



כ"ה בשבט תשע"א

30 בינואר 2011

**חוזר מס' ח-06-2292**

### **הנדון: ניהול טכנולוגיית המידע**

(ניהול בנקאי תקין, הוראה מס' 357)

#### **מבוא**

1. ממועד העדכון האחרון של הוראת ניהול בנקאי תקין מס' 357 (להלן ההוראה) בשנת 2003, חלו שינויים טכנולוגיים בעלי השלכות על ניהול הסיכונים במערך טכנולוגיית המידע. לאור האמור לעיל, בעקבות ניסיון שנצבר בתחום זה, ולאחר התייעצות עם הוועדה המייעצת בעניינים הנוגעים לעסקי בנקאות ובאישור הנגיד, תיקנתי הוראה זו.

#### **עיקרי התיקונים להוראה**

2. המפקח על הבנקים יתיר, במקרים חריגים, למנהל טכנולוגיית המידע ולמנהל אבטחת המידע בתאגיד הבנקאי לשמש בתפקידים אלו גם בתאגידים הנשלטים על ידיו **(סעיפים 4(א1) ו-9(א1) להוראה)**.

#### **דברי הסבר**

במקרים חריגים, כשמדובר בתאגיד נשלט עליו חלה ההוראה, וכן כאשר התאגיד הנשלט מקבל את שירותי המחשוב עבור עסקי הליבה שלו מתאגיד האם, ייתכן מצב שיקשה על התאגיד הבנקאי למנות כמנהל טכנולוגיית המידע גורם שיהיה חבר הנהלה או כפוף למנכ"ל, ו/או כמנהל אבטחת המידע גורם שיהיה כפוף לחבר הנהלה. למשל, כאשר התאגיד הנשלט הוא תאגיד קטן.

3. התאגיד הבנקאי נדרש לדאוג להצפנה גם כאשר מדובר בבנקאות בתקשורת הנעשית באמצעות דואר אלקטרוני. יחד עם זאת, במשלוח דואר אלקטרוני בנוגע לחשבון של בנק הפועל והמפוקח מחוץ לגבולות ישראל לא תידרש הצפנה, בהתקיים התנאים המפורטים בסעיף **(סעיפים 13(א) ו-13(א1) להוראה)**.

#### **דברי הסבר**

מטרת התיקון להדגיש כי בנקאות בתקשורת באמצעות האינטרנט כוללת גם דואר אלקטרוני, ולפיכך גם הדרישה להצפנה. יחד עם זאת, במקרים חריגים כאשר מדובר בהעברת מידע לבנק הפועל והמפוקח מחוץ לגבולות ישראל (להלן: "בנק זר"), קיימת אפשרות שלא להצפין את הדואר האלקטרוני. לדוגמה, כאשר המידע שנשלח מצומצם (כגון, עמלות, שיעורי ריבית וכד'), אך לא עסקאות וכד') ולא ניתן להסיק ממנו נתונים חסויים הקשורים לחשבון הבנק הזר. בכל מקרה, החרגה זו כפופה לתנאים בהוראה.

