



הרשות למשפט,  
טכנולוגיה ומידע



מדינת ישראל  
משרד המשפטים

## היכרות עם הרשות למשפט טכנולוגיה ומידע אבטחת מידע לצורך הגנת הפרטיות



עמית אשכנזי, מנהל המחלקה המשפטית  
הרשות למשפט, טכנולוגיה ומידע



- סקירה קצרה על הרשות למשפט טכנולוגיה ומידע
- הגנת הפרטיות במאגרי מידע
  - עקרונות פרק ב' לחוק הגנת הפרטיות והמצב בעולם
  - פעילויות רלבנטיות מתוכננות של הרשות
- הצגת טיוטת תקנות הגנת הפרטיות (אבטחת מידע)



# היכרות עם הרשות למשפט טכנולוגיה ומידע



## הרשות למשפט, טכנולוגיה ומידע: תרשים ארגוני





## ■ הגנת הפרטיות במאגרי מידע במובן הרחב

### ■ חוק חתימה אלקטרונית

- תיקון מס' 2 – פרויקט תעודת הזהות החכמה
- מעקב אחר מגמות טכנולוגיות והכנת עדכוני תקנות

### ■ ראיות וארכיבאות אלקטרונית

### ■ סיוע בפרויקטי "ממשל זמין" (לפי הצורך)

- דיווחים לרשות המסים
- מצהרים
- מגנ"א (רשות ני"ע)
- סד"א – במ"ה
- "בחירות באמצעים ממוחשבים"
- מכרזים מקוונים

### ■ פעילות בינלאומית [חלקי]

- הכרה בישראל כ- "נאותה" לפי דיני הפרטיות האירופאים
- OECD/WPISP
- FESA



## הגנת הפרטיות במאגרי מידע – פרק ב' לחוק



- חוק יסוד: כבוד האדם וחירותו ועקרון המידתיות
- פרק א' לחוק הגנת הפרטיות - עוולות הפוגעות בפרטיות, לאו דווקא מידע
- פרק ב' לחוק – רגולציה שמטרתה הגנה וצמצום החשש מפני פגיעה בפרטיות בדרך של שימוש לרעה ב-מידע אודות אדם הנאגר במאגר מידע
- התמודדות עם הסיכונים המיוחדים הקשורים בצבירה ועיבוד מידע ממוחשב – קלות הגישה, ההעתקה וההפצה.
- ההסדר מבוסס על שני אדנים-

– אדן משפטי – המותר והאסור [הסכמה, הרשאה חוקית]

– אדן אבטחתי – התמודדות עם סיכונים -אבטחת מידע

\*יש גם הסדרים נוספים [איסור האזנת סתר, נתוני תקשורת, דואר זבל, שירות נתוני אשראי, איסור הלבנת הון]



## OECD ■

- עקרונות הגנת הפרטיות במאגרי מידע והעברות מידע (1980)
- הגברת שיתופי פעולה באכיפה בינגבולית

## אירופה ■

- האמנה האירופית לזכויות אדם
- אמנה 108 של מועצת אירופה
- דירקטיבה EC/95/46

## מדינות APEC [כולל אוסטרליה וניו זילנד] ■

## קנדה ■

## ארה"ב ■

– FTC section 5

– DHS

– HIPPA





- "מידע" – מידע אודות אדם מזוהה
- קבלת מידע ב- "הסכמה מדעת"
- הסכמה מדעת – האמנם?
  - עובדים
  - צרכנים
  - קטינים
  - עקרונות העיבוד
- מניעת שימוש בניגוד למטרה [סעיף 2(9) לחוק]
- אבטחת מידע – "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין"
- שקיפות (ס' 11)
- עיון ותיקון
- מחיקה כשלא נדרש
  - דיוור ישיר
  - פרק ד' – העברת מידע בין גופים ציבוריים
  - הקפדה על עקרונות אלה גם במיקור חוץ



- המידע האישי חשוף לסיכונים גוברים בשל הקישוריות וקלות העברה והעתקה של מידע
- נושא מהותי ללקוחות ובעל השפעה על מוניטין
- יכול ליצור סיכונים משמעותיים וחשיפה משפטית
- עלול לפגוע בפעילות העסק
- מודלים עסקיים - מיחשוביים חדשים ("ענן") לעיבוד מידע אישי במסגרת פעילות העסק



International Chamber of Commerce®  
The world business organization®

## Policy and Business Practices

Now open  
**758** ICC Hearing Centre

Learn more  
ICC on CNN

Learn more  
Incoterms

7<sup>th</sup> World Chambers Congress  
Mexico, 8-10 June 2011

ICC RESEARCH FOUNDATION

ICC 90th anniversary

- What do we do?
- How does it work?
- Become a member
- Leadership
- Task Forces
- Contact us

Topics  
Internet & Telecoms infrastructure &

E-business, IT & Telecoms

**ICC Commission on E-Business, IT and Telecoms (EBITT)**

**Task Forces**

*Task Force on Privacy and the Protection of Personal Data*

**Chair** - Christopher Kuner (Hunton & Williams, Belgium)

**Data Protection and Privacy**



- פיקוחי רוחב מגזריים
- בדיקת תלונות לא מתואמת מראש
- קנסות מנהליים
- הנחיות
- שינוי חקיקה ותקנות (בחודשים הקרובים)
  - עדכון תקנות הגנת הפרטיות (אבטחת מידע)\*
  - תזכיר הגנת הפרטיות (אכיפה)\*
  - עדכון תקנות הגנת הפרטיות (עיון ותיקון)\*
  - עדכון תקנות הגנת הפרטיות (העברות מידע לחו"ל)\*
  - המלצות בנושא ניהול מאגרי מידע במסגרת יחסי עבודה
- \* בתיאום עם מחלקת ייעוץ וחקיקה במשרד המשפטים
- נוהל preruling



