

AYR

עמר רייטר ז'אן שוכטוביץ ושות'

מאי עד אוקטובר
מה למדנו?

אייל שגיא, עו"ד



דיווח על אירוע אבטחה – פרקטיקה

- קשיים טכניים
- תוך 24 שעות ממועד גילוי האירוע; עד 72 שעות ממועד גילוי האירוע
- שעות, לא ימי עבודה...
- שאלות שחובה לענות בדיווח "ראשוני":
 - איך קרה האירוע?
 - איזה מידע היה בסיכון?
 - מה מספר הרשומות?
 - כמה אנשים הושפעו?
 - מה ההשלכות?
- האם הנתונים חזרו להיות מוגנים, באיזה אמצעים?
- האם הנתונים מוצפנים?

אירוע אבטחה שיש לדווח עליו



- כל מה שכתוב בתקנות וגם:
 - כשקם חשש סביר לאירוע לאבטחה חמור
 - כשהאקר "כובע לבן" מתריע (אבל לא פרצה שהתגלתה במסגרת בדיקת אבטחה מוזמנת)
 - כשהמידע מוצפן
 - גילוי מידע של הארגון בdark web וכו'
 - גניבה / אובדן של ציוד / דיסקים (לא עניין רק של מחלקת מערכות מידע)
 - הצפנה או מחיקה ע"י וירוס
 - טעות של נציג שירות
 - חשש ממשי של גניבת סיסמא של בעל הרשאת גישה
- זיהוי וודאי של ניסיון גישה במתכוון על-ידי משתמש - אף כשניסיון זה לא צלח Failed login
- אירוע שמישהו אחר כבר דיווח עליו (חוץ ממחזיק / בעל מאגר – בתיאום)

הקלות בדיווח



- "אירועי אבטחה אשר **בשלב זה** הרשות לא תאכוף את חובת הדיווח עליהם...":
- גישה למידע אישי על ידי עובד או ספק חיצוני בניגוד להרשאה, בשוגג ובאופן חד פעמי
- זיהוי ניסיון גישה של עובד פנימי או ספק חיצוני למאגר מידע ללא הצלחה (failed login) בשוגג ובאופן חד פעמי
- התפרצות של וירוס כופר - אך המאגר שוחזר מחדש בהצלחה ולא הייתה כל אינדיקציה כי במסגרת ההתפרצות גם זלג מידע מהארגון
- ניסיונות סריקה/פריצה לתוך רשת הארגון אשר נחסמו על ידי מערכות הארגון
- ניסיונות הדבקה ברשת הארגון אשר נחסמו על ידי מערכות הארגון
- עדיין יש לתעד!

חובת מיפוי מידע



מיפוי טכני – תקנה 5

- מיפוי מערכות
- מערכות חומרה, תוכנה, ממשקים, תרשים רשת, מבנה מאגר ורשימת מצאי..
- סקר סיכונים ומבדקי חדירה (רמה גבוהה)

מיפוי מהותי – תקנה 2

- מסמך הגדרות מאגר
- איך נאסף המידע, מטרות, סוגי מידע, העברות מידע, פעולה באמצעות מיקור חוץ, בעלי תפקידים (מנהל מאגר, ממונה אבטחת מידע וכו')
- עדכון אחת לשנה או בשינוי משמעותי
- בדיקה אם יש מידע עודף

ובינתיים באירופה...



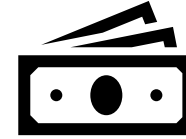
- הצפה
- ה ICO מקבל 500 פניות בשבוע
- שליש מיותרות
- ה CNIL קיבל 600 דיווחים בארבעה חודשים
- אירוע פייסבוק
- בדיקה האם יושם ה GDPR

"מחזיק" ו"גורם חיצוני" בתקנות



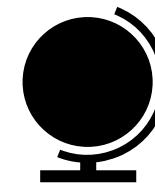
- מחזיק: "מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש"
- מונחון הרשות: "הישות אשר מעבדת את המידע עבור בעל המאגר, קרי ספק מיקור חוץ"
- גורם חיצוני: עמו מתקשרים "לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע"
- תקנה 15(א)(2) – הסכם מיקור חוץ כולל את
- תקנה 15(א)(2)(ה): "אופן יישום החובות בתחום אבטחת המידע **שהמחזיק** חייב בהן לפי תקנות אלה"
- תקנה 19(א) מחילה את התקנות על מחזיק, אבל לא על "גורם חיצוני"

גישה למידע שאינה מיקור חוץ



- המעבד / מחזיק – מעבד מידע עבור בעל המאגר
 - ולכן – המידע חוזר לבעל המאגר בסיום השירות
 - בעל המאגר אחראי לפעילות המחזיק וחובה להתקשר בהסכם כתוב
- הבדל בין "מיקור חוץ" לשירות נוסף:
 - מעסיק שמעביר פרטי עובדים לבנק לתשלום משכורת, ביטוח פנסיוני, כרטיסי שי לחג, לחברה סלולרית, לליסינג
 - חברת ביטוח שמעבירה תשלומים באמצעות בנק
 - תנביס, גט טקסי:
 - מה מעמד נהג המונית / מסעדה?
- אם תקנה 15 לא חלה, מכוח מה מעבירים את המידע
 - מי אחראי לאבטחת מידע, לצמידות מטרה

איזה חוק חל על מיקור חוץ בחו"ל?



