הגנה על הפרטיות
היבטים משפטיים ופרקטיים

עו"ד מיכאל גילינסקי, שותף
אודיט בקרה וביקורת

מגמות שהביאו לגידול בהיקף הסיכון המשפטי ביחס למידע הנאגר

- הצמיחה של עולם הסייבר
- ריבוי במידע הנאגר
- רשתות חברתיות האיצו את מהירות העברת המידע
- הגברת החקיקה בנושא זכויות הציבור וגידול במודעות לזכויות אלו (קמפיינים של הרגולטור)

אודיט
בקרה וביקורת

מגמות שהביאו לגידול בהיקף הסיכון המשפטי ביחס למידע הנאגר

- גידול בהיקף פעילות הרגולטורים, הרגולציה והסמכויות
- גידול השימוש במנגנוני "אכיפה פרטית" (תביעות)
- גיוון בכלים המשפטים – תובענות ייצוגיות, תביעות נגזרות, "ידיד בית המשפט", "עותר ציבורי" ועוד
- ריבוי ארגונים חברתיים העוסקים בתחומים שונים

אודיט
בקרה וביקורת

מאגרי מידע סובבים את האירגון

לאירגון מידע מסוגים שונים:

- **<u>האירגון כמספק שירותים</u>** – נתונים אודות חברי הארגון ומקבלי השירות.

- **<u>האירגון כמעסיק</u> –**
  1. נתונים אודות עובדים הכוללים מידע אודות: מצב בריאותם, נתוני שכר, דיווחי מחלה, עיקולים, נוכחות, תיק אישי ואישורים שונים.
  2. נתונים אודות מועמדים לעבודה (כולל סיבות דחיה), מבחני אמינות וכדו'...

אודיט
בקרה וביקורת

מאגרי מידע סובבים את האירגון

- **<u>הארגון כמקבל שירותים</u>** – נתונים אודות ספקים (דירוג ספקים וסיבה להפסקת פעילות).
- **<u>הארגון כמגייס משאבים</u>** – נתונים אודות תורמים או תורמים פוטנציאליים
- **<u>ובנוסף</u>** – מצלמות אבטחה, רשתות חברתיות וכו'...

אודיט
בקרה וביקורת

קצת הגדרות

"מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

"**אבטחת מידע**" - הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין

"מאגר מידע" - אוסף נתוני מידע, המוחזק באמצעי **מגנטי או אופטי** והמיועד לעיבוד ממוחשב, למעט –

(1) אוסף לשימוש אישי שאינו למטרות עסק; או

(2) אוסף הכולל רק שם, מען ודרכי התקשרות, שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ו**בלבד של בעל האוסף או לתאגיד בשליטתו**

אין אוסף נוסף;

אודיט
בקרה וביקורת

קצת הגדרות

מהו מידע רגיש?

נתונים אישיים:

על אישיותו של אדם	מידע ששר המשפטים קבע שהוא רגיש
על צנעת אישיותו	
מצב בריאותי	
מצב כלכלי	
דעותיו ואמונותיו	

אודיט
בקרה וביקורת

השינוי הגדול – תקנות הגנת הפרטיות(אבטחת מידע)

הגדרת "אירוע אבטחה"

קביעת רף נדרש לאבטחת המידע

קביעת אבחנה בין רמת הפעילות הנדרשת לסיכון הגלום במאגר

חובת מינוי גורם אחראי

אודיט
בקרה וביקורת

אז מהן החובות?

אודיט
בקרה וביקורת

במקביל לשינויים אלו

גדל גם

תחום הפשיעה המקוונת

אודיט
בקרה וביקורת

כמה סיפורים מהחיים

טיפול במידע עודף

ספק שירותים / מחזיק מאגר - איפה עובר קו הגבול

רמת האבטחה הנדרשת - רגישות "שאינה רגולטורית" (מאגר של ארגון החולים ב.... שמכיל מעט רשומות ומעט משתמשים - האם ברמה הבסיסית?!)

ההבדל בין המשפטי לטכנולוגי - מה בין "מערכת" או אפליקציה למאגר

דילמת ה- PAPERLESS – לסרוק או לא לסרוק, זאת השאלה...

