

A pair of glasses is positioned in the top left corner. The background is a light-colored, textured surface with several water droplets of various sizes scattered across it. The text is centered in the middle of the page.

# מצגת בנושא תקנות הגנת הפרטיות

תשתיות מידע וטכנולוגיות בע"מ

## תקנות הגנת הפרטיות

- ביום 21 במרץ 2017, אושרו בוועדת חוקה, חוק ומשפט של הכנסת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "התקנות").
- התקנות הן שינוי מהותי ברגולציית אבטחת המידע בישראל, והן מטילות חובות משמעותיות על בעלי מאגרי מידע לאבטחת המידע שברשותם.
- בין החובות הכלולות בתקנות: אימוץ מדיניות מחייבת ונוהלי אבטחת מידע מקיפים, מיפוי מערכות המידע בארגון וביצוע סקר סיכונים, הטמעת תפיסות אבטחת מידע בניהול כוח האדם בארגון, וחובות דיווח על אירועי אבטחה. בנוסף, ביחס למאגרי מידע בעלי רגישות גבוהה, התקנות קובעות גם ביצוע מבדקי חדירות והטמעת אמצעי אבטחה.

## רמות אבטחה שונות למאגרי מידע

- ככלל, התקנות יחולו על כל מאגר מידע שחייב ברישום לפי חוק הגנת הפרטיות. עם זאת, חלק מההוראות יחולו רק על מאגרי מידע ברמת אבטחה בינונית או גבוהה, אשר יהיו כפופים לנהלים מחמירים יותר.
- מאגרי מידע ברמת אבטחה בינונית כוללים, בין היתר, מאגרים הכוללים מידע רפואי, מידע על צנעת חייו של אדם, מידע על דעותיו הפוליטיות או אמונותיו של אדם, מידע ביומטרי, מידע כלכלי לרבות מידע על הרגלי צריכה של אדם, וכן מאגרי מידע שנועדו לצורך דיוור ישיר.
- מאגרי מידע ברמת אבטחה גבוהה הם מאגרים הכוללים מידע רגיש כמפורט לעיל הכוללים פרטים על 100,000 אנשים ומעלה, או שמספר מורשי הגישה אליהם עולה על 100.

## מסמכי מדיניות נהלים ובעלי תפקידים

- התקנות מחייבות כל בעל מאגר מידע לאמץ מסמך מדיניות המגדיר את מטרות המאגר, את סוגי השימושים בו, את הסיכונים העיקריים לפגיעה באבטחתו ואת דרכי ההתמודדות עמם.
- כל בעל מאגר מידע יחויב לקבוע נוהל אבטחת מידע בהתאם להגדרות מאגרי המידע שברשותו. הנוהל יחייב את כל עובדי הארגון וייתחס, בין היתר, למיפוי מערכות המידע בארגון ואבטחתן, למדיניות הרשאות הגישה למאגרי המידע ולמערכות המידע, לאמצעי אבטחת המידע המוטמעים בארגון, לסיכוני אבטחת המידע הקיימים בארגון ודרכי ההתמודדות עמם ולאופן ההתמודדות עם אירועי אבטחת מידע בזמן אמת. בעלי מאגרי מידע ברמת אבטחה בינונית או גבוהה יצטרכו לכלול גם התייחסות לגיבוי המידע שברשותם, לעריכת בדיקות תקופתיות ולשימוש בהתקנים ניידים בארגון.
- התקנות קובעות כי ממונה אבטחת המידע לפי חוק הגנת הפרטיות (בין אם חלה חובה חוקית למנותו ובין אם מונה באופן וולונטרי), לא ימלא תפקיד אחר בארגון שעלול לגרום לו להימצא בניגוד עניינים (למשל, מנהל מערכות המידע בארגון), ויהיה כפוף למנכ"ל או לנושא משרה בכיר אחר. עוד קובעות התקנות, כי על הארגון להעמיד לרשות הממונה את המשאבים הנדרשים כדי לציית להוראות התקנות.

