

6 במרס 2017

ח' באדר תשע"ז

לכבוד	לכבוד
חה"כ עוה"ד רויטל סוייד	חה"כ ניסן סלומינסקי
ועדת החוקה, חוק ומשפט	יו"ר ועדת החוקה, חוק ומשפט
<u>הכנסת</u>	<u>הכנסת</u>

מכובדיי,

## הנדון: טיוטת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ו – 2016

אנו מבקשים לפנות אליכם בנושא שבנדון, כדלקמן:

1. בחודשים האחרונים דנה ועדת הכספים של הכנסת בטיטת התקנות שבנדון, אשר עוסקות בנושא בעל חשיבות רבה למערכת הבנקאית – הגנה על מאגרי המידע וניהולם. אין זה סוד שהמערכת הבנקאית משקיעה משאבים רבים מאוד בנושאי אבטחת מידע והגנת הסייבר, והיא עושה זאת בשיתוף פעולה הדוק מאוד ואינטנסיבי עם הפיקוח על הבנקים בבנק ישראל, שהוא הרגולטור המפקח באופן שוטף על מערכת הבנקאות.
2. איגוד הבנקים עצמו נטל חלק בשימוע הציבורי שערכה הרשות למשפט טכנולוגיה ומידע ("רמו"ט") בזמנו, ותיאר במפורט את הבעייתיות בהחלת התקנות האמורות על הבנקים, שהם גופים מורכבים מאוד אשר נתונים כבר כיום לרגולציה קפדנית, מדויקת וקשיחה של בנק ישראל בתחום אבטחת המידע, רגולציה המותאמת ספציפית למערכת הבנקאית ולאופייה המיוחד. יצוין כי במקרים רבים הוראות הפיקוח על הבנקים בתחום זה מהוות את "חוד החנית" של הרגולציה המתפתחת בתחום, ורגולציה זו במקרים רבים מחמירה מהתקנות המוצעות.
3. התקנות בהן עסקינן, כוללות סעיפים שאינם מתאימים, ואף חלקם יוצרים כפילויות ולעיתים סתירות לרגולציה הבנקאית המאוד מפורטת. בנושא כה רגיש ומורכב של אבטחת מידע, לא יכולה להיות מחלוקת שאין מקום למצב בו קיימת רגולציה כפולה באותו תחום בדיוק. רגולציה כפולה תביא בהכרח לאי סדר ולבלבול, ולטיפול לא יעיל ולא נכון בתחום זה.

4. על כן, סברנו, ואנו סבורים אף עתה, כי הסקטור הבנקאי צריך להיות מוחרג מלכתחילה מתחולת התקנות. אנו חושבים כי המנגנון להחרגת הבנקים לא צריך להיות, כפי שאולי ניתן לעשות זאת, באמצעות סעיף 20 (ב) לתקנות - שכנוע הרגולטור כי הבנקים עומדים בהנחיות הרשות המוסמכת לעניין אבטחת מידע, מאחר ואין כל מחלוקת כי הבנקים כפופים לפיקוח על הבנקים בעניין זה (ובעניינים אחרים), ומנגנון מאולץ וכפוי כמו זה לא מתאים למערכת הבנקאית.

עמדתנו החד משמעית היא שיש לכתוב באופן מפורש כי הסקטור הבנקאי מוחרג מהתקנות. במקרים שרמו"ט או מטה הסייבר הלאומי מעוניינים יהיו לקבל דיווח על אירועי אבטחה ספציפיים, או לחדד את הנחיותיהם למערכת הבנקאית, הם יכולים לעשות זאת, כפי שאף ידוע לנו שהם עושים כך עכשיו, בצורה אפקטיבית וקואופרטיבית בהידברות עם הפיקוח על הבנקים, כאשר הפיקוח על הבנקים – הוא ורק הוא יכול להביא בחשבון את כל השיקולים הרלוונטיים למוסדות הבנקאיים, על המיוחדות והרגישות של סקטור זה.

יצוין, כי למיטב הבנתנו רמו"ט (שעמה ניהלנו דיאלוג ממושך ומקצועי בקשר עם תקנות אלו ובנושאים אחרים), אינה מסתייגת מכך שהבנקים מוסדרים באופן נפרד ומקיף, אולם, הדבר לא בא על ביטויו בתקנות הקיימות.

