשר תהא מבוצעת על ידי ובנוכחות ששה מעובדי החברה. נוהל נוקשה זה נקבע לאור החשיבות הרבה של אבטחת מפתח החתימה בפעילות של גורם מאשר.

מהעובדות המתוארות, אשר נתמכות אף בראיות אובייקטיביות, התעורר החשד כי נציגי חברת קומסיין מסרו ביודעין מסמך שתוכנו כוזב על מנת להניח את דעתו של הרשם שערך ביקורת בחברה. מדובר במעשה חמור, שכן, כאמור לעיל, ישנה חשיבות רבה לאמון שרוכש הרגולטור לחברה, במיוחד לאור התלות בחברה הן לאור היותה החברה היחידה שרשומה במרשם והן לאור אופי המערכות הציבוריות המשתמשות בתוצרי החברה.

בהתייעצות עם המשנה לפרקליט המדינה, מר שוקי למברגר ובהנחייתו הוגשה לעניין זה תלונה למשטרה. התלונה נחקרה במהלך שנת 2008 והתיק הועבר לפרקליטות להמשך טיפול.

פיקוח על פעילות ההוצאה לאור של לשכת עורכי הדין כגורם רושם

במסגרת הפעילות השוטפת, אושר לקומסיין להתקשר עם ההוצאה לאור של לשכת עורכי הדין, כדי שתשמש כגורם רושם, וזאת בהתאם לסמכות הרשם על פי תקנה 10(1) לתקנות חומרה ותוכנה. בהתאם לכך, מבצעת לשכת עורכי הדין את תפקיד אימות הזהות של עוה"ד המבקשים להנפיק תעודה אלקטרונית, שהינו השלב הראשון שנעשה בהנפקת תעודה , וזאת בשמה של חברת קומסיין.

האישור ניתן לאחר בחינת ההסדרה החוזית והנהלית של הנפקת תעודות אלקטרוניות, בין קומסיין לבין ההוצאה לאור של לשכת עורכי הדין. האישור הראשון ניתן בתנאים שנקבעו בו, החל מיום 20.08.07, לתקופה של חצי שנה, כלומר עד ליום 20.02.08. הפעילות לפי הסדר זה החלה בפועל בשנת 2008 ובהתאם לכך הוארך האישור עד לספטמבר 2008.

בפיקוח שבוצע בהוצאה לאור של לשכת עורכי הדין, התגלו ליקויים באופן הפעולה של קומסיין וההוצאה לאור, באופן שעומד בסתירה להסדרה החוזית והנהלית, שהיו תנאי לאישור. הליקויים התגלו הן במישור דרישות אבטחת המידע מהמחשב המשמש להנפקה, והן באופן ההתקנה של הכרטיסים החכמים שעל גבם הונפקו התעודות האלקטרוניות לעורכי דין. על רקע ממצאי הפיקוח לא הוארך האישור בספטמבר 2008 עד לביצוע פיקוח נוסף שבו הוצג תיקון הליקויים. בעקבות הפיקוח שונה אופן ההתקנה של הכרטיסים החכמים לעורכי דין. הממצאים לא היו במחלוקת ובעקבותם התקבלה התחייבות אישית של מנכ"ל קומסיין ושל מנכ"ל ההוצאה לאור, כי בחנו את ממצאי הפיקוח.

בעקבות זאת הוארך באוקטובר 2008 האישור לשיתוף הפעולה בין לשכת עורכי הדין לחברת קומסיין עד 01.06.09. לאחר תקופת הדו"ח, ובעקבות ממצאים חיוביים הוארך תוקף האישור עד סוף שנת 2009.

פעולות נוספות (שאינן פיקוח)

<u>הפעלת סמכות הרשם "לחתום" בחתימה משלו על תעודה אלקטרונית של גורם מאשר.</u>

במהלך שנת 2008 הוחל בצעדים מעשיים להפעלת הסמכות המוקנית לרשם בסעיף 12 לחוק לחתום בחתימה אלקטרונית מאובטחת את התעודות האלקטרוניות המשמשות גורמים מאשרים.

נושא זה מקובל בחלק ממדינות אירופה ובמסגרת מערך האמון המשמש עובדי מדינה בארה"ב, והינו בין ההמלצות שנדונו בועדה המייעצת לרשם. המטרה היא לייצר זיהוי טכנולוגי של הגורם המאשר, ולקבוע נהלים מחייבים באמצעות התשתית הטכנולוגית המקובלת. לאחר בדיקות שבוצעו, הכוונה היא להפעיל במהלך שנת העבודה 2009 מערך כאמור, אליו יוכפף כל גורם מאשר המנפיק תעודות לפי החוק.