## מיפוי מערכות מידע, סקרי סיכונים ומבדקי חדירות

- בעלי מאגרי מידע יחויבו לערוך ולהחזיק מסמך הממפה את מערכות המידע הנוגעות לכל מאגר ומאגר (לרבות חומרה, תוכנה וציוד קצה) ואת אמצעי האבטחה החלים עליהן.
- בעלי מאגרי מידע ברמת אבטחה גבוהה יידרשו גם לערוך סקרי סיכונים ומבדקי חדירות למערכות המידע שברשותם אחת ל-18 חודשים, לדון בתוצאותיהם ולאמץ נהלים ואמצעי אבטחה בהתאם למסקנות הנובעות מהם.

## אמצעי אבטחת מידע

- בעלי מאגרי מידע יחויבו לפי התקנות להטמיע אמצעי אבטחת מידע שונים בארגון. כך למשל, יהיה על בעלי מאגרי מידע לדאוג, בין היתר, לאבטחה פיזית של המאגר, לניהול הרשאות גישה בארגון, לקביעת מנגנוני זיהוי ואימות (לרבות סיסמאות חזקות ואמצעי זיהוי חכמים), לתיעוד של אירועי אבטחה במערכות המידע, להפרדה בין מערכות המידע השונות הנוגעות למאגר ולהצפנת העברת מידע מהמאגר ברשתות ציבוריות.
- בעלי מאגר מידע ברמת אבטחה בינונית וגבוהה יחויבו לתעד את הגישה הפיזית למערכות המידע בארגון, להנהיג מנגנון קפדני של זיהוי ואימות משתמשים (לרבות מנגנוני ניתוק אוטומטיים וזיהוי באמצעים פיזיים), לתעד באופן אוטומטי את הגישה האלקטרונית למערכות המידע בארגון, ולשמור את נתוני התיעוד במשך 24 חודשים לפחות. עוד מורות התקנות כי על בעל המאגר לקבוע נהלים הנוגעים לגיבוי ושחזור המידע ולבצע אחת ל-24 חודשים לפחות ביקורת פנימית או חיצונית שמטרתה לבחון את הציזת להוראות התקנות.

## ניהול מורשים לגישה למאגר מידע

- התקנות מחייבות בעלי מאגרי מידע לנקוט בהליכים הולמים על מנת לוודא שעובדים שיש להם גישה למאגר מידע מתאימים לקבלת המידע המצוי בו, וזאת בשים לב לרגישות המידע. בנוסף, בעלי מאגרי מידע יחויבו לקיים הדרכות לעובדים בטרם יקבלו גישה למאגרי המידע.
- בעלי מאגרי מידע ברמת אבטחה בינונית וגבוהה יחויבו לקיים פעילות הדרכה תקופתית לעובדיהם אחת לשנה לפחות. חובות אלה תחולנה גם על עובדים המועסקים בארגון כיום ולהם גישה למאגר המידע

## דיווח על אירועי אבטחת מידע

- התקנות מטילות על ארגונים שחוו אירוע אבטחת מידע, לדווח על כך – במקרים מסוימים – לרשם מאגרי המידע.
- התקנות מעניקות לרשם מאגרי המידע סמכות להורות לאותו ארגון לדווח על אירוע האבטחה גם לכל מי שמידע אודותיו נחשף בעקבות אותו אירוע.



**ערנות עובדים – הנושא: העברות בנקאיות  
שיטות האקינג פשוטות לגניבת כספים**

מקרה לדוגמא...

# סופס העברה בנקאית SWIFT

FSHC.COM SWIFT-SWIFT

SWIFT-SWIFT SWIFT-SWIFT SWIFT-SWIFT

SWIFT-SWIFT SWIFT-SWIFT SWIFT-SWIFT



... THE ...

... THE ...

... THE ...

# סופס העברה בנקאית SWIFT

... THE ...

... THE ...

... THE ...



... THE ...

... THE ...

... THE ...

## איך יודעים מה אמיתי ומה מזויף?

- בודקים את הפרטים הבאים:
  - בדוק עם השולח בשיטה שונה מזו שקיבלת את המסמך האם הוא זה ששלח את המסמך? (דוגמא: אם הגיע בפקס – בדוק עם השולח טלפונית)
  - בדוק באינטרנט שבאמת קיים כזה סניף בנק
  - בדוק עם הבנקאי שלך מי עומד מאחורי הבקשה? לבנקאים יש יותר נתונים על חשבונות מוגבלים, מספרי SWIFT לא תקינים ומידע בנקאי על הצד השני.