5. מבלי לגרוע מהאמור לעיל, ומבלי לפרט כאן את כל הסעיפים בתקנות המהווים רגולציה כפולה ואף סותרת על הבנקים, **אנו מבקשים לציין במיוחד את הבעייתיות בסעיף העוסק בתיעוד של אירועי אבטחה (ס' 11):** על פי הסעיף האמור, אם ארע אירוע אבטחה חמור, אזי בעל המאגר (התאגיד הבנקאי), צריך להודיע על האירוע לרשם מאגרי מידע. אנו סבורים שהתאגידים הבנקאים צריכים לדווח על אירועי אבטחה ברמת חומרה מסוימת אך ורק לגורם המפקח עליהם ישירות, כלומר - הפיקוח על הבנקים. כך הם עושים כבר היום מכח הרגולציה שחלה עליהם. הפיקוח על הבנקים הכתיב לבנקים מתודולוגיית דיווח מסודרת ומפורטת בנושאי אבטחת מידע, במסגרת הוראת נב"ת 361 ובמסגרת הוראות הדיווח לפיקוח מס' 848, שזו, כידוע, חקיקה בפני עצמה. דיווח כפול לרמו"ט על ידי הבנקים הוא מיותר וטומן בחובו סיכונים עצומים. אנו חושבים כי הדרך הנכונה יותר, היא להמשיך במתכונת הדיווחים הקיימת

-3-

שחלה על הבנקים מכוח הוראות הפיקוח על הבנקים. הפיקוח על הבנקים יעביר במקרים בהם הדבר נחוץ, דיווח על אירועים מהותיים לרשם מאגרי המידע. כך תמנע זליגת מידע עודף מהבנקים, וכך יצומצמו נזקים פוטנציאליים העלולים להיגרם מהפצת הדיווחים המבוקשים.

עוד קובעות התקנות כי אם אירע אירוע אבטחה חמור, רשאי הרשם להוראות לבעל המאגר, ולאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע. אנו מבקשים להבהיר כי פרשנות שגויה של הציבור למידע אודות אירוע אבטחה, עלולה להיות בעלת השלכות דרמטיות, על המערכת הבנקאית ועל המשק כולו. לכן, כל החלטה באשר להפצת מידע אודות אירוע אבטחה בבנקים, חייבת להישקל באופן יסודי ולאחר שלנגד עיני הגוף המדווח עומדים כל השיקולים על נגזרותיהם – החל משיקולי אבטחה, עבור לשיקולים צרכניים, וכלה ביציבות המערכת הבנקאית. לפיכך, לא ייתכן שהחלטה על הפצת מידע רגיש מהסוג האמור תתבצע לאחר תהליך ההיוועצות שבו לא ייקח חלק הפיקוח על הבנקים (זוהי עוד דוגמא לכך שלא ניתן להחיל את התקנות על הבנקים כלשונו).

6. לאור כל האמור לעיל, אנו חושבים כי הבנקים צריכים להיות מוחרגים מתחולת התקנות כבר עכשיו, ובמפורש. רגולציה כפולה במקרה זה אינה תוצאה רצויה ויש למנוע אותה כבר עכשיו במסגרת הליכי התקנת התקנות.

העוסקים בנושא מטעמנו יעמדו לרשות הוועדה הנכבדה בכל הסבר נוסף שיתבקש בסוגיה.

בכבוד רב,

**טל נד"ב, עו"ד**  
סמנכ"ל, היועץ המשפטי

העתק:  
משה פרל, מנכ"ל איגוד הבנקים  
רחל יעקובי, הפיקוח על הבנקים, בנק ישראל  
עו"ד שירלי אבנר, המחלקה המשפטית, בנק ישראל  
עו"ד חן פליישר, המחלקה המשפטית, בנק ישראל  
טיבי רבינוביץ, מנהל קשרי החוץ, איגוד הבנקים  
עו"ד לבנת קופרשטיין-דאש, איגוד הבנקים.

#23798v3