

1285.41 - אנשי מקצוע מנתחים

כך שמענו, משלושה מומחים מובילים בתחום הפרטיות:



עו"ד יורם הכהן, הוא מנכ"ל איגוד האינטרנט הישראלי, שבתפקידו הקודם, הקים ועמד בראש הרשות למשפט, טכנולוגיה ומידע (רמו"ט), במשרד המשפטים ☎ 9700900 (www.isoc.org.il). לדבריו, מצב השמירה על הפרטיות בארץ דומה לאירופה, מבחינת חובת רישום מאגרי מידע ומתן זכות עיון במידע לאדם, שפרטיו נשמרו. חובה נוספת היא ליידע אדם, שפרטיו נאספים, האם הוא חייב למסור פרטים אלו מתוקף חוק, איזה שימוש ייעשה בפרטים אלו והאם הם יימסרו לגורם נוסף. חובות נוספות, שמוטלות על הארגון, הן אבטחת מאגר הפרטים האישיים וחובות, שקשורות לשימוש במידע לדיוור ישיר. **רשם מאגרי המידע** הוא גוף הרגולציה שמטפל בכך והוא בעל סמכויות פיקוח, חקירה פלילית והוצאת הנחיות, שנוגעות למאגרי מידע. קיימת מגמת עיסוק הולך וגובר בפרטיות, כיון ששומר יותר מידע, כולל מידע, שמופק באופן אוטומטי, כמו קבצי לוג וחיישני IoT, ומתפתחות שיטות חדשות לניתוח המידע. לכן, מנמ"רים צריכים לקחת בחשבון, שפיקוח הרגולציה יגבר וגם מודעות הצרכנים לפרטיות תעלה. ארגונים נוטים לשמור מידע רב, מאחר שהיום האחסון והעיבוד זולים וזמינים, דבר שעלול להפר תקנות רגולציה ולגרום לחשיפת מידע רב במקרה פריצה. מומלץ ליישם תפיסת **Privacy by Design**, שדוגלת בתכנון היבט הפרטיות כבר בזמן תכנון והקמת מערכות מידע. כחלק מהתפיסה, מומלץ לבצע תהליך **Privacy Impact Assessment**, שייסקור כיצד שמירה על הפרטיות, משפיעה על מערכות מידע. כמו כן, מומלץ לחבר בין אנשי הטכנולוגיה לבין מומחים, שמכירים את דרישות החוק, בעוד שאבטחת מידע עוסקת לרוב בגישת גורם לא לגיטימי למידע, פרטיות עוסקת גם במצב בו גורם לגיטימי, משתמש במידע באופן לא ראוי. למשל, מעביד, שעוקב אחרי גלישת העובדים באינטרנט, בכדי לזהות פריצת אבטחה. בית המשפט פסק, שלעובדים יש זכות מסיימת לפרטיות בגלישה, גם במקום העבודה. בנוסף, חשוב שמנמ"רים יידעו, שמעבר לענן כרוך לרוב בהעברת מידע לחו"ל וישנן מגבלות בחוק, שצריך לקחת בחשבון.

