הגנה על הפרטיות
היבטים משפטיים
ופרקטיים

עו"ד מיכאל גילינסקי, שותף
אודיט בקרה וביקורת

מגמות שהביאו לגידול בהיקף הסיכון המשפטי ביחס למידע הנאגר

- גידול בהיקף פעילות הרגולטורים, הרגולציה והסמכויות
- ריבוי ארגונים חברתיים העוסקים בתחומים שונים
- גידול השימוש במנגנוני "אכיפה פרטית" (תביעות)
- מהירות העברת המידע – רשתות חברתיות
- גיוון בכלים המשפטים – תובענות ייצוגיות, תביעות נגזרות, "ידיד בית המשפט", "עותר ציבורי" ועוד
- הגברת החקיקה בנושא זכויות הציבור וגידול במודעות לזכויות אלו (קמפיינים של הרגולטור)
- ריבוי במידע הנאגר

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'...

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 שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף**;

קצת הגדרות

"**<u>מידע רגיש</u>**" - (1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו

(2) מידע ששר המשפטים קבע שהוא מידע רגיש

אודיט
בקרה וביקורת

חובת רישום מאגר

8(א) לא **<u>ינהל</u>** אדם ולא **<u>יחזיק</u>** מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:

(1) המאגר נרשם בפנקס

(2) הוגשה בקשה לרישום המאגר

(3) המאגר חייב ברישום ... והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו

(ב) לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר

אודיט
בקרה וביקורת

מהו מאגר המחייב רישום?

- יש במאגר מידע רגיש
- מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000
- המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה
- המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג
- המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23

אודיט
בקרה וביקורת

רקע כללי

<u>זכות העיון</u>

13. (א) כל אדם זכאי לעיין בעצמו, או על ידי בא-כוחו שהרשהו בכתב או על ידי אפוטרופסו, במידע שעליו המוחזק במאגר מידע.

<u>החובה לאבטח את המידע ששמור במאגר</u>

17. בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע.

אודיט
בקרה וביקורת

השינוי הגדול – תקנות הגנת הפרטיות (אבטחת מידע)

- קביעת רף נדרש לאבטחת המידע
- קביעת אבחנה בין רמת הפעילות הנדרשת לסיכון הגלום במאגר לפי 3 פרמטרים: סוג המידע האגור, כמות המורשים להכנס למאגר וכמות היישויות עליהם אגור המידע
- חובת מינוי גורם אחראי
- הגדרת "אירוע אבטחה" - אירוע שנעשה בו שימוש (מלא או חלקי) במידע מן המאגר, בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע

אודיט
בקרה וביקורת

הפרמטר	בסיסית	בינונית	גבוהה
סוג המידע	המידע משמש לניהול עסק בלבד, אינו כולל מידע נוסף (א,ג,ד,ז) מלבד מידע המפורט להלן הכולל <u>תמונות פנים בלבד</u>: (ב) מידע רפואי או מידע על מצבו הנפשי של אדם; (ה) מידע על אודות עברו הפלילי של אדם; (ו) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007; (ז) מידע ביומטרי; מידע המתייחס לעובדים וספקים של בעל המאגר וכולל מידע מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם.	1) ... שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק... (2) ...בעליו הוא גוף ציבורי... (3) מאגר מידע הכולל מידע שהוא אחד מאלה: (א) מידע על צנעת חייו האישיים של אדם, לרבות התנהגותו ברשות היחיד; (ב) מידע רפואי או מידע על מצבו הנפשי של אדם; (ג) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000; (ד) מידע על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם; (ה) מידע על אודות עברו הפלילי של אדם; (ו) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח-2007; (ז) מידע ביומטרי; (ח) מידע על נכסיו של אדם, חובותיו והתחייבויותיו הכלכליות, מצבו הכלכלי או שינוי בו, יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם; (ט) הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים (א) עד (ז) או על אישיותו של אדם, אמונתו או דעותיו.	כמו בינונית – לא כולל גוף ציבורי
בעלי הרשאה	עד 10	בין 11-99	מעל 100
מספר רשומות	כל כמות	עד 100,000	מעל 100,000

אז מהן החובות?