<u>חתימה אלקטרונית מאובטחת</u>

במהלך שנת 2008 ובתחילת שנת 2009 התעוררה אי בהירות בהקשר של תקנות מס הכנסה (ניהול פנקסי חשבונות), לגבי חתימה אלקטרונית מאובטחת ומהותה. בנושא זה יפרסם הרשם במהלך שנת 2009 נייר עמדה מטעמו.

חקיקה והנחיות

במסגרת הטיפול השוטף בחוק ובתקנות נערכת על ידי הרשות בדיקה של הצורך להמליץ למחלקת ייעוץ וחקיקה במשרד המשפטים על תיקונים ושינוים בחוק ובתקנות. הנושאים המרכזיים הנבדקים:

<u>שיפור כלי אכיפה ופיקוח</u>

במהלך שנת 2008 התגלו מספר הפרות של הנחיות ונהלים על ידי הגורם המאשר, קומסיין. הסתבר כי בידי הרשם אין סנקציות יעילות, פרט להתליית רישום, כנגד הפרות אלה.

הגורם המאשר נקט סחבת בביצוע תיקוני ליקויים והנחיות הרשם, כאשר לרשם לא עמדו כלים יעילים ומרתיעים להגברת הציות. מאחר שכיום פועל רק גורם מאשר אחד, התליית רשיונו הינה בעלת השפעה מיידית לפרויקטים הנסמכים על חתימה אלקטרונית מאושרת, ולכן מחייבת זהירות מרובה.

<u>שינוי תקנות בתחום מכשירים השומרים על אמצעי חתימה</u>

תקנה 8 לתקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001 כוללת פירוט הדרישות לקיום חזקה של "חתימה אלקטרונית מאובטחת". במסגרת זו נדונה השאלה מה צריכות להיות דרישות המינימום מהתקן המשמש לאיפסון מפתח לחתימה אלקטרונית מאובטחת או מאושרת. התקינה המופיעה כיום בתקנה מציבה רף נמוך מדי, לדעת הרשם.

באיחוד האירופי הוחלט לקבוע כדרישה להתקן protection profile שנכתב לפי תקן ה- common criteria ברמה 4. בנוסף, כל ה- protection profile השונים שנכתבו להתקנים ולכרטיסים חכמים הם ברמה 4 לפחות. בועדה המייעצת לרשם הגורמים המאשרים שפעלה במשרד המשפטים בשנת 2004 נשמעה המלצה לקבוע את הדרישה מהתקן המשמש לחתימה אלקטרונית מאושרת לפי common criteria רמה 4 לפחות, ולא להפנות כלל לתקן fips.

בנושא זה מוצע לטפל בשנת 2009.

שינוי תקנות כתוצאה מהתפתחויות במחקר ההצפנה

חתימה אלקטרונית מבוססת על שימוש בישומים המבוססים על טכנולוגיות הצפנה מקובלות. ההתפתחויות בתחום מחקר ההצפנה ופריצת הצפנות, הביאו לדיון בדבר צורך בשידרוג טכנולוגי[17]. בימים אלה נערכת בדיקה בנושא זה עבור משרד המשפטים.

שינוי כללי זיהוי מבקשי תעודות אלקטרוניות

התקבלו תלונות ממבקשי תעודות שאין בידם רשיון נהיגה או דרכון ובשל כך נמנעת האפשרות להנפיק עבורם תעודה אלקטרונית.

דרישת הצגתם של שני מסמכי זיהוי המכילים את תמונתו של מבקש התעודה נסמכת על הרצון לקיים תהליך זיהוי פנים-אל-פנים אמין ככל האפשר. עקב קלות הזיוף של תעודת הזהות, יש צורך להסתמך על יותר ממסמך אחד נושא תמונה.

הפתרון אפשרי לבעיה זו[18] הוא בשינוי התקנות באופן שניתן יהא להסתמך על מסמכים נוספים נושאי תמונה ואמינים, כגון תעודות צבאיות או ממשלתיות.

עדכונים אודות חתימה אלקטרונית באירופה

כפי שצויין לעיל, החוק הישראלי מבוסס במידה רבה על תובנות מקובלות בעולם. בהקשר זה, בוצעה עבודת תקינה והסדרה משמעותית באיחוד האירופי על פי הדין האירופי, במסגרת קבוצות עבודה בארגון התקינה ETSI[19].

בהקשר זה, בשל הדמיון בין הדין האירופי לדין הישראלי, והאינטרס בתנועה חופשית של תקשורת, יזם משרד המשפטים עם מינהל סחר חוץ במשרד התעשייה המסחר והתעסוקה, שיתוף הפעולה בתחום זה מול האיחוד האירופי, ונושא זה נכלל גם במסגרת תוכנית הפעולה התלת שנתית של האיחוד האירופי מול ישראל.