לדברי נעמי אסיא, מייסדת ומנהלת משרד עורכי-דין ועורכי פטנטים נעמי אסיא ושות' ☎ 03-6444808, באוקטובר 2015 התקבל **באיהוד** - **האופי** פסק דין, שניתן בעקבות תלונת אזרח אוסטרי כנגד העברת מידע מפיפבוק אירלנד לארצות הברית, אשר ביטל הנחיות, שמתירות הוצאת מידע פרטי של אזרחי האיחוד לארה"ב, באופן אלקטרוני. פסק דין זה, שתקף גם לישראל, יצר אנדרלמוסיה והצריך קבלת הנחיות חדשות, מטעם הרשות למשפט וטכנולוגיה. לפי חוק הגנת הפרטיות, המנמ"ר או מנהל מאגר המידע צריך לרשום מאגרי מידע, שנמצאים ברשות הארגון ולמלא אחר הנחיות אבטחת המידע. בנוסף, **רשות התקשוב** הממשלתית הוציאה מסמך, שמנחה לגבי אבטחת המידע בענן. על המנמ"ר להכיר את החוק ולהיצמד אליו. מותר להשתמש בנתונים שברשות הארגון, רק למטרה, שלשמה הם נאספו. כדי להשתמש בהם למטרה אחרת, יש להשיג הסכמה מפורשת של האדם אליו מתייחס המידע, עבור המטרה החדשה. התקפות סייבר על ארגונים הפכות לנפוצות יותר ולכן אבטחת הנתונים הופכת למאתגרת יותר. בנוסף, **הרשות למשפט וטכנולוגיה** תגביר אכיפה במקרים של הגנה לא מספקת על פרטיות, לכן, חשוב להתעדכן בהנחיות **רשות התקשוב**, מנמ"ר, שלא ינקוט באמצעי האבטחה הנדרשים, ייחשב לרשלן ויחולו עליו ועל ארגונו סנקציות.



לדברי אבנר בן אפרים, מנכ"ל חברת אב-סק ☎ 050-5798132, כבר היום, חברות הענק הן חברות ידע, שאוספות מידע והמצב רק ילך ויחמיר. למשל, דרך אפליקציות, שמבקשות גישה לכל מידע אפשרי. במקביל, מתפתחים יותר כלים לניתוח מידע זה. הארגון אומנם יכול



לאסור שימוש באפליקציות מסוימות, אך במידה והעובד משתמש במכשירו האישי, שמשדר את המיקום, אפשר יהיה לעקוב אחריו. גופים עסקיים עלולים לנצל מידע אישי של לקוחות, כפי שהוא משתקף בשימוש באינטרנט. למשל, בנק עלול לגבות ריבית גבוהה על הלוואה, אם מבקש אותה לקוח, שפרסם פוסט על מצבו הכלכלי הרעוע. חברת ביטוח עשויה לסרב לבטח אדם, שערך חיפוש על מחלת הסרטן. אם בעבר,

מועמד לעבודה היה צריך להביא ממליצים, היום עורכים עליו חיפוש ברשתות חברתיות. לכן, מידע על חשד שפורסם בעבר, יפגע באדם לטווח ארוך מאוד. בנוסף, עולה הלגיטימיות למעקב אחר לקוחות ועובדים, הפצת מידע חסוי לאינטרנט ושיימוג. אומנם קיים חוק להגנת הפרטיות, אך הוא נאכף בצורה מוגבלת. חשוב שארגונים ועובדים ידעו את גבולות החוק. למשל, איזה תוכן מותר לקרוא והיכן מותר לשים מצלמות. למעסיק אסור לדעת לאילו אתרים העובד גולש בזמן העבודה, אם לא מדובר באתרים, שהגלישה אליהם נאסרה במפורש. לעובדים במיוחד, אין מספיק ידע בנושא. לכן, חשוב שתהייה גישה לייעוץ משפטי או גורם מארגון עובדים, שמתמחה בתחום. פרטיות היא היבט נפרד מאבטחה ואולי היום הלכנו רחוק מדי מבחינה זו. למרבה הצער, בארץ יש פחות מודעות לשמירה על פרטיות. מידע על חיפוש באינטרנט למשל, יכול תיאורטית להישמר לנצח. באירופה, בעקבות מחאה ציבורית, גוגל הוגבלה לשמירת פרטי חיפוש ל-3 שנים בלבד.