- תקנות אבטחת מידע מחייבות הסכם
 - כולל התייחסות לקיום החובות החלות על המחזיק לפי התקנות
 - האם התקנות חלות על מחזיק זר?
- תקנות העברת מידע מתירות העברה לחו"ל בלי כפיפות לחוק הישראלי
 - אפשר "לתרגם" קיום התקנות בהעברה לפי תקנה 8(1) (מדינה חברה באמנה האירופית להגנת הפרט בקשר לעיבוד אוטומטי של מידע רגיש)
 - הנחה שהחוק הזר מעניק רמת הגנה מספקת (אבל מה אומר החוק הרוסי?)
 - יצוא מחוץ לאירופה - תקנה 2(8)(2) ("המקבלת מידע ממדינות החברות בקהיליה האירופית, לפי אותם תנאי קבלה"):
 - אין חלופה ל Privacy Shield, Safe Harbor לא חל
 - אפשר להסתמך על Model Clauses (בינתיים)
 - אבל דין של איזו "מדינה חברה" חל?
- תקנה 2(4): "המידע מועבר למי שהתחייב בהסכם... לקיים את התנאים... החלים על מאגר מידע בישראל, בשינויים המחויבים"
- תקנה 3 = תקנה 15?

איזו אבטחת מידע חלה על מידע אירופי בישראל?



- תיאורטית, רק התקנות:
- “The effect of [an adequacy] decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.”

• בפועל, גם GDPR

• כי כולם מחתימים על DPA

GDPR – תחולה משפטית



- פעילות עיבוד מידע באירופה
- ומחוץ לאירופה אם אנשים שנמצאים באירופה:
 - מנטרים
 - מוצעים להם שירותים או מוצרים
- תחולה חוזית
- תיירים

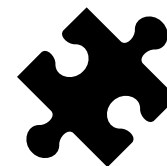
"Your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject to the rules of the GDPR."

GDPR - תחולה טריטוריאלית בפועל



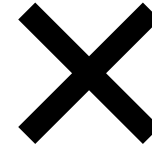
- ממתנים להנחיות מה EDPB
- טיוטה להערות הציבור צפויה בקרוב
- **תכלול הוראות לגבי מינוי נציג**
- אכיפה נגד Cambridge Analytica מקנדה על בסיס "ניטור אנשים שנמצאים באירופה"
- מצד שני – נאסר עיבוד מידע של אזרחי ותושבי האיחוד בלבד (תזכורת: עיבוד כולל אחסון).
- בחרתם מדינה מארחת באירופה?
- אז מה. רגולטור גרמני (יש הרבה) רשאי לאכוף את ה-GDPR גם ביחס לפייסבוק אירלנד
- שימו לב לחקיקה המקומית
- חובת מינוי DPO – הנחיות מקומיות
- תשלום ודיווחים

GDPR – שונות בין המדינות



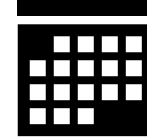
- 'large scale processing' = יש למנות DPO ולקיים DPIA
 - הוצעו 260 סוגי עיבוד
 - החל מ 5000 נושאי מידע (בקשר למידע רגיש) וכלה ב 5,000,000 נושאי מידע
 - חובת מינוי DPA נרחבת בגרמניה
 - חובת דיווח ותשלום בבריטניה

GDPR – הסכמה כבסיס עיבוד



- הסכמה כבסיס עיבוד מאבדת כוח
- הסכמות לא תקפות במקרה של...
- התניית שימוש באפליקציה בהסכמה לעיבוד
- אי הפרדת ההסכמה לכל שימוש ושימוש
- הסכמה לשימוש לא מידתי
- רשימת נעברים לא מלאה
- פערי כוחות בין הצדדים
- מעסיקים צריכים בסיס עיבוד אחר

מה צפוי



- GDPR
 - אכיפה משמעותית ראשונה "עד סוף השנה"
 - הנחיות לגבי תחולה בינ"ל ועוד
 - החלטת adequacy של ישראל
 - ePrivacy
- ישראל
 - אכיפת רחב
 - ייצוגיות – אירועי אבטחה, שימושים משניים במידע, זכות העיון
 - זכות העיון, מחיקת מידע עודף
 - תיקון החוק?

AYR

עמר רייטר ז'אן שוכטוביץ ושות'

תודה רבה

<http://www.ayr.co.il/practice-areas/>
פרטיות-ועיבוד-נתונים

eyals@ayr.co.il

המצגת היא כללית ואינה תחליף לייעוץ משפטי

