Digital Whisper
Technologic Papers

איך לא עומדים ב-GDPR?

מאת עו"ד יהונתן קלינגר

הקדמה

תקנות הגנת הפרטיות (אבטחת מידע) והוראות הרגולציה הכלליות על פרטיות (GDPR) באירופה נכנסו שתיהן לתוקף בחודש האחרון, וכמו כל רגולציה חדשה הן לוו בפאניקה, שהביאה איתה כמה הונאות, נוכלויות ובעיות אחרות. בטקסט הקצר שלנו נדבר על מה לא לעשות כדי לעמוד בתקנות וב-GDPR, ואיך אנשים אחרים יכולים לנצל בורות, חולשה ופאניקה כדי לקדם את האינטרס העסקי שלהם.

מה זה ה-GDPR? תקנות הגנת המידע הכלליות (General Data Protection Regulation) האירופיות הן תקנות חדשות שחלות על כל שימוש במידע של אדם הנמצא באירופה. להבדיל מהחקיקה הקודמת שהיתה באיחוד האירופי, שבה לתושבי אירופה הובטחה הגנה מסוימת, התקנות החדשות הגיעו בזכות הרבה מאוד אקטיביזם, פרשת סנודן ופרשות דומות.

לפי האיחוד האירופי, התקנות חלות על מי שמטפל במידע על תושבי אירופה; כלומר, אם העסק שלך הוא עסק שאינו רלוונטי לתושבי אירופה (נניח, מרכז קהילתי בשפלה) שאינו מספק לתושבי אירופה שירות, התקנות לא רלוונטיות לך.

ה-GDPR הוא מסמך ארוך, בין עשרות עמודים, שקובע רשימה של זכויות כלליות לכל אדם באשר הוא, בעת שאחרים אוספים, שומרים, מעבירים או מעבידים מידע. הראשונה היא הזכות שלו שמידע יעובד רק בצורה לגיטימית (תקנה 5) ובהסכמתו: כלומר, אין אפשרות לאסוף מידע של אדם לצורך מתן שירותי ניתוח אישיות ולאחר מכן למכור מידע זה לצורך אחר. הזכות השניה היא שהוא יקבל מידע על כל השימושים הנלווים למידע; כלומר, שאם המרכול שאני רוכש ממנו מוצרים מעביר מידע על הרכישות שלי לספקים שלו, אני לא רק אדע על כך, אלא ההעברה הזו תהיה רק כדי להגשים את אינטרס הרכישה שלי.

הזכויות הנוספות שנלוות לאנשים (נושאי מידע, כהגדרתם ברגולציה) הן הזכות לכך שהם יוכלו לקבל עותק מהמידע (תקנה 15) וכי אם משהו במידע לא נכון הם יוכלו לתקנו) תקנה 16 (יש עוד זכות, שמוגדרת בטעות כ"זכות להשכח", והיא הזכות להמחק ממאגרי מידע שאינם רלוונטיים עוד; כלומר, הזכות של אדם לבקש מחיקה של מידע ישן, לא מעודכן, ושאינו נחוץ. אם המידע עדיין נחוץ (לדוגמא, פרטי תשלום לחשבוניות), אזי אין חובה למחוק אותו.

יש לכל אדם גם את הזכות לקבל הודעה כאשר מתחילים לאסוף עליו מידע שלא בידיעתו. כלומר אם קיבלתי את המידע על כל תושבי פתח תקווה מספר טלפונים, ואני מתחיל לאגור את המידע ולהשתמש בו בתור Call-Center לפעילות של טלמרקטינג, הרי שאני חייב לשלוח לכל תושבי פתח-תקווה הודעה על כך.

יש לאדם גם את הזכות כי יפסיקו להשתמש במידע עליו; כלומר, שאף אם עדיין אוגרים את שמו ואת מספר הטלפון שלו, הרי שמותר לו לבקש כי לא יתקשרו אליו יותר, או כי לא ישתמשו במידע עליו לצרכי הצגת פרסומות.