הרשם הישראלי חבר כמשקיף לא פורמלי בארגון הוולנטרי של הרשויות המפקחות על החתימה האלקטרונית באירופה (FESA - Forum of European Supervisory Authorities). מדובר באותן רשויות פיקוח שהוקמו על פי הדירקטיבה האירופית במדינות אירופה. במסגרת ארגון זה נדונות סוגיות טכנולוגיות ומשפטיות העולות.

לישראל אינטרס גבוה להשתתף בדיונים הפנים אירופאים, מאחר וכך תתאפשר הערכות והתאמה מול ההתפתחויות בתחום באירופה והידע הנרכש בפורום עשוי לשמש לפיתוח המדיניות הישראלית הפנימית בנושא זה.

מהדיונים בפורום זה עולה כי במדינות רבות באירופה היישום של החתימה האלקטרונית, בפורמט הדומה לחוק הישראלי טרם זכה לתפוצה משמעותית. השימוש בפועל בחתימה אלקטרונית הוא בפרוייקטים ממשלתיים.

ניתן לומר כי יעד מרכזי במדיניות האיחוד בתחום זה (בשונה מהמדיניות בכל אחת מהמדינות) הינו לקדם את האחידות בתחום שירותי "ממשל מקוון" וחתימה אלקטרונית.

---

[17] ראו: ETSI, TS 102-176 Ver 2.0.0, Electronic Signatures and Infrastructures; Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, ("Algo" paper) באתר ETSI, לעיל.

[18] וזאת כל עוד לא הונפקה תעודת הזהות ה"חכמה" החדשה.

[19] ראו: http://portal.etsi.org/esi/el-sign.asp.

בנובמבר 2008 אימצה נציבות האיחוד האירופי "תוכנית עבודה בדבר חתימות אלקטרונית וזיהוי אלקטרוני לצורך אספקת שירותים ציבורים חוצי גבולות בשוק המשותף"[20] ("Action Plan on eSignatures and eIdentification to facilitate the provision of cross-border public services in the Single Market").

מטרת תכנית העבודה לאפשר אספקת שירותים ציבורים באמצעות האינטרנט, על בסיס **חתימות אלקטרוניות (e-signature) וזיהוי אלקטרוני (e-identification)**, בעלי תוקף כלל-אירופאי, ולא רק תוקף בכל אחת מהמדינות.

בהקשר של חתימות אלקטרונית, מבקשת תוכנית העבודה ליצור תשתית אחידה לשימוש בחתימות אלקטרוניות מצד אחד ופיתוח שירותים המסתמכים על חתימות אלקטרוניות מצד שני, במדינות השונות, תוך יצירת בסיס משפטי משותף של הכרה בחתימות אלקטרוניות.

מהלך זה מבוסס ברובו על ממצאי מחקרים מקיפים בדבר הקשיים בפני הטמעה של חתימה אלקטרונית במדינות אירופה. נציבות האיחוד האירופי ביצעה מחקרים בנושא זה וכן מיפוי הפערים בין המדינות השונות, לצורך התמודדות עם סוגיה זו על מנת לקדם שימוש בחתימה אלקטרונית "כלל אירופאית"[21].

התכנית השנתית בתחום החתימה האלקטרונית ברמה הגבוהה (המקבילה לחתימה אלקטרונית מאושרת) כוללת בין היתר את הרכיבים הבאים:

1. זיהוי סטנדרטים של מוצרים בתחום החתימות האלקטרוניות, וניתוח האפשרות להרחיב את קו המוצרים מעבר לזה המאושר כיום על ידי הנציבות.

2. עריכת רשימה מפוקחת של כל ה- "גורמים המאשרים" המאושרים לפי הדירקטיבה האירופית. (Qualified Certification Service Providers).

3. קביעת קווי יסוד והכוונה של הצרכים על מנת לתמוך בהטמעות של החתימות המוכרות על פי הדירקטיבה האירופית.

בתחום החתימה האלקטרונית ברמה הנמוכה יותר, המקבילה לחתימה אלקטרונית מאובטחת, מכירה הנציבות בערך הרב של מוסד זה, ובשימוש בו, ולכן מבקשת גם כן להסדיר קווים טכנולוגים מנחים למימושו.

יש לציין כי בנציבות האיחוד האירופי מתנהל פרוייקט נסיוני רחב היקף לשימשו בחתימה אלקטרונית בין מדינות אירופאיות שונות, בתחום הרכש הממשלתי.[22] על פי הדירקטיבות החלות על תחום זה נדרש שימוש בחתימה אלקטרונית לצורך הגשת הצעות מקוונות.