4. ניתן לאפשר קישוריות עובדים לרשת האינטרנט גם להורדת קבצים (סעיף 14(ג) ו- 14(ד)(2) להוראה).
- דברי הסבר**
- ההוראה מבטלת את האיסור על הורדת קבצים באמצעות קישוריות עובדים לרשת האינטרנט. כפי שנדרש גם בעבר, קישוריות זו תתאפשר בכפוף להערכת הסיכונים וליתר התנאים המפורטים בסעיף 14 להוראה.
5. תאגיד בנקאי יחיל אמצעי מעקב ואבטחה מסוימים לעניין הקישוריות לאינטרנט על כלל אתרי הבנק, לרבות האתר השיווקי שלו (סעיף 14(ז) להוראה).
- דברי הסבר**
- יש להגן על כלל אתרי התאגיד הבנקאי, לרבות האתר השיווקי, באמצעי ההגנה המינימליים המפורטים בהוראה, שכן פגיעה בהם עלולה לגרום להתממשות סיכונים תפעוליים וסיכונים אחרים (למשל, סיכון מוניטין).
6. נקבע כי לעניין הבקורות ואבטחת המידע, כל רמת שירות בפסקאות (ב) עד (ד) של סעיף (ב)(1) כוללת את רמות השירות שקדמו לה (סעיף 19(ב)(1) להוראה).
- דברי הסבר**
- התיקון קובע כי תאגיד בנקאי יוכל להציע ללקוחותיו רמת שירות אשר איננה כוללת שירותים הניתנים ברמת שירות הנמוכה מרמת השירות המוצעת, אולם בכל מקרה לעניין הבקורות ואבטחת המידע כל רמת שירות תכלול גם את רמות השירות הקודמות לה.
7. נקבע כי ניתן יהיה לעדכן פרטים אישיים המשמשים להעברת מידע ללקוח באמצעות בנקאות בתקשורת (סעיף 19(ב)(2) להוראה).
- דברי הסבר**
- המטרה היא לאפשר עדכון פרטים אישיים באמצעות בנקאות בתקשורת. בשלב זה התיקון יאפשר לעדכן רק פרטים אישיים המשמשים להעברת מידע ללקוח (כגון, מספרי טלפון), אולם לא יתאפשר עדכון פרטים אישיים אחרים. התיקון מפרט את התנאים בגינם יתאפשר תיקון הפרטים האישיים. רמת השירות לעדכון פרטים אישיים היא (2). עם זאת, ללקוחות שצורפו לרמת שירות (1) בלבד, עדכון פרטים אישיים יחשב כרמת שירות (1). במקרה זה, התאגיד הבנקאי נדרש לאפשר ללקוח ברמת שירות (1), לבחור באפשרות של עדכון הפרטים ולהבהיר לו כי הוא יכול לבקש את ביטולה של אפשרות זו בכל עת.
8. התיקון מאפשר לבצע הסכם מקוון גם באמצעות הטלפון, בכפוף לקיום התנאים המפורטים בהוראה, לרבות הפעלת אמצעים לכך שהלקוח ראה את ההסכם וכן הסכמת הלקוח לאמור בהסכם. בנוסף התיקון מאפשר ללקוח לבחור בהסכם מקוון אחד מספר ערוצי תקשורת, ובלבד שבחר בכל אחד מהם במפורש. בהסכם מקוון עבור כל רמת שירות, יידרש התאגיד הבנקאי לוודא שהלקוח חתם על הסכם בסניף בעבר, ללא קשר למספר השנים שקדמו למועד חתימת ההסכם המקוון (סעיפים 20(ב) ו- 20(ג) להוראה).

בהסכם מקוון יאפשר התאגיד הבנקאי ללקוח, לגרוע כל רמת שירות שנכרתה בעבר בהסכם מסוג זה. התיקון נועד למנוע מצב בו הלקוח יוכל לגרוע רמת שירות כאמור רק בסניף התאגיד הבנקאי (סעיף 20 (ג)1 להוראה).

במקרים חריגים, למפקח על הבנקים נשמרת האפשרות לאשר לתאגיד בנקאי להציע הסכם מקוון בתנאים שונים מאלו הנכללים בסעיף (סעיף 20(ו) להוראה).

#### **דברי הסבר**

מטרת התיקון היא להקל על ביצוע הסכמים מקוונים, על מנת לעודד ולאפשר חדשנות והתייעלות.

יודגש כי, סעיף 20 (ב)3 אינו מייתר את הצורך לתת אפשרות ללקוח לבחור בהסכם המקוון בנפרד, כל אחת מרמות השירות כנדרש בסעיף 20 (א) להוראה.

9. תאגיד בנקאי יוכל לחרוג מהעיקרון של פעילות בבנקאות בתקשורת במבנה הרשאות הזוהה לזה שהוסכם עם הלקוח בחשבון, וזאת במקרה שמדובר בלקוח שהוא תאגיד, ותוך הסכמה מתאימה בכתב ואימות התאגיד הבנקאי את ההסכמה באמצעות העתק מהחלטת האורגן המוסמך בעניין זה בתאגיד (סעיף 22(ג)2 להוראה).

#### **דברי הסבר**

במקרה של תאגידיים, רשאי התאגיד הבנקאי ליתן הרשאות לערוצי בנקאות בתקשורת, השונות מההרשאות שהוסכמו בחשבון התאגיד. לדוגמה, בחשבון תאגיד שמחייב שתי חתימות בסניף, ניתן להסכים עם התאגיד, בהתאם להחלטה מתאימה שהתקבלה ע"י האורגן המוסמך בתאגיד לעניין זה, כי התאגיד יפעל באינטרנט גם באמצעות זיהוי של מורשה אחד בלבד. יודגש כי הקלה זו לא תחול על חשבונותיהם של יחידים, גם אם ניתנה לגביהם הסכמתו המפורשת של הלקוח בכתב, לפיה הרשאותיו בערוצי הבנקאות בתקשורת יהיו שונות מההרשאות שהוסכמו בחשבון הלקוח.