1285.42 - טיפים לשמירה על פרטיות

אלו כמה טיפים מסייעים, לשיפור הטיפול בפרטיות:

- **ריבוי פרצות** - כיוון שארגון מתקשר עם לקוחות וספקים במגוון ערוצי התקשורת, שרק הולך ומתרחב, הסיכון לפריצה ופגיעה בפרטיות, גדל גם הוא. לכן, לפני שמיישמים ערוץ תקשורת חדש, חיוני להעריך את פוטנציאל הפגיעה בפרטיות ממנו ולהתכונן בהתאם.
- **גניבה בחשאי** - כדאי לזכור, שתקיפה, שמטרתה גניבת פרטים, עשויה להישאר חשאית לאורך זמן רב, להימשך תקופה ארוכה או שלא להתגלות כלל. זאת, להבדיל מתקיפה, שמטרתה לשבש פעילות, שלרוב מתגלה תוך זמן קצר מרגע התרחשותה.
- **הימנעות ממחשוב** - במקרים מסוימים, בהם נחשף מידע רגיש במיוחד, כדאי לשקול לצמצם שימוש במחשב. למשל, להיפגש באופן אישי ולא להכניס טלפונים ניידים לפגישת או לאתר רגיש.
- **ליידע ולהיות מודע** - חשוב לדרוש מספקים מידע בנוגע לדרכים, שנקטות לשמירת הפרטיות. מה המידע שהם אוספים? ולאיזה צורך הוא משמש? כמו כן, על הארגון ליידע את לקוחותיו בדבר מדיניות הפרטיות שלו ואופני האיסוף והשימוש במידע.
- **כללי אצבע** - אתר **Security Intelligence** מביא 10 כללי אצבע לאבטחת מידע ולשמירה על פרטיות, תוך שימוש במשל על שודדי ים ואוצרות - **bit.ly/42-privacy-best-practices**
- **מוצרים לשמירה על פרטיות** - אתר **CSO** ממליץ על 6 מוצרים, שמסייעים לשמירה על פרטיות במחשב - **bit.ly/42-privacy-products**
- **פרטיות ב-BYOD** - שימוש ב-BYOD, כולל התנתקות תוכנות ניהול להתקנים ניידים במכשיר. הדבר עלול לפגוע בפרטיות העובד, במיוחד אם אינו מקפיד להפריד בין שימוש עסקי לפרטי. אתר **iapp.org** מציע פתרון - **bit.ly/42-byod-privacy**

1285.43 - לשפר באופן שיטתי

אלו הצעדים המומלצים, לשיפור הטיפול בפרטיות בארגון:

1. **הקדשת תשומת לב** - יש להגדיר את נושא הפרטיות כנושא בעל חשיבות ולהקצות זמן ללימוד הנושא, ברמה האישית והארגונית.
2. **תמונת מצב** - חיוני לגבש תמונת מצב של תחום הפרטיות בארגון. האם קיים אחראי לנושא? האם קיימת מודעות לפרטיות במחלקות ובדרגים השונים? האם יש לארגון כלים למניעת פגיעה בפרטיות ולהתמודדות עם פגיעה שהתרחשה? מי הגורמים שרוצים לפגוע בארגון וכיצד הם יכולים לעשות זאת?
3. **שיתוף פעולה** - טיפול יעיל בהיבטי המחשוב של נושא הפרטיות, מחייב שיתוף פעולה, בין המחלקות השונות בארגון לבין המנמ"ר.
4. **ייעוץ** - כיוון שפרטיות היא נושא בינתחומי, חשוב להתייעץ עם גורמים מקצועיים, מתחומי אבטחת המידע, המשפט וכח האדם.
5. **שיפור** - יש להגדיר מהם התחומים שטעונים שיפור, מהם הכלים שעומדים לרשות הארגון לצורך השיפור ומהם המשאבים, שעל הארגון להשקיע.
6. **הגנה** - חשוב להבטיח הגנה על פעילויות רגישות במיוחד, בהן מחשוב נייד, מחשב ענן חוץ ארגוני, רשתות חברתיות וגלישה באינטרנט. כמו כן, יש להמשיך בניסור ההתפתחויות, האיזמים והפתרונות בתחום זה.