מחברי התכנית מציינים כי היא אמנם מתמקדת בזיהוי אלקטרוני וחתימות אלקטרוניות לשימוש באפליקציות ממשלתיות ברשת, אך הצפי הוא שפעילות זו תשמש בסיס גם לפיתוח גם בסקטור הפרטי.

---

20 לדיווח כללי ראו: http://ec.europa.eu/idabc/en/document/7768. לתוכן ההחלטה, ראו: Action Plan: on eSignatures and eIdentification to facilitate the provision of cross-border public services in the Single Market – COM (2008) 798 final.,

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

21 ראו: http://ec.europa.eu/idabc/en/document/6485

22 http://ec.europa.eu/idabc/en/document/2084/5874

נספח - אופן הפעלת סמכויות הפיקוח בחברת קומסיין

כנדרש בתקנה 16 לתקנות חומרה ותוכנה, מפורטות להלן אופן הפעלת סמכויות הפיקוח לפי התקנות השונות בתקופה הנסקרת.

תקנה 2. תקן

נוסח התקנה:

"גורם מאשר יקבל מאת מכון התקנים או מאת מי שאושר לעניין זה לפי סעיף 12 לחוק התקנים קודם לתחילת פעילותו לפי החוק תעודת בדיקה בדבר התאמה לת"י 7799, חלקים 1 ו-2, ויעמוד בתקן במשך כל זמן פעילותו."

בהתאם למידע שהתקבל ממכון התקנים, תוקף ההסמכה לתקן ישראלי 7799 הסתיים ביוני 2008, והחל ממנו תתחייב עמידה בתקן ישראלי 27001. אף כי הודעה מתאימה פורסמה על ידי הרשם ונמסרה לחברת קומסיין זמן רב מראש, לא עמדה חברת קומסיין במועד שנקבע, ולאחר משלוח התראות ובטרם נקיטת אמצעים, השלימה את הערכותה, וזאת לאחר המועד שנקבע לתפוגת האישור.

תקנה 3. זמינות

נוסח התקנה:

"גורם מאשר ידאג להבטיח כי במערכות הדרושות לבדיקת מאגרי תעודות בטלות ועדכון תתקיים בכל עת רמת זמינות גבוהה להנחת דעתו של הרשם."

במהלך שנת 2008 ארע מקרה בו מאגר התעודות הבטלות של הגורם המאשר לא עודכן בהתאם לכללים החלים על הגורם המאשר. תחקור האירוע בידי חברת קומסיין ובידי הרשם העלה כשל אנושי ארגוני בתפקוד הגורם המאשר.

תקנה 4. אמצעי החתימה של הגורם המאשר

נוסח התקנה:

"גורם מאשר ישתמש באמצעי חתימה שמתקיימים בו לפחות כל אלה:

(1) הוא מבוסס על מפתח RSA או DSA באורך 2048 סיביות לפחות או ECDSA באורך 160 סיביות לפחות.

(2) הוא מוגן באמצעי שמתקיימות בו לפחות דרישות האבטחה של FIPS 140-2 רמה 2.

(3) הוא מגובה באמצעים מוגנים ומאובטחים להנחת דעתו של הרשם. הגיבוי יישמר בנפרד.

(4) דרישות נוספות שהעמיד הרשם לשם קיום אבטחה ברמה סבירה מפני חדירה, שיבוש או שימוש לרעה."

בבדיקה שגרתית התברר לרשם כי קומסיין החליטה על דעת עצמה שאחד השרתים המשמשים להנפקת תעודות אלקטרוניות יהיה כזה העושה שימוש באורך מפתח שהינו באורך 1024 סיביות במקום 2048 ביט, וזאת בניגוד לתקנה 4 לתקנות. זאת בשל עמדתה, ולפיה דרישת התקנות חלה רק על מפתח "שורש" ולא על אמצעי החתימה המשמש לחתימה על תעודות אלקטרוניות לפי החוק בפועל.

עמדה זו לא נתקבלה ע"י הרשם הן ברמה המשפטית והן ברמה הטכנולוגית. זאת משום שדרישת התקנות הינה לחוזק קריפטולוגי בכל רכיבי השרשרת המזהה את הגורם המאשר, וחוזקה כחוזק החוליה החלשה. על כן הנחה להפסיק להשתמש באופן מיידי בשרת זה כשרת הנפקה. נכון למועד הגשת דו"ח זה, כעולה מממצאי הפיקוח בקומסיין, קומסיין פועלת על פי הנחייה זו.

