

סודיות מידע

1. בהתאם לסמכותי לפי סעיף 88 יד(א) לחוק הדואר, התשמ"ו-1986 ("החוק" או "חוק הדואר"), אני קובע הוראות אלה:

2. תחולה;

הוראה זו תחול על חברת דואר ישראל בע"מ ("חברת הדואר" או "החברה") בנותנה את השירותים הכספיים לפי הוראות פרק 1ו לחוק הדואר ("בנק הדואר").

2.1 הגדרות

2.1.1 "אמצעי זיהוי" - אמצעי המספק אימות לגבי זהותו של אדם, דוגמת שם חשבון משתמש

או כרטיס חכם, בתהליך ההזדהות והכניסה למערכות מידע.

2.1.2 "הנדסה חברתית" - ניצול אדם במטרה להשיג מידע, בעזרת שימוש בהונאה, התחזות,

שכנוע, הסחת דעת וכו'.

2.1.3 "מידע" - כול מידע כספי, וכן נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו,

מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו, הנוגע ללקוחות בנק

הדואר, בעבר ובהווה וכן ללקוחות מזדמנים.

2.1.4 "נכס טכנולוגיות המידע" - מערכת מידע או רכיביה לדוגמה חומרה, תוכנה ומערכת

הפעלה.

2.1.5 "נכס מידע" - נתונים המאוחסנים באופן אלקטרוני (לדוגמה מאגר נתונים) או במסמכי

נייר.

2.1.6 "סודיות מידע" - הגנה על המידע מפני גורמים שאינם מורשים לעשות בו שימוש.

2.1.7 "סיווג" - קטלוג של נכסי מידע, על פי מידת החיסיון הנדרשת עבורם ובהתאם למדרג

אשר הוגדר מראש.

סודיות מידע

3. מבוא

3.1. רקע

❖ הזכות לפרטיות נקבעה לראשונה בחוק הגנת הפרטיות תשמ"א-1981: סעיף 1 לחוק הגנת הפרטיות קובע: "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". סעיף 4 קובע כי "פגיעה בפרטיות היא עוולה אזרחית...". סעיף 5 קובע כי במקרים מסוימים פגיעה בפרטיות נחשבת גם עבירה פלילית שדינה מאסר 5 שנים. פרק ב' בחוק הגנת הפרטיות עוסק בהגנה על פרטיות המידע שבמאגרי מידע: בסעיף 8(ב) נכתב כי "לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר". ואילו סעיף 16 קובע עבירה פלילית של גילוי מידע שהגיע אל הבנק מתוקף החזקתו במאגר המידע שדינה מאסר 5 שנים.

❖ בסעיף 7 לחוק יסוד כבוד האדם וחירותו נכתב:

"(א) כל אדם זכאי לפרטיות ולצנעת חייו.

(ב) ...

(ג) ...

(ד) אין פוגעים בסוד שיחו של אדם, בכתביו או ברשומותיו."

חוק יסוד זה מעגן ומחזק את הזכות לפרטיות, ומהווה אבן דרך משמעותית בכול הנוגע לפעולות החקיקה והאסדרה בישראל.

❖ בסעיף 88(ט)(א) לחוק הדואר נכתב כי "כל החובות החלות על בנקאי בדבר שמירת סוד

יחולו על החברה בנותנה את השירותים הכספיים ועל כל אדם הממלא תפקיד בה."

לאור האמור, חובה על בנק הדואר לשמור על סודיות המידע שהובא לידיעתו, ומניעת גילוי בידי צד שלישי, הן במישרין והן בעקיפין.

סודיות מידע

הוראה זו מותאמת לבנק הדואר והיא מושתתת על חקיקה ואסדרה קיימת בישראל ועל מתודולוגיות וסטנדרטים מקובלים, לרבות:

- 3.1.1** CobiT 4.1 - מסגרת בקרה מקובלת לעניין קיום ענייני בקרה ופיקוח יעילים בתחום טכנולוגיות המידע;
- 3.1.2** COBIT 5 - Enabling Information
- 3.1.3** ISO 27001 - תקן בינלאומי לאבטחת מידע;
- 3.1.4** חוק הגנת הפרטיות התשמ"א-1981;
- 3.1.5** חוק הדואר, התשמ"ו-1986;
- 3.1.6** תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986.
- 3.1.7** רישיון כללי לחברת דואר ישראל בע"מ למתן שירותי דואר, שירותים כספיים מטעם החברה הבת ושירותים נוספים, ("הרישיון");
- 3.1.8** תקנות הדואר (שירותי דואר בסיסים ושירותים כספיים אשר יינתנו לכלל הציבור בכל המדינה), תשס"ח-2008, ("תקנות הדואר" או "התקנות").