לסיום, לכל אדם יש את הזכות לנייד את המידע שלו, מתוך הבנה שהמידע הוא קניין כמו כל דבר. כל אדם זכאי לקבל עותק מהמידע בצורה שהיא קריאת-מחשב (Machine Readable) ותאפשר לו לנייד את ספק השירותים שלו לצד שני.

יש עוד אגד זכויות בחוק הארוך במיוחד, אבל העקרונות ברורים: התקנות נועדו לייצר מצב שבו אנשים שולטים במידע שאחרים אוספים עליהם.

הבעיה העיקרית היא שבעוד שלתאגידי ענק כמו גוגל ופייסבוק קל מאוד (יחסית) לעמוד בתקנות האלו, שכן יש להן את כח המחשוב וצבא עורכי הדין כדי לעמוד בהן, לאנשים אחרים, העסקים הקטנים, יהיה קשה מאוד לעשות זאת.

מה הן תקנות אבטחת מידע?

במקביל להוראות ה-GDPR, ובערך באותה תקופה, יצאו לאור תקנות אבטחת מידע בישראל. התקנות הישראליות אמנם לא נוקשות כמו ה-GDPR, אבל הן מחייבות חשיבה מחדש. הגם שהתקנות מאוד טכניות במהותן, יש בהן שני עקרונות חשובים: הראשון הוא שכל מאגר מידע שמוקם, כל איסוף של מידע, חייב להעשות כאשר בבסיסו יש תכנון של מבנה המאגר, יש מיפוי של המידע שנכנס ויוצא ובדיקה של הדרכים בהן המידע מושג. רק לאחר כל אלה, ניתן להקים את המאגר. לאחר מכן יש להחזיק בדיקות של הסיכונים בפגיעות במאגר. כלומר, לבחון מה יקרה במקרה שבו המאגר ידלוף, יפרץ, ימחק או יושחת. אותן בדיקות הן משהו שרוב הארגונים בכלל לא חוו במהלך הקיום שלהן. עד היום הנחת המוצא היתה כי המאגרים מאובטחים ודי בכך (אפשר לקרוא עוד כאן).

איך עומדים בהוראות האלה בכלל? ההנחיות הרבות שמוטלות הן לא משהו שקל לעמוד בו. חלק ניכר ומהותי מהארגונים לא רק שלא ערוכים להנחיות, לתקנות ולחוקים אלא שלא יכולות להערך לכך. משרדים שאספו במשך שנים מידע במאגרים שונים לא יודעים למפות מהם המאגרים שיש להם, ולא בטוח שיכולים לעמוד בהוראות ה-GDPR או התקנות הישראליות. לדוגמא, מעצב שיער, שאסף לאורך השנים את הפרטים של כל הלקוחות שלו והיה שולח להם מדי פעם מסרונים על מבצעים ושעות פתיחה, היה צריך עד היום לעמוד רק בהוראות חוק הספאם כדי לוודא הסכמה.

כרגע, הוא צריך לאתר את כל אחד מהלקוחות ולבדוק האם הוא יכול להמשיך לשלוח להם הודעות; ויותר גרוע, להתחיל לבדוק איך מאוחסן קובץ האקסל שלו, למי יש גישה למאגר ולהחתים את קבלני המשנה ששולחים עבורו על שלל הסכמים.

האם הוא יכול לזהות, לאתר, למפות את כל המערכות האלו? כנראה שלא. האם יש לו את הכסף לשלם לעורכי דין לעשות זאת? גם די בטוח שלא. כלומר, למעצב השיער נותרו שתי ברירות: לעבור על החוק ולהמשיך לשלוח הודעות או למחוק את המידע ולהיות מעצב שיער שלא שומר מידע.

האם יש נוסחת קסם?