# הגנת הפרטיות במאגרי מידע – אבטחת מידע

[עיקרי ההסדר]



## ■ סעיף 17 לחוק:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע."  
סעיף 3 לחוק - "אבטחת מידע" –  
"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;"



"מערכות מידע רבות לא נועדו מלכתחילה להיות בטוחות. האבטחה שניתן להשיג באמצעים טכניים היא מוגבלת, והיא זקוקה לתמיכה הולמת של ניהול ונהלים. זיהוי אמצעי הבקרה המתאימים דורש תכנון זהיר ושימת לב לפרטים. ניהול אבטחת המידע בארגון נזקק קודם כל לשיתוף פעולה של כל העובדים. לפעמים יש גם צורך בשיתוף פעולה של ספקים, לקוחות או בעלי מניות, ואף בייעוץ של מומחים שמחוץ לארגון. הכללת אמצעי הבקרה לאבטחת המידע בשלב הגדרות הדרישות והתוכן, תהיה באופן משמעותי זולה יותר ואפקטיבית יותר לעומת הכללתם בשלב מאוחר יותר." [ת"י 7799, מבוא, עמ' 2]



- הפחתת הסיכונים לשימוש לרעה במידע אישי
- אחריות כוללת של הארגון לאבטחת מידע במאגר
- הבהרת אחריות ארגונית ואישית לקיום ההוראות
- הגברת מודעות ההנהלה והעובדים של בעל מאגר לאבטחת מידע
- תכנון לפרטיות
- כלים ונהלים מקובלים להקטנה של הסיכונים למידע
- מודולריות





- הגדרה ברורה של הנהלת הארגון חיונית למימוש האחריות הניהולית של בעל המאגר.
- אפיון של המידע המצוי במאגר
- בחינת האיומים
- אופן ההתמודדות עם האיומים
- תיאום פנים ארגוני בין הפונקציות הרלבנטיות השונות
- דיון תקופתי



- שפה ארגונית משותפת
- קביעת הרשאות גישה
- הוראות קבע בתחום אבטחת מידע
  - אבטחה פיזית
  - אופן בקרה
  - אבטחת מערכות התקשורת
  - התקנים ניידים
  - גיבוי ושחזור
  - ביקורות



- יש להטמיע את שיקולי אבטחת מידע בעת עיצוב המערכת.
- האם המידע נאסף או נשמר אינו מעבר לנדרש לשימוש מטרות המאגר.
- האם מטרות המאגר מאפשרות שימוש במידע בדרך שתאפשר שמירה על האנונימיות של נושא המידע.
- יש להקפיד על מניעת סיכונים מיותרים בכל החלטה הקשורה במאגר.



## ■ אבטחת מידע בניהול כוח אדם

- קליטת עובדים ומיון לפי רגישות המשרה
- הדרכה
- התחייבות לשמירת סודיות

## ■ ניהול הרשאות גישה

- גישה בהיקף ובמידה הנדרשים בלבד
- ניהול רשימת הרשאות תקפות
- [הפרדת תפקידים]

## ■ זיהוי ואימות

- תיעוד גישה [רמה בינונית וגבוהה]



## ■ התקנים ניידים והסיכונים הקשורים בהם

– רישום

– הצפנה

## ■ תקשורת [קישוריות לאינטרנט ולדוא"ל]

– הפרדה בין מערכות ורשתות

– מערכות אנטי וירוס ופיירוול

– הצפנה

– סיכונים הקשורים בגישה מרחוק של עובדים ולקוחות



- הגדרה ברורה של המידע, השירות והסיכונים חיונית למימוש האחריות הניהולית של בעל המאגר.
- אפיון של המידע והגדרת השירות
- בחינת האיומים והסיכונים
- [לדוגמא]
- הוצאת עותקים של המאגר
- גישה מרחוק
- אופן ההתמודדות עם האיומים
- תיאום פנים ארגוני בין הפונקציות הרלבנטיות השונות
- הפנמה של מחיר הסיכון לעלות השירות וכדאיותו
- הסדרה של החובות שמטרתן הקטנת הסיכון



- תכנון לפרטיות - הטמעה של שיקולי אבטחת מידע
- אופן בחירת הקבלן [מניעת חשש לניגוד ענינים]
- הוראות ברורות לעניין מטרת השימוש והגישה למידע
- [מנגנוני תיאום עם הקבלן]
- הוראות בנושא אבטחת מידע והפרדה בין שירותים
- הוראות בנושא עובדים והדרכה
- קביעת מנגנוני דיווח/מסירת מידע ובקרה
- מערך סעדים אפקטיבי
- הוראות בעניין מחיקה בתום השירות



- שימוש במומחים
- תיעוד אירועי אבטחה
- לימוד מאירועי אבטחה
- ביקורות פנימיות ו/או חיצוניות





## דרישות הרמה הגבוהה





■ דוא"ל (להצטרפות לרשימת תפוצה):

[ilita@justice.gov.il](mailto:ilita@justice.gov.il)

■ אתר (להגשת תלונות ולעיון

במידע): [ilita.justice.gov.il](http://ilita.justice.gov.il)

■ כתובת: קריית הממשלה, קומה 9, מנחם בגין 125, תל-

אביב