כמהלך משלים הרשם דרש מקומסיין לבטל את התעודות שהונפקו על ידי שרת 1024 סיביות, באופן שיאפשר ביטול תעודת שרת זה שהינה בניגוד לתקנות, ולסגירתו של שרת 1024 באופן סופי, באופן שיפסיק לפרסם גם רשימת תעודות בטלות. על מנת למנוע פגיעה בעסקיה של קומסיין ובלקוחותיה, הסכים הרשם לפתרון שהוצע על ידי קומסיין, של החלפה אוטומטית, בתהליך שיאושר, של תעודות אלו בתעודות שיונפקו משרת 2048 סיביות. קומסיין התחייבה לסיים פעילות זו עד לסוף שנת 2008. יחד עם זאת, הפיתוח שנדרש לשם כך הושלם ע"י קומסיין רק בפברואר 2009. הפיתוח שהוצג לבסוף לא היה בטוח דיו לדעת הרשם ויועץ האבטחה שלו, ובעקבותיו נדרשו תיקונים נוספים בהליך. אישור סופי של הרשם לתהליך ההחלפה המוצע ניתן רק לאחר תקופת הדוח, ביוני 2009.

תקנה 5. אבטחת מרכיבי המערכת ואמצעי התקשורת

נוסח התקנה:

"(א) מרכיבי המערכת המשמשים לזיהוי המבקש, להנפקת תעודה אלקטרונית ולביטולה (להלן – פעולות חיוניות) יעמדו ברמת ביטחון של תקן common criteria EAL4 או לפי תקן מקובל אחר המבטיח רמת אבטחה מקבילה להנחת דעתו של הרשם.

(ב) אמצעי התקשורת המשמשים לפעולות חיוניות של הגורם המאשר יעמדו בדרישות אבטחה גבוהות להנחת דעתו של הרשם."

במהלך שנת 2008, עקב פיקוחים חוזרים בקומסיין, שהעלו ממצאים מדגמיים מטרידים בתחום אבטחת המידע, דרש הרשם מקומסיין לערוך סקר סיכונים בלתי תלוי ומקיף למערכות באמצעות יועץ חיצוני. סקר כאמור נערך על ידי מומחה שנבחר על ידי קומסיין. ממצאיו של סקר זה נמסרו לרשם. יועץ האבטחה של קומסיין מצא שורה של ליקויי אבטחה, ונתן המלצות מקיפות לתיקונם. קומסיין התחייבה לתקן את הליקויים ואף הציגה לרשם מצגים לפיהם התוכנית בביצוע ותושלם תוך זמן קצר. בפיקוח שנערך בסוף דצמבר 2008 התברר כי למרות התחייבויות קומסיין לתיקון הליקויים לא הושלם תיקונם במלואו, ואף לא הוחל בחלק מהתיקונים שהוצגו כתיקונים בעבודה. רק בעקבות הערות הרשם בפיקוח, לאחר חודש פברואר 2009, הוחל בביצוע מלוא התיקונים. בבדיקת ביניים שנערכה במרץ 2009, ניתן היה להתרשם משיפור משמעותי של מערך אבטחת המידע.

תקנה 6. אבטחה פיזית

נוסח התקנה:

"גורם מאשר יבטיח כי חלקי המערכת החיוניים לפעילותו כגורם מאשר (להלן – "החלקים החיוניים") יישמרו במקום מוגן המונע חדירה וכניסה בלא הרשאה והתואם את אופי פעילותו של גורם מאשר להנחת דעתו של הרשם."

נכון למועד הגשת דוח זה, ועל פי דיווח של מבקר אבטחת המידע ביחס לפעילות החברה, ליקויים שהיו בנושא זה בעבר תוקנו.

תקנה 7. בקרת גישה והפרדת תפקידים

נוסח התקנה:

(א) "גורם מאשר יבטיח כי ביצוע הפעולות החיוניות לא יהא בשליטתו של אדם אחד בלבד

(ב) גורם מאשר יבטיח את מידור הגישה לחלקים החיוניים כך שלאותו אדם לא תהא גישה לכל החלקים החיוניים."

במהלך שנת 2008 התרחשה בקומסיין תקלה ביום שבתון, והתקלה תוקנה על ידי אדם אחד בלבד. במסגרת תיחקור האירוע התברר כי הגישה למערכת החיתום של קומסיין הוגדרה באופן שגם אדם אחד בלבד יכול לגשת אליה. זאת למרות שלצד הוראת התקנה, גם נהלי החברה חייבו גישה על ידי שני אנשים. גם בעת הביקורות הוצגה תמיד גישה של שני אנשים למערך זה, למרות שכאמור התברר בדיעבד, כי ניתן היה להפעיל את המערך באמצעות אדם אחד בלבד. לפי הצהרת מנהל האבטחה של קומסיין, נושא זה תוקן.