יש תוכנה שתעשה לי את זה? אנשים נוטים לשים בטחם בטכנולוגיה במקום בעקרון. אין תוכנת קסם שתקח את מאגר המידע שלך ותהפוך אותו לתואם GDPR, כמו שאין תוכנת קסם שיכולה לקחת את ביל קוסבי ולהפוך את האונס שביצע לחוקי. אם אספת מידע ואין לך תיעוד של דרכי קבלת ההסכמה, אין לך מיפוי של מאגרי המידע שלך ותיעוד של הסיבות להן אתה באמת צריך את המידע, אז מה לעשות? אתה בבעיה.

יותר מזה, גם עורכי דין הם לא הפתרון שלך. בעבר, עורכי דין היו מנסחים הצהרות פרטיות בהן היה כתוב שבעצם ההרשמה לאתר אתה מסכים שמידע עלייך יועבר למפרסמים. היום, בעידן ה-GDPR בהתאם לחוק הישראלי, אי אפשר לעשות זאת. העברת המידע מותרת רק אם יש צורך לכך בעת אספקת השירות.

כלומר השאלה היא לא "אלו מילות קסם יכולים עורכי הדין לכתוב כדי שאנחנו נעמוד בחוק", אלא "מה אנחנו צריכים לשנות במערכת שלנו כדי לעמוד בחוק". ההבדל בין השאלות האלו הוא משמעותי. עורכי דין הם לא הפתרון, הם הבעיה.

האם יש לוגו או אישור שאני יכול להציג באתר כדי להראות שאני עומד בהוראות ה-GDPR? יש תעודה שמקבלים או הסמכה? התשובה היא לא. להבדיל מתקנים כמו PCI-DSS, של כרטיסי האשראי, או-ISO 27001, של אבטחת מידע, אין תקן רשמי של "אני עומד בהוראות החוק". הסיבה לכך, ובכן, היא כי כולם צריכים לעמוד בהוראות החוק. כלומר, אם אתה לא עומד ב-GDPR ואתה מספק שירותים לתושבי אירופה אתה בבעיה.

יש הרבה אנשים שחושבים כי אפשר להשיג תעודות כאלה ואחרות, ויש גורמים שמציעים תעודות כאלה ואחרות, וגם עורכי דין קופצים על העגלה. אבל בפועל, שום דבר לא מחליף חשיבה הגיונית, טובה, מלאה, על איך לנהל את מאגרי המידע שלך.

מה זה PBD, ולמה צריך לעשות חשיבה על כל המאגרים

עיצוב לפרטיות, הנדסה לפרטיות, Privacy By Design, זו מתודה שלמה שדורשת חשיבה. המתודה הזו מתחילה קודם כל בשאלה: מה המידע המזערי שאני צריך לשירות שלי, ואיך אני משתמש בו לצורך מתן השירותים בלי לחשוף את הלקוחות שלי לסיכונים.

עיצוב לפרטיות הוא משהו שלוקה בחסר בישראל. הסיבה הראשונה היא כי עסקים ישראלים חושבים על לשמור קודם ואז לטפל. כלומר, בשלב הראשון הם רוצים לוודא שיש להם את כל המידע, שאפשר לנתח את הכל ולבדוק אם הוא נחוץ, ורק לאחר מכן להחליט מה עושים איתו. החשיבה הזו מסוכנת; היא סוג החשיבה שהביאה עלינו את המאגר הביומטרי והיא סוג החשיבה שמאפיינת מערכות מחשוב ישראליות.

לדוגמא, כאשר המדינה אפיינה את מערכת מרכב"ה (מערכת רצינית כאשר בונים הגנה, או ראשי תיבות מיותרים אחרים), היא בנתה אותה כך שליותר מדי אנשים יש הרשאות גישה אליה גם אם הם לא עובדי מדינה. כך גם את המערכת של רשות המסים, שעוצבה כך שכל עובד של רשות המסים יכול לגשת לכל תיק, גם אם הוא לא תיק של המחוז שהוא מטפל בו.