<u>כתיבת מסמך הגדרות מאגר - הכולל</u>

תיאור כללי של **<u>פעולות האיסוף והשימוש</u>** במידע

תיאור **<u>מטרות</u>** השימוש במידע

סוגי המידע השונים הכלולים במאגר המידע

פרטים על **<u>העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה</u>** ...

פעולות עיבוד מידע באמצעות מחזיק

הסיכונים העיקריים של פגיעה באבטחת המידע, וההתמודדות עמם

שמו של **מנהל מאגר** המידע, של **מחזיק המאגר** ושל **הממונה על אבטחת מידע** בו, אם מונה כזה

בדיקת עדכניות המסמך **<u>ובדיקה של כמות המידע הנאגר</u>** – **אחת לשנה** (האם כל המידע אכן נדרש)

<u>מינוי ממונה על אבטחת מידע</u> (למחזיק מעל 5 מאגרים המחייבים רישום) – היעדר ניגוד עניינים והקצאת משאבים

אודיט
בקרה וביקורת

אז מהן החובות?

<u>הטמעת נוהל אבטחה</u> – כולל בין היתר את החובה לכלול את "הסיכונים שחשוף להם המידע שבמאגר...לרבות אלה הנובעים ממבנה מערכות המאגר...אופן קביעת סיכונים אלה, ואופן הטיפול בהם..."

- ❑ מיפוי המאגר
- ❑ מבדקי חדירה וסקרי סיכונים (ברמה הגבוהה)
- ❑ אבטחה פיזית וסביבתית
- ❑ ניהול כ"א – מגבלת הרשאות, בדיקות, הדרכות וכדו'
- ❑ ניהול ובקרת הרשאות
- ❑ מדיניות "נתיקים"
- ❑ הגנת התקשורת
- ❑ מיקור חוץ
- ❑ ביקורות
- ❑ החובות החלות על בעל המאגר חלות גם על המחזיק בשינויים המחוייבים

אודיט
בקרה וביקורת

לא לשכוח – הטיפ החשוב ביותר!

הרשם **<u>רשאי</u>**, אם ראה כי קיימים טעמים שמצדיקים זאת, **לפטור מאגר מסוים מחובות אבטחת מידע לפי תקנות אלה**, או להחיל על מאגר מסוים חובות לפי תקנות אלה, כולן או חלקן, לפי נסיבות העניין, ובין השאר בהתחשב **בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר או מספר בעלי ההרשאות בו**

הסנקציות הפליליות

31א. (א) העושה אחד מאלה, דינו - מאסר שנה:

(1) מנהל, מחזיק או משתמש במאגר מידע בניגוד להוראות סעיף 8
(2) מוסר פרטים לא נכונים בבקשה לרישום מאגר מידע כנדרש בסעיף 9
(4) אינו מקיים את הוראות סעיפים 13 ו-13א לענין זכות העיון במידע המוחזק במאגר מידע, או אינו מתקן מידע על פי הוראות סעיף 14
(5) מאפשר גישה למאגר מידע בניגוד להוראות סעיף 17א(א)

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? (ברשותנו, ענן, מחזיק 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

כמה סיפורים מהחיים

- ההבדל בין המשפטי לטכנולוגי - מה בין "מערכת" או אפליקציה למאגר
- רמת האבטחה הנדרשת - רגישות "שאינה רגולטורית" (מאגר של ארגון החולים ב.... שמכיל מעט רשומות ומעט משתמשים - האם ברמה הבסיסית?!)
- ספק שירותים / מחזיק מאגר - איפה עובר קו הגבול
- החלת הוראות החוק על משתמשים שאינם עובדי הארגון
- דילמת ה-PAPERLESS – לסרוק או לא לסרוק, זאת השאלה...
- טיפול במידע עודף

אודיט
בקרה וביקורת

שאלות

אודיט
בקרה וביקורת

תודה!

עו"ד מיכאל גילינסקי, שותף
אודיט בקרה וביקורת