תקנה 8(1)(ג). חזקה לענין חתימה אלקטרונית מאובטחת

נוסח התקנה:

"חתימה אלקטרונית שמתקיים בה אחד מאלה, חזקה שהיא חתימה אלקטרונית מאובטחת:

(1) לגבי אמצעי לאימות החתימה שמחזיק בידיו המבקש, ואמצעי אימות החתימה שאותו הוא מזהה, מתקיימות לפחות הדרישות כמפורט להלן:

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

עד היום לא התבקש הרשם להפעיל את סמכותו לקביעת דרישות חלופיות לסיסמא לפי התקנה הנ"ל.

עם זאת, במסגרת תיקון נהלים של הגורם המאשר, וכן אישור פעולת ההוצאה לאור של לשכת עורכי הדין, ובהתאם למקובלות בתחום זה, הנחה הרשם כי אורך סיסמת הגישה יהיה **לפחות 6 תוים.** במסגרת ביקורת שנערכה בהוצאה לאור של לשכת עורכי הדין התברר כי הונפקו כרטיסים חכמים שלא על פי הנחיה זו. על פי הוראת הרשם, ליקוי זה תוקן על ידי ההוצאה לאור.

תקנה 9. אישור לעניין חתימה אלקטרונית מאובטחת.

"(א) מי שמעוניין בכך רשאי לפנות בכתב לרשם לשם קביעה –

(1) אם טכנולוגיה מסוימת עומדת בדרישות שנקבעו בתקנה 8(1), פניה כאמור תכלול מסמכים המתארים את הטכנולוגיה לרבות תעודת התאמה לתקן מקובל אם ישנה וחוות דעת של מומחה אבטחת מידע בדבר אמינותה של הטכנולוגיה, הרשם רשאי לדרוש כל מידע אחר הדרוש לו כדי לבחון אם מדובר בטכנולוגיה העומדת בדרישות תקנה 8(1) וכדי לאשרה.

(2) כי טכנולוגיה מסוימת מפיקה חתימה אלקטרונית שחזקה שהיא חתימה אלקטרונית מאובטחת אף שאין מתקיימות בה הוראות תקנה 8(1), פניה כאמור תכלול מסמכים כאמור בפסקה (1).

(ב) אישר הרשם לפי תקנת משנה (א) כי חזקה שחתימה אלקטרונית מסוימת היא חתימה אלקטרונית מאובטחת, יפרסם ברשומות את דבר אישורה של הטכנולוגיה שלגביה אישר כאמור, נוסף על כך ינהל הרשם רשימה מעודכנת של טכנולוגיות שקיבלו את אישורו באתר האינטרנט המשמש לכך."

בשנת 2007 הוגשו לרשם שתי בקשות בנושא זה. ככלל, מוצרים המשמשים לביצוע פעולות הצפנה, והמחזיקים מידע רגיש, כגון חתימה אלקטרונית, נדרשים לעבור הסמכה במכון תקינה לפי תקני אבטחת מידע מקובלים, ובראשם ISO 15408, וכן תקן של ארגון NIST האמריקאי, מסדרת FIPS. הבדיקות לפי תקנים אלה מחייבות תשתיות בדיקה ממוסדות, ידע והכשרה, שאינן מצויות במלואן בשוק האזרחי במדינת ישראל. בהתאם לכך, עמדת הרשם היא כי ככלל יש להסתמך על אישורים שניתנים ממוסד מוכר בחו"ל בהתאם לתקנים אלה.

בנושא זה נערכת בדיקה נוספת בידי הרשם לעניין אופן מימוש הסמכות הנתונה בתקנה זו על רקע האמור.

תקנה 10(2). זיהוי המבקש

נוסח התקנה:

"10. לא ינפיק גורם מאשר תעודה אלקטרונית אלא לאחר שאימת את זהות המבקש כמפורט להלן:

(1) הגורם המאשר, או נציגו או שליח מטעמו שאישר הרשם ובתנאים שקבע באישור, זיהה פנים אל פנים את המבקש, ואם היה המבקש תאגיד — את מורשה החתימה מטעם התאגיד;

(2) הגורם המאשר יאמת את פרטי הזיהוי של המבקש:

(א) ביחיד שהוא תושב ישראל — על פי תעודת זהות, וכן על פי דרכון ישראלי תקף או רישיון נהיגה