החלת הוראות החוק על משתמשים שאינם עובדי הארגון

אודיט
בקרה וביקורת

המלצות

- **מודעות עובדים -** רעננו את הידע של העובדים בהיבטי הגנת סייבר באופן תדיר, גם אם הם עובדים מרחוק. הקפידו על תכנית הדרכות מודעות, דפי מידע עתיים, עלונים דיגיטליים וכדומה.

- **מוצרי הגנת סייבר על הציוד של הארגון -** העובדים משתמשים במכשירים שניתנו על ידי העסק? וודאו כי על כל מחשב, נייד או נייח, מותקנים מוצרי הגנת סייבר כגון: אנטי וירוס, עמדה להגנת תחנות קצה וחומת אש.

- **תוכנות ברישוי -** הקפידו שכל התוכנות המותקנות על מחשבי העסק יהיו ברישוי. תוכנות ללא רישוי אינן מקבלות עדכונים ותמיכה, ולכן עשויות להיות פרוצות – זוהי דרך כניסה של גורמים עוינים לרשת הארגון.

- **עדכונים אוטומטיים -** הגדירו שכלל המוצרים והתוכנות המותקנות על מחשבי הארגון יוכלו לקבל עדכונים אוטומטיים.

אודיט
בקרה וביקורת

המלצות

- **הגדרות פרטיות -** צרו הזדהות חזקה באמצעות סיסמה חזקה וקשה לניחוש ומנגנון אימות רב. הנחו את העובדים לבחור סיסמה קשה לניחוש ואפשרו זאת מבחינת המערכות בארגון. בנוסף, הפעילו עבור העובדים את השימוש באימות דו-שלבי/רב-גורמי, מומלץ באמצעות אפליקציית אימות או זיהוי ביומטרי, לזיהוי חזק וכדי למנוע אפשרות לגניבת סיסמאות.

- **דאגו לשגרת גיבויים ושחזורים** - וודאו כי המידע החשוב של העסק מגובה. בדקו שיש שגרת גיבויים סדורה – וכדי לוודא שהגיבויים נשמרים בצורה תקינה, בצעו בדיקה מפעם לפעם שאתם מצליחים לשחזר את המידע מגיבוי.

- **הצפינו את המידע על שרתי ומחשבי הארגון** - קיימים היום פתרונות הצפנה אשר נותנים מענה להצפנת המידע גם על המחשבים וגם בתעבורת המידע מהארגון החוצה ומחוץ לארגון פנימה.

אודיט
בקרה וביקורת

אז מה עושים?

- ❑ בודקים - איזה מאגרים יש לי בכלל?
- ❑ האם כל מה שהגדרתי כמאגר המחוייב ברישום אכן נרשם?
- ❑ הזדמנות לעשות סדר – מחיקת וביעור כל מידע שאינו נדרש
- ❑ עוד קצת סדר – מי יכול לגשת לאיזה מידע בארגון? האם זה נחוץ לנו?
- ❑ סיווג המידע לפי רמת האבטחה הנדרשת
- ❑ קביעת מדיניות ונהלים:
  - ○ מי יכול לראות איזה מידע?
  - ○ מי יכול להוציא מידע? איך? איזה מידע?
  - ○ איך אפשר לגשת למידע שברשותי? (אבטחה שיש לנקוט)
  - ○ איפה נמצא המידע שלנו? (ענן, התקן חיצוני), והאם זה מספק את הרמה שהיינו רוצים?
- ❑ מינוי מנהלי מאגר וממונה אבטחת מידע (גם אם רגולטורית איננו מחוייבים בכך)
- ❑ מכתבי נוחות ממחזיקים או מגורמים בעלי גישה למאגרים שברשותנו
- ❑ הטמעת תהליכים סדורים ולא פחות חשוב מכך - **<u>בקרות</u>**

אודיט
בקרה וביקורת

שאלות?

אודיט
בקרה וביקורת

תודה רבה!

אודיט
בקרה וביקורת

טלפון: 03-5616303 | מייל: info@audit-fa.co.il