כלומר, השאלה הראשונה היא האם אתה סומך על העובדים שלך, או שאתה מתכנן מראש מערכת שתמנע שימוש לרעה. לדוגמא, מערכת של ביטוח לאומי מאפשרת לעובדים של חברה חיצונית לגשת למידע. כשנבנתה המערכת, לא הותקנו אמצעים לוודא כי רק מי שמזדהה מול צד שלישי יכול לתת לעובד החיצוני גישה למידע, אלא לעובדים יש גישה כמעט ולא מוגבלת למאגר המידע. כלומר, העיצוב מראש היה צריך להיות בנוי כך שהוא לא יאפשר שימוש כזה.

אז השאלה הראשונה היא "איך בונים מערכת שתקח את המינימום ההכרחי". השאלה מהו המינימום ההכרחי היא לא תמיד כל כך ברורה. לדוגמא, אם יש לנו מאגר מידע ואנחנו צריכים מזהה ייחודי, הרבה פעמים אנחנו רצים ואומרים "תעודת זהות!". אבל האם זה חכם? בשנת 2012, אחרי פרשת "ההאקר הסעודי" הצעתי בועדה בכנסת כי עסקים לא יוכלו לשמור תעודות זהות ורמו"ט המשיכה עם הקו הזה והוציא טיוטא (שנגנזה). כלומר, למה צריך מזהה ייחודי של תעודת זהות במקום שבו יש שירות שהוא לא קריטי?

האם שופרסל, רמי לוי, סלקום או הוט צריכים את תעודת הזהות שלנו כדי לספק לנו שירות? לא.

כלומר, המבחן הראשון ב-PBD הוא האם בכלל צריך את המידע הזה .הרבה פעמים מה שנראה לנו נחוץ וטריויאלי הוא בכלל לא כזה.

המבחן השני הוא איך מסדרים את הרשאות הגישה. האם המזכירה שלך צריכה גישה לכל המיילים שלך או רק ליומן שלך? האם העוזרת האלקטרונית שלך צריכה לדעת עם מי אתה נפגש, או רק מתי אתה

תפוס? האם אפליקציית הזמנת המוניות צריכה לתת לכל נהגי המונית לדעת מי אתה לפני שאתה מזמין מונית?

המבחן השלישי הוא האם ניתן להפוך מידע מזהה לכזה שהוא אנונימי. לדוגמא, אפליקציה מסוימת משמשת, לנסיעה בתחבורה ציבורית. היא צריכה לדעת, בסופו של דבר, כמה אנשים משתמשים בכל קו ובאיזה שעות. זה הגיוני לגמרי. אבל מה שהיא לא צריכה לדעת זה מי בדיוק השתמש, ואפילו לא באיזה עוד קווים הוא משתמש. ועדיין, זה לא מפריע לרב-קו לשמור את כל המידע הזה, סתם. כלומר בלי צורך.

המבחן הרביעי של PBD הוא מתי אפשר למחוק את המידע. גם כאשר שמרנו מידע, לא כל מידע צריך להיות שם לנצח. מידע על נסיעות היסטוריות בקווי תחבורה יכול להפוך למידע לא-מזהה ממש מהר, מידע מזהה על משתמשים שהפסיקו את השימוש בשירות אפשר להעיף בתוך שנתיים שלוש, וגם Waze לא צריכה לשמור את כל המסלולים המדויקים שנסעתם מהבית לעבודה בשבע השנים האחרונות, מספיק לה לדעת באיזה ימים נסעתם ובאיזה ימים לא. כלומר, המחיקה של המידע הוא המשך של ה-PBD בדרך אחרת.

לסיכום

אחרי שהבנו איך עושים PBD, צריך להבין שבלי PBD כל התקנות האלה הן צ'קליסט יפה והסכמי. לא מעט חברות פשוט קיבלו, בגלל ה-GDPR, עוד מסמכים מעוד עורכי דין. פתאום, במקום לעשות PBD, מה שעורכי הדין הנחו אותם זה להחתים את כל מי שמקבל מידע על הסכמים שהוא ישתמש במידע רק למטרות שה-GDPR מרשה. זה בדיוק הפוך מהמטרה של ה-GDPR. ה-GDPR לא נועד לייצר עוד ניירת, הוא נועד לייצר עוד פרטיות.