ישראלי תקף עם תמונה או על פי מידע שהתקבל ממרשם האוכלוסין במשרד הפנים (להלן — מרשם האוכלוסין); הרשם רשאי להורות, בהתחשב בעלות קבלת המידע ובתועלת העשויה לצמוח ממנו, כי האימות בהתאם לפסקת משנה זו, לגבי כלל התעודות האלקטרוניות או לגבי תעודות אלקטרוניות מסוימות, יתבצע על פי מידע שהתקבל ממרשם האוכלוסין; בפסקת משנה זו, "מידע שהתקבל ממרשם האוכלוסין" — הפרטים שדרש הרשם, כולם או חלקם, מבין אלה: מספר הזהות של המבקש, שם משפחתו ושם משפחה קודם, אם ישנו, שם פרטי, שם האב, שם האם, שנת לידה, תאריך הנפקת תעודה אחרון, סיבת הנפקת התעודה, מען נוכחי, אם ישנם — סטטוס פטירה ותאריך פטירה;

(ב) ביחיד שהוא תושב חוץ — על פי דרכון חוץ או תעודת מסע או תעודת זהות, וכן על פי מסמך זיהוי נוסף הנושא תמונה של המבקש ופרטים מזהים שלו ושל מי שהנפיק את המסמך הנוסף;

(ג) בתאגיד הרשום בישראל — על פי תעודת הרישום, אישור של עורך דין על קיומו של התאגיד, שמו ומספרו הרשום, או במקום אישור של עורך דין כאמור — על פי אימות במרשמים המתאימים, וכן על פי העתק מאושר של החלטת האורגן המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד, או אישור של עורך דין על מורשה החתימה כאמור;

(ד) בתאגיד שאינו רשום בישראל — על פי העתק מאושר ממסמך המעיד על רישומו, אישור של עורך דין על קיומו של התאגיד, שמו ומספרו הרשום, או במקום אישור של עורך דין כאמור — על פי אימות במרשמים המתאימים, וכן על פי העתק מאושר של החלטת האורגן המוסמך בתאגיד בדבר מורשה החתימה מטעם התאגיד או אישור של עורך דין על מורשה החתימה כאמור;

(ה) במוסד ציבורי — על פי הצהרת המבקש, לאחר שהגורם המאשר נוכח, על פי מסמך, כי מורשה החתימה מוסמך לפעול בשם המוסד הציבורי; לענין פסקה זו, "מוסד ציבורי" — משרדי ממשלה, רשויות מקומיות, וכן רשויות, תאגידים או מוסדות אחרים שהוקמו בישראל לפי חיקוק;

(3) לענין פסקאות משנה (ג) עד (ה) שבפסקה (2) — יזהה הגורם המאשר את מורשה החתימה לפי הוראות פסקאות משנה (א) או (ב) שבאותה פסקה, לפי הענין;

(4) לענין פסקאות משנה (ד) ו-(ה) שבפסקה (2), "העתק מאושר" — העתק מתאים למקור המאומת בידי אחד מאלה:

(א) הרשות שהנפיקה את מסמך המקור;

(ב) עורך דין בעל רישיון לעריכת דין בישראל;

(ג) נציג דיפלומטי או קונסולרי ישראלי בחוץ לארץ."

בהחלטתו מיום 1.1.03 הורה הרשם לגורמים המאשרים לזהות יחידים שהנם תושבי ישראל על סמך מידע שהתקבל ממרשם האוכלוסין.

בדצמבר 2008 גובשה הנחיית ביניים בתיאום עם קומסיין לזיהוי ביחס ליחידים שבהם יש אי התאמה חלקית בפרטי רישום, והנחייה זו תעודכן בתקופה הקרובה.

תקנה 12. זיהוי לצורך הנפקת תעודה אלקטרונית חדשה

"בהנפקת תעודה אלקטרונית חדשה, על סמך תעודה אלקטרונית שטרם פג תוקפה, יכול גורם מאשר לנקוט הליכי זיהוי שונים מאלה האמורים בתקנה 10, ובלבד שהרשם אישר הליכים כאמור."

במסגרת סמכותו הנ"ל אישר הרשם לקומסיין לנקוט בהליך זיהוי שונה מזה האמור בתקנה 10 בעת חידוש תעודה אלקטרונית תקפה. במסגרת הליך הזיהוי המתוקן אושר שימוש באמצעי זיהוי חלופיים במקום זיהוי המבקש פנים אל פנים. מבירור שנערך עם חברת קומסיין, בשנת 2008 לא היה שימוש בנוהל זה. הרשם בוחן תיקון לאישור שניתן.

תקנה 15. שינוי תקן

"(א) הוחלף תקן מן התקנים הנזכרים בתקנות אלה, לרבות מסמך RFC, בתקן או מסמך חדש, לפי העניין, יהיו התקן או המסמך החדש מחייבים במקביל לתקן או המסמך הישן, זולת אם אין עוד בתקן או במסמך הישן כדי להבטיח תנאי אבטחה נאותים להנחת דעתו של הרשם, שאז יחייב התקן או המסמך החדש בלבד, בתוך זמן שיורה הרשם".