10. תאגיד בנקאי יכול לאפשר ללקוח לאשר רשימת מוטבים שלא חל בה כל שינוי, באמצעות מערכת בנקאות בתקשורת, ובלבד שהסכם ההתקשרות שנחתם בין הלקוח לבין התאגיד הבנקאי באותו ערוץ תקשורת הינו לרמת שירות הגבוהה מרמת שירות (1). במקרה שהלקוח אישר את רשימת המוטבים כאמור, ישלח הבנק ללקוח הודעה באמצעות הדואר, אודות אישורו את רשימת המוטבים, בתוספת הרשימה עצמה (סעיף 26(ג)3 להוראה).

#### **דברי הסבר**

הסעיף מאפשר לתאגיד בנקאי להציע ללקוחותיו לאשר רשימת מוטבים שלא חל בה כל שינוי מאז האישור הקודם, באמצעות מערכת בנקאות בתקשורת לגביה חתם הלקוח על הסכם התקשרות לרמת שירות הגבוהה מרמת שירות (1). התיקון מהווה הקלה, משום שבמקרה ספציפי זה של אישור (שלא חל כל שינוי ברשימה) הוא מייתר את הצורך בשימוש בטכנולוגיה כאמור בסעיף 12(ג)1 להוראה או לחילופין לבצע את האישור בסניף. כבקרה על פעולת האישור, נדרש התאגיד הבנקאי לשלוח ללקוח הודעה באמצעות הדואר אודות אישורו את רשימת המוטבים, בתוספת הרשימה עצמה.

11. **בסעיף 27(ד) להוראה** במקום המילים: "תאגיד בנקאי רשאי לשלוח באמצעות דואר אלקטרוני או באמצעות אתר התאגיד הודעות אשר כללי גילוי נאות מאפשרים העברתן ללקוח באמצעות הדואר, וכן מידע אחר שחובת החיסיון חלה עליו..." יבוא: " תאגיד בנקאי רשאי לשלוח באמצעות דואר אלקטרוני או באמצעות אתר התאגיד (להלן: אמצעים אלה), הודעות שחובת הסודיות חלה עליהן".

#### **דברי הסבר**

סעיף זה קובע, כי כל הודעה שחובת הסודיות חלה עליה, ובכלל זאת ההודעות המנויות בכללי גילוי נאות, רשאי התאגיד הבנקאי לשלוח באמצעות דואר אלקטרוני או אתר התאגיד, בהתקיים התנאים הקבועים בסעיף, וזאת, יודגש, מבלי לגרוע מחובת התאגיד הבנקאי לשלוח את ההודעה באמצעים אחרים (כגון: דואר) אם נקבע כך מפורשות לגבי אותה הודעה. עבור משלוח הודעות באמצעות אתר התאגיד הבנקאי, בוטלה החובה של התאגיד הבנקאי להפעיל כלים ממוחשבים המאפשרים לו לקבוע חד משמעית האם הלקוח קיבל את הדואר ופתח אותו, או ביצע הורדה (Download) של מסר הדואר למחשבו האישי או הדפסתו. עבור משלוח הודעות באמצעות דואר אלקטרוני – לא נעשה כל שינוי.

12. **סעיף 27(ד)(2) להוראה** קובע כי בהתייחס להודעות המנויות בהוראת ניהול בנקאי תקין מס' 420, ניתן להסתפק בהעברת המידע באמצעות דואר אלקטרוני או באמצעות אתר התאגיד בלבד, אם התקיימו התנאים האמורים בסעיף.

#### **דברי הסבר**

סעיף זה מפנה להוראת ניהול בנקאי תקין 420, שעניינה "מסירת מידע באמצעים אלקטרוניים", ואשר מגדירה את סוגי ההודעות המותרות במשלוח באמצעות דואר אלקטרוני או באמצעות אתר התאגיד בלבד. היינו, עם משלוח הודעות כאמור באמצעים אלו, יהיה התאגיד הבנקאי פטור ממשלוח ההודעות גם באמצעות הדואר, וזאת בהתקיים התנאים הקבועים בסעיף.

#### **תחילה**

13. תחילתה של הוראה זו היא ביום פרסומה.

#### **עדכון הקובץ**

14. מצ"ב דפי עדכון לקובץ הוראות ניהול בנקאי תקין. להלן הוראות העדכון:

<u>להכניס עמוד</u>	<u>להוציא עמוד</u>
357-1-20 [5] (1/11)	357-1-20 [4] (9/03)

בכבוד רב,

דוד זקן

המפקח על הבנקים