סודיות מידע

4. סודיות מידע

4.1. יעדים

שמירה על סודיות המידע של לקוחות הבנק, וכן על מידע של גורמי צד שלישי, המשמש את הבנק, בין אם הוא נשמר בחצרי הבנק ובין אם מתאפשרת אליו גישה בתקשורת.

הוראה זו מתייחסת להיבטים הנוגעים לגורם האנושי ולתהליכי עבודה בבנק, והיא אינה מתייחסת להיבטים טכנולוגיים ולנכסי טכנולוגיות המידע, המסייעים בשמירה על סודיות המידע.

4.2. קווים מנחים

4.2.1. דירקטוריון הבנק, יגבש מדיניות בנוגע לשמירה על סודיות המידע של לקוחות הבנק.

4.2.2. בין היתר, יתייחס דירקטוריון הבנק להיבטים הייחודיים הנוגעים לכל הגורמים השונים בבנק, לרבות לכול אחד מהגורמים הבאים:

- עובדי הבנק;
- סוכני דואר ועובדיהם;
- עובדי חברת הדואר, העוסקים במתן שירותים כספיים.
- ספקי צד שלישי;
- עובדי מחלקת מערכות מידע.

4.2.3. דירקטוריון הבנק יגבש מנגנון דיווח, ויגדיר בין היתר את הגורמים האמונים על הדיווח, את תכולת הדיווח, לרבות בנוגע לאירועים בהם התגלו חריגות מהקבוע במדיניות ובנהלים או באירועים בהם התגלה כשל בבקורות, וכן בנוגע לפעילויות אשר בוצעו במטרה להגביר את המודעות בתחום.

4.2.4. דירקטוריון הבנק יקבע את תדירות הדיווח העיתי אליו, ואת התנאים בהם נדרש דיווח מידי.

4.3. גיבוש תהליך

4.3.1. ההנהלה תיישם תהליכים ובקורות, אשר יבטיחו שמירה על סודיות המידע של הלקוחות בבנק הדואר, וייתייחסו, בין היתר, להיבטים הבאים:

4.3.1.1. קיומו של רישום עדכני של נכסי מידע פנימיים של הבנק וכן נכסי מידע של גורמים חיצוניים, אליהם קיימת גישה של הגורמים המנויים בסעיף 4.2.2 לעיל.

4.3.1.2. הנחיות באשר לשימוש המותר במידע, על ידי הגורמים המנויים בסעיף 4.2.2 לעיל, באופן שיימנע פגיעה בסודיות המידע, בהתאם לחוקים ולתקנות בתחום, לרבות חוק הגנת הפרטיות;

4.3.1.3. אופן הבקרה על ספקי צד שלישי, להם גישה למידע;

סודיות מידע

- 4.3.1.4.** אופן הבקרה על עובדי מחלקת מערכות מידע, להם הוקצו הרשאות על, המאפשרות להם גישה נרחבת, בין היתר למידע רגיש;
- 4.3.1.5.** כללים והנחיות באשר להוצאה והכנסה של מידע אל ומחוץ לחצרות הבנק;
- 4.3.1.6.** קביעת כללים והנחיות בנוגע לשימוש במידע פנימי או חיצוני של הבנק ברשת האינטרנט, רשתות חברתיות, דואר אלקטרוני וכו'.
- 4.3.1.7.** שמירה ואחסון מדיות ומצעים פיזיים, דוגמת תדפיסים.
- 4.3.2.** הנהלת הבנק תנחה את הגורמים המנויים בסעיף 4.2.2 בדבר חובתם לשמירה על סודיות המידע ותגדיר תהליכי בקרה למידת העמידה בדרישות השונות.
- 4.3.3.** הנהלת הבנק תנחה את הגורמים המנויים בסעיף 4.2.2 בנוגע לשימוש במידע של צדדים שלישיים, בו הם עושים שימוש במסגרת עבודתם.
- 4.3.4.** הנהלת הבנק תגבש בקרות טכנולוגיות ותהליכיות, אשר יצמצמו את הסיכוי לפגיעה בסודיות המידע.
- 4.3.5.** הנהלת הבנק תגבש תהליך לתחקור וניתוח אירועי כשל בהם דלף מידע רגיש, לרבות מינוי גורם אשר יהיה אחראי לקיום התחקור, והגדרת הגורמים אשר ידווחו אודות מסקנות שהוסקו, פעולות מתקנות שננקטו, ובהתאם לצורך, אודות הצעדים אשר ננקטו כנגד מי מהגורמים המעורבים באירוע.