(ב) הרשם יודיע לגורמים המאשרים על שינוי תקן או מסמך RFC מחייב כאמור בתקנת משנה (א) ויפרסם באתר האינטרנט שיועד לכך רשימה מעודכנת ש להתקנים והמסמכים המחייבים לפי תקנות אלה."

בהחלטתו מיום 18.2.04 קבע הרשם כי המסמך RFC 2527 שלפיו יש לערוך מסמך נהלים של גורם מאשר כאמור בתקנה 1 לתקנות יוחלף החל מיום 1.3.04 במסמך חדש המסומן RFC 3647 . בנוסף, כאמור נמסרה הודעה על פי תקנה זו כי עד ולא יאוחר מ– 30.06.08 על גורם מאשר להציג תעודה על התאמה לתקן ישראלי 27001, במקום ההתאמה לתקן ישראלי 7799.

כמו כן נבדקות התפתחויות בתחום ההצפנה ואבטחת המידע לצורך בחינת סוגיית עדכון ההנחיות בנושא זה בתקנות ועל פיהן.

דין וחשבון של רשם שירותי נתוני אשראי ושירותי מידע על עוסקים לשנת תשס"ח-2008

דין וחשבון אודות פעולות הרשות למשפט, טכנולוגיה ומידע בשנת 2008

מבוא

להלן פירוט הפעילויות ברשות במסגרת הפעלת סמכויות רשם שירותי נתוני אשראי ושירותי מידע על עוסקים (להלן - **הרשם**) מכוח חוק שירות נתוני אשראי, התשס"ב-2002 (להלן - **החוק**) ותקנות שירות נתוני אשראי, התשס"ד-2004 (להלן - **התקנות**).

מתן רישיונות

במהלך 2008 המשיך הליך בדיקת הבקשה לרישיון שירות נתוני אשראי של חברת לב אמון בע"מ, כולל מספר ביקורים במתקני החברה. ביום 14.8.08 ניתן לחברת לב אמון רישיון שירות נתוני אשראי המוגבל לאיסוף נתונים בלבד, ואוסר על מסירתם, עד להשלמת בדיקות הרשם ומתן אישור מפורש למסירת מידע.

התקבלו מספר פניות של גורמים אשר הביעו עניין בקבלת רישיון שירות נתוני אשראי, עם זאת עד כה לא הוגשה בקשה מסודרת לרישיון.

פיקוח על בעלי הרישיונות

<u>בי די איי ביזנס דאטה ישראל בע"מ</u> - נערכה ביקורת שירות נתוני אשראי. במהלך הביקורת נבדק מערך אבטחת המידע והיבטים מסוימים לגבי הפעלת השירות. לא נמצאו ליקויים מהותיים.

<u>סי אי איי בע"מ</u> - נערכו מספר ביקורות אבטחה פיסית במשרדי החברה, היות והמשרדים הועברו למיקום חדש. ליקויים שזוהו במהלך הביקורות תוקנו על ידי בעל הרישיון.

טיפול בתלונות

במהלך 2008 הוגשו תלונות בודדות מהציבור כלפי בעלי הרישיונות. בכולן נמצא שהרקע לתלונה הוא אי הבנת ההסדר בחוק על ידי המתלונן.

הנחיות הרשם

ביום 24.1.08 פורסמה הנחיית הרשם מס' 2/2008 שעניינה אופן הטיפול בבקשות לתיקון מידע על ידי בעל רישיון שירות נתוני אשראי לפי סעיף 31 לחוק.

<u>ליווי הליכי תיקון החוק והתקנות</u> - במהלך הדיונים לגבי תיקון החוק והתקנות במשרד המשפטים ובוועדת הכלכלה בכנסת נכח הרשם ו/או נציגיו.

<u>תשלום לתאגידים הבנקאיים</u> - בינואר 2008 הוציא הרשם דרישה לשניים מבעלי הרישיונות (חברות בי.די.איי ביזנס דאטה ישראל בע"מ ודי. אנד בי. החברה לנתוני אשראי בע"מ) לבצע את התשלום הנדרש לתאגידים הבנקאיים המעבירים אליהם מידע, וזאת על פי פרק ח' לתקנות.

על דרישה זו השיגו שני בעלי הרשיונות. במהלך השנה בחן הרשם את טענות בעלי הרישיונות ותגובת איגוד הבנקים עד שמסר לצדדים הכרעתו בנובמבר 2008, לפיה על בעלי הרשיונות לשלם את הנדרש לתאגידים הבנקאיים. על הכרעה זו הוגשה עתירה לביהמ"ש העליון כשבתו כבג"ץ ביום 2.2.09 והיא נדונה בימים אלה.