טל פרנקל, עו"ד
יורם ליכטנשטיין, עו"ד, CIPP/E

16 צעדים פרקטיים להתאמת העסק שלכם ל-GDPR

ה-General Data Protection Regulations היא חקיקה אירופית מרחיבה שעשוייה לחול גם על עסקים ישראלים רבים, וגם על העסק שלכם. בידי הרשויות האירופיות ובידי האנשים הפרטיים נמסרו כלי אכיפה בדמות קנסות גבוהים ביותר, תביעות משפטיות (לרבות נגד האחראים בעסק) ובכלל - חשיפה משמעותית לעסקים ולמנהליהם. במדריך זה נתמקד במספר צעדים חשובים שכדאי לנקוט בהם, כדי לשפר משמעותית את התאמת העסק שלכם לרגולצית הגנת המידע והפרטיות האירופית, ה-GDPR.
חשוב להבין שאין מדובר בפתרון קסם שמבטיח התאמה גורפת (לשם כך עליכם להעזר בעורכי דין מומחים ובמומחי אבטחה, שילכו עמכם יד ביד ויבצעו את ההתאמה ספציפית לעסק שלכם), אבל בהחלט מדובר בצעדים שישפרו משמעותית את יכולתכם להוכיח ציות לרגולציה.
חשוב גם לדעת - תהליך ההתאמה של עסק להוראות התקנות החדשות יהיה תהליך ארוך וצורך זמן. עכשיו הזמן לבחון את העסק, לבדוק את ההוראות החדשות ולתכנן את התהליך.
מדריך זה מספק מידע כללי בלבד. בשל מורכבות העניין הוא אינו משקף את מכלול האפשרויות והחריגים. בהחלט ייתכן שמדריך זה לא יתאים או לא יספיק למקרה שלכם. לכן, אין להסתמך על הכתוב כאן להתאמה בפועל של העסק שלכם לרגולציה. ככל שתבקשו לבצע התאמה ספציפית, יש להתייעץ ולהעזר בשירותיו של בעל מקצוע מומחה.

.1 הכרת ה-GDPR וזיהוי הבעיה

על שכבת ההנהלה הבכירה לבחון את השפעת החקיקה החדשה (בישראל ובאירופה) על העסק. זו אחריותם האישית של המנהלים והדירקטורים לוודא שהנושא נבחן ומטופל כראוי, ושככל שנדרשת עבודת התאמה – היא תחל מיידית.

.2 מיפוי המידע שנמצא בידיכם ודרכי עיבודו

תחילה יש לבצע "מיפוי מידע". בסקר כזה תמפו את מכלול המידע בעסק, את אופן איסוף המידע ואת השימוש בו בעסק ובעסקים קשורים. יש להרחיב ולאתר את כל רכיבי המידע האישי, ולתת משנה תוקף לאיתור מידע אישי רגיש (המחייב טיפול מיוחד).

.3 האם הרגולציה האירופית חלה עליכם

על בסיס תוצאות המיפוי יהיה צורך לקבל החלטות על תחולת ה-GDPR על העסק שלכם. בין היתר - האם המידע שבידיכם הוא מידע אישי? האם המידע האישי מתייחס לאנשים הנמצאים באירופה? האם המידע האישי מעובד באירופה (למשל בשרתי ענן)? האם מתקבלות באירופה החלטות ביחס לאיסוף המידע ולשימושים בו? ועוד

.4 מדיניות והודעות פרטיות ומידע

יש לעבור על ההודעות השונות הניתנות לפרטים במסגרת איסוף המידע. לוודא שהן "שקופות" מספיק כדרישת התקנות ומספקות את המידע המחוייב על פיהן. יש לבדוק למשל את ההודעה על איסוף המידע, את נוסח ההסכמה, את מדיניות הפרטיות, את ההודעה על הפעלת שירותי ניטור (כמו cookies ואמצעי ניטור אחרים) וכדומה.

.5 קביעת בסיס חוקי נכון לעיבוד

כל פעולת איסוף או עיבוד של מידע אישי חייבת להיות מבוססת על בסