לשכת עורכי הדין בישראל
ISRAEL BAR ASSOCIATION
نقابة المحامين في إسرائيل

ועדת הגנת הפרטיות

ת"א, י' בטבת התשע"ז
08/01/2017

לכבוד
חה"כ ניסן סלומיאנסקי
יו"ר ועדת החוקה, חוק ומשפט
כנסת ישראל

שלום רב,

הנדון: <u>טיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ו-2016</u>

<u>נייר עמדה לקראת הדיון הקבוע ליום 10/01/17</u>

בשם הוועדה להגנת הפרטיות בלשכת עורכי הדין (להלן- "**הוועדה**") הננו מתכבדים להעביר את הערותינו לטיוטת התקנות שבנדון כדלקמן:

<u>מבוא</u>

1. תקנות הגנת הפרטיות (אבטחת מידע) (להלן- "**התקנות**") המוצעות בטיוטה אשר פורסמה על-ידי שרת המשפטים, נועדו לקבוע הסדר מקיף ומפורט מההסדר הנוכחי העוסק בהגנה על מאגרי מידע. ההסדר בא להתאים את המציאות החקיקתית להתקדמות הטכנולוגית בתחום.

2. התקנות מותקנות מכוח חוק הגנת הפרטיות, התשמ"א-1981 (להלן- "**החוק**"), אשר קובע הוראות שונות וחובות המוטלות על בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע. אחת החובות המרכזיות היא חובת אבטחת המידע, שמטרתה צמצום החשש מפני שימוש לרעה או פגיעה בשלמות המידע.

כך סעיף 17 לחוק קובע כי:

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

ואילו "אבטחת מידע" מוגדרת בסעיף 7 לחוק באופן הבא:

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

רח' דניאל פריש 10, תל-אביב 64731, טל. 1-599-500-606 פקס. 03-6918696
רח' שופן 1, ירושלים 92190, טל. 1-599-500-606, פקס. 02-5610062
http://www.israelbar.org.il - E-mail: vaadmerkazi@israelbar.org.il

עינינו הרואות כי בהוראות ובהגדרות אלה לא די ויש מקום לפרט את החובה המוטלת על בעל ומחזיק במאגר מידע. זו מטרת התקנות ויש לברך על כך.

3. התקנות החדשות כוללות מנגנונים וכלים פנים ארגוניים שמטרתם להמחיש את חובתם ואחריותם של ארגונים בתחום אבטחת מידע אישי, ולהנחיל עקרונות אבטחת מידע בתוך הארגון. מטרת ההסדר המוצע היא מימוש תכליות החוק, כלומר, הגנה על זכויות נושאי המידע במאגר המידע מפני שימוש לרעה במידע אודותיהם, הן על ידי גורמים מחוץ לארגון והן על ידי העובדים. ניתן לומר כי עמידה בעקרונות המוצעים בתקנות אלה, תבטיח כי ניהול המידע בארגון יהיה תקין.

4. **כפי שנראה להלן, אנו סבורים כי יש לברך על היוזמה להתקין תקנות חדשות בנושא אבטחת המידע ויותר מכך, כי טיוטת התקנות המונחת על שולחן הוועדה ראויה. במסמך זה להלן ננסה להביא הצעות לתיקונים בנוסח המוצע, הצעות שהן בבחינת הצעה להשביח את התקנות המוצעות, אשר, כאמור, ראויות אף בנוסח המוצע.**

<u>בקצירת האומר</u>

5. כאמור, הלשכה רואה בהתקנת התקנות החדשות צעד נדרש ומבורך. ההתקדמות הטכנולוגית בנושא מאגרי המידע הביאה עמה מנגנונים חדשים לשמירה על מידע, וראוי שמנגנונים אלו יוסדרו בחקיקה. מעבר לכך, ההתקדמות הטכנולוגית והתפיסתית יצרה חסרים משפטיים רבים בהסדר הנוכחי אשר קבוע בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו- 1986 (להלן- "**ההסדר הנוכחי**").

6. עם זאת, כאמור, יש מקום להציע מספר תיקונים לנוסח התקנות המוצע. כך יש מקומות בהם התקנות מנוסחות בצורה כללית, כאשר במספר לא מבוטל של סעיפים, חלקם מהותיים מאוד, ישנו שימוש במושגי שסתום רבים אשר עלולים ליצור חסר משפטי בתקנות. בהתאם לכך, הצענו להרחיב את המפורט בתקנות וזאת על-מנת שהסעיפים לא יוכלו להשתמע לשני פנים.

<u>הערות הוועדה לטיוטת התקנות</u>

7. תקנה 2 המוצעת מחייבת קיומו של "מסמך הגדרות" אשר יכלול מספר הגדרות בסיסיות בנוגע למאגר המידע. סעיף קטן (6) לתקנה קובע כי יש לפרט במסמך את הסיכונים העיקריים באבטחת המידע, ואופן ההתמודדות עימן. לטעמנו, קביעה כי בעל המאגר

יצטרך להעריך לבדו את הסיכונים משיתה אחריות כבדה מידי על בעלי המאגרים. הצעתנו היא שהתקנות ייפרטו סיכוני אבטחה מסוימים וקבועים שתהא חובה להכניס התייחסות אליהם ל"מסמך ההגדרות", וכי בעל המאגר יוכל להוסיף על אותם הסיכונים. בהמשך לכך המאגר יצטרך להציע פתרונות לכלל הסיכונים שהועלו.

8. תקנה 3 המוצעת עוסקת במינוי ממונה על אבטחת מידע כחלק מבעלי התפקידים במאגר. מספר הערות ביחס לכך:

א. סעיף קטן (1) לתקנה 3 קובע כי הממונה יהיה כפוף ישירות למנהל המאגר או למנהל פעיל מטעם בעל המאגר או המחזיק בו. לטעמנו, הסעיף יוצר מצב מסוכן מאחר ועבודת הממונה תחת סמכויות אלו עלולה להביא לניגוד עניינים חריף. הסיכון טמון בכך שהממונה יתקשה לעתים לבצע את עבודתו באופן אובייקטיבי וישר, לאור העובדה שהאחראי עליו הוא מנהל המאגר או מנהל פעיל מטעם בעל המאגר. אנו מציעים כי הממונה על אבטחת המידע במאגר לא יחויב להיות כפוף לאותם הגורמים שצויינו, אלא יהיה לכל הפחות באותה רמה הירארכית כמוהם.

ב. הסעיף אינו קובע איזו הכשרה מתאימה (כנדרש בסעיף 17ב לחוק) תהיה לממונה על אבטחת המאגר. אנו מציעים ללמוד וליישם מן ההסדר אשר נקבע בתקנות שוויון זכויות לאנשים עם מוגבלות (התאמת נגישות לשירות), תשע"ג-2013, הסדר אשר קבע כי כל "רכז נגישות", אשר ימונה בגוף מסוים, יצטרך להיות בעל ניסיון מסוים בנגישות או שיצטרך לעבור השתלמות רכזי נגישות. ניתן להקיש מתקנות השוויון שהוזכרו, ולקבוע כי ממונה אבטחת מידע יהיה בעל ניסיון של שנה באבטחת מידע, או שיצטרך לעבור השתלמות מסוימת לשם קבלת כלים שיעזרו לו בתפקידו.

ג. הסעיף אינו קובע הוראות לגבי גופים אשר באמתחתם יותר ממאגר מידע אחד תוך התייחסות פרטנית לכך.

ד. סעיף קטן (3) לתקנה 3 קובע כי הממונה יכין "תכנית בקרה שוטפת" לצורך עמידה בתקנות. נראה כי מדובר בדרישה כללית ולאקונית, ויש לפרט בתקנות את עיקרי תכנית הבקרה אשר על הממונה לנסח.

9. תקנה 5 המוצעת קובעת חובות מסוימות שיש לבצע לשם הערכת סיכוני אבטחה:

א. סעיף קטן (ב) מחייב קיום "סקר סיכונים" במאגר בעל רמת אבטחה גבוהה, אחת לשמונה עשר חודשים, לשם הערכת סיכונים דינאמית. עם זאת, אין פירוט על אופן ביצוע הסקר ועל זהותו של הסוקר. לטעמנו, יש לקבוע בתקנות הוראות אופרטיביות לגבי התשתיות המערכתיות שיש לבדוק כחלק מביצוע הסקר, ובנוסף, יש לקבוע מי אמון על ביצוע הסקר, כאשר ההעדפה תהיה סקירה על-ידי גוף חיצוני ולא סקירה פנימית.

ב. סעיף קטן (ג) מחייב "מבחני חדירות" למאגר בעל רמת אבטחה גבוהה, אחת לשמונה עשר חודשים. הצעתנו היא להגדיר במפורש כי מבדקי החדירות יהיו לגבי חדירות פיזית לתשתיות המאגר וכן מבדקי חדירות טכנולוגיות. כפי שהוסבר בסעיף האחרון, אנו מציעים בנוסף לציין בסעיף את זהות עורך המבדקים (בעדיפות לבודק חיצוני).

10. תקנה 14 המוצעת קובעת הוראות בעניין מאגרים המחוברים לרשת האינטרנט:

א. סעיף קטן (א) קובע שחיבור מאגר לרשת האינטרנט או לרשת ציבורית אחרת לא ייעשה אלא אם יותקנו "אמצעי הגנה מתאימים" מפני חדירה או תוכנות זדוניות. אנו גורסים שיש לקבוע בתוספת לתקנות מה הן אמצעי ההגנה המתאימים, כיוון והשארת הניסוח על כנו יותיר חופש פעולה נרחב מידי לבעלי המאגרים, אשר חלקם עלולים לחסוך בעלות אמצעי ההגנה, דבר העלול לפגוע באיכות ההגנה על המידע.

ב. סעיף קטן (ב) קובע כי העברת מידע מהמאגר דרך הרשת ייעשה תוך שימוש ב"שיטות הצפנה מקובלות". גם כאן, בדומה לטענה בסעיף 9א', אנו חושבים שיש לבצע רשימה מסודרת של אמצעי הצפנה מקובלים, על מנת לבטל את חופש הפעולה הניתן לבעלי המאגרים בנושא.

11. תקנה 16(א) המוצעת מחייבת ביצוע ביקורות, אחת לשנתיים, לאבטחת המידע במאגר שרמת אבטחתו בינונית או גבוהה. ישנה חשיבות עצומה לביצוע הביקורת, כיוון והיא זו המבטיחה את עמידת בעל המאגר בתקנות המוצעות. עם זאת, הסעיף מנוסח בצורה לאקונית, כאשר לא נקבע מי הוא זה שיבצע את הביקורת, ובנוסף, מה ההכשרה הנדרשת לאותו גורם המבצע את הביקורת. בהתאם לכך, אנו מציעים מספר שיפורים אשר יבטיחו כי הביקורות תהיינה מקצועיות ובעלות השפעה חיובית ככל האפשר:

א. יש לקבוע בתקנות כי הביקורת תתחלק לשניים: האחת, ביקורת טכנית-טכנולוגית שתבוצע על-ידי גורם בקי במערכות אבטחת מידע ומטרתה תהיה ווידוא עמידה בתקני האבטחה. השניה, ביקורת משפטית אשר תוודא עמידה בנהלי העבודה הנדרשים בתקנות.

ב. יש לקבוע כי הביקורת לא תהיה ביקורת פנימית אלא חיצונית, וזאת לשם הבטחת קיום ביקורת אובייקטיבית ככל הניתן.

ג. יש לקבוע כי בעל מאגר המידע/מנהל המאגר יחויב בשיתוף פעולה מלא עם עורך הביקורת. החובה לשיתוף פעולה תהיה לפני הביקורת עצמה (שליחת מסמכים וכדומה), ובמהלכה.

12. פרט 3(א)(1) לתוספת הראשונה בתקנות, קובע כי מאגר ברמת אבטחה בינונית יהיה בין היתר מאגר המכיל מידע על "צנעת חייו האישיים של אדם". מדובר בהגדרה קריטית אשר מבחינה בין מאגר רגיל למאגר באבטחה בינונית/גבוהה, אך עם זאת לא ניתן להבין באופן ברור את פירוש המונח. בהתאם לכך, יש לקבוע פירוש ברור וספציפי למונח "צנעת חייו האישיים של אדם".

<u>סיכום</u>

13. מטרתן של התקנות המוצעות הינה מבורכת, וכניסתן לתוקף בוודאי תגרום למהפכה חיובית בתחום אבטחת מאגרי המידע. התקנות המוצעות מתאימות את עצמן לעידן הטכנולוגי שבו אנו נמצאים, ויישומן יגרום לאזרחי המדינה, אשר חלק לא מבוטל ממנה "חבר" במאגר מידע כלשהו, להרגשת ביטחון גבוהה מבעבר.

14. עם זאת, עינינו הרואות כי יש לבצע שיפורים מסוימים בתקנות המוצעות. השיפורים המוצעים על-ידי הוועדה יביאו לאכיפה צודקת, להבנה מלאה של הוראות הסעיפים, ולצמצום אפשרות של "עיגולי פינות" מצד בעלי המאגר.

15. נשמח להרחיב בנושא בעת הדיון בתקנות בפני הוועדה הנכבדה.

בכבוד רב ובברכה,

דן חי, עו"ד
יו"ר הוועדה להגנת הפרטיות
לשכת עורכי הדין בישראל

<u>העתקים</u>:
עו"ד אפי נוה – ראש לשכת עורכי הדין.
מר אורי אלפרסי – מנכ"ל לשכת עורכי הדין.
עו"ד שלי ואקנין-אדם – ממונה תחום משפט חוקתי וזכויות אדם, לשכת עוה"ד.
עו"ד פנחס מיכאלי – ממונה תחום חקיקה, לשכת עוה"ד.
גב' דנית בוסקילה – מנהלת יחידת כנסת, לשכת עוה"ד.
חברי ועדת החוקה, חוק ומשפט, כנסת ישראל