4.4. ניהול שוטף

- 4.4.1.** הנהלת הבנק תאמוד, בהתייחסות כוללת ובתדירות שתקבע, את יעילות המדיניות, הנהלים, התהליכים והבקורות אשר מוסדו לצורך שמירה על סודיות המידע.
- 4.4.2.** הנהלת הבנק תקיים בקרה שוטפת, אחר הבקורות אשר הוגדרו, במטרה לצמצם את הסיכוי לפגיעה בסודיות המידע.
- 4.4.3.** הנהלת הבנק תאמוד, בתדירות שתקבע, את השלכות הפגיעה בסודיות המידע ואת השפעתן על פעילות הבנק.
- 4.4.4.** הנהלת הבנק תבטיח את קיומן של הדרכות מודעות, באשר לחובה בשמירה על סודיות מידע, אשר יתייחסו לסיכונים השונים, לרבות איומי הנדסה חברתית.
- 4.4.5.** במידת הצורך, תקיים ההנהלה תהליך של תחקור וניתוח אירועי בהם לא נשמרה סודיות המידע.

4.5. דיווח

- 4.5.1.** לפחות אחת לחצי שנה, ידווח ממונה אבטחת מידע בבנק, להנהלת הבנק אודות אירועי כשל במהלכם דלף מידע רגיש ואודות פעילויות שונות המתבצעות בבנק, במטרה לצמצם את הסיכון לפגיעה בסודיות מידע.

סודיות מידע

- 4.5.2.** בהתאם להנחיות הדירקטוריון, יתקיים דיווח לדירקטוריון הבנק, בכל הנוגע לשמירה על סודיות המידע בבנק הדואר.
- 4.5.3.** יוגדרו אירועים, אשר בגינם נדרש דיווח מידי לגורמים שונים, לרבות: דירקטוריון, הנהלה והמפקח על בנק הדואר.

סודיות מידע

5. תקפות

הנחיות הוראה זו אינן באות להחליף הנחיות קיימות, הנובעות מחוקים ומהוראות קיימות, לרבות הדוגמאות המפורטות להלן, מתוך הוראת ניהול תקין בנושא ניהול טכנולוגיות המידע ואבטחת מידע במערכות המידע בבנק הדואר, אלא להוסיף עליהן.

הנושא	הנחיות קיימות בהוראת ניהול תקין בנושא ניהול טכנולוגיות המידע ואבטחת מידע במערכות המידע בבנק הדואר
סיווג ותיוג מידע	<ul style="list-style-type: none"> הגדרת רמות סיווג לנכסי מידע וקביעת הקריטריונים המאפיינים כל רמה (סעיף 4.1.2.1); גיבוש מדיניות בנוגע להצפנת מידע השמור במערכות המידע או המועבר אל גורמי חוץ (סעיף 5.2.2.3).
רשימת נכסי מידע	<ul style="list-style-type: none"> הגדרת רמות סיווג לנכסי מידע וקביעת הקריטריונים המאפיינים כל רמה (סעיף 4.1.2.1).
שם משתמש וסיסמא	<ul style="list-style-type: none"> הצורך בזיהוי חד ערכי של משתמשי מערכות מידע (סעיף 5.3.2.1) ושימוש בסיסמא מורכבת (סעיף 5.3.2.2).
התקשרות עם ספקי צד ג'	<ul style="list-style-type: none"> הסכם עם ספק חיצוני יכולול התייחסות לחובת סודיות (סעיף 7.3.3.3); הבטחת מהימנות ושלמות המידע בעת העברת מידע בממשקים מ/אל ספקים ושותפים עסקיים, ובהתאם להערכת סיכונים, יש ליישם עקרונות אבטחה מקובלים לרבות בקרת גישה, הצפנה, והגדרת פעולות בקרה נדרשות (סעיף 4.1.2.6).
זיהוי לקוחות	<ul style="list-style-type: none"> התייחסות לאמצעי זיהוי אישיים לכל מורשה גישה בעת שימוש בשירותים בתקשורת (סעיף 8.2.2); זיהוי לקוחות חסרי תיעוד רשמי בקרות אירוע אסון (סעיף 6.3.4).
טיפול במצאים פיזיים	<ul style="list-style-type: none"> הגדרת תהליך מאובטח לטיפול בנכסי מידע פיזיים דוגמת מסמכי נייר ומדיה מגנטית המכילים מידע רגיש (סעיף 5.1.2.4).

6. החלת ההוראה

תחילת הוראה זו ביום י"א בשבט תשע"ה, 31 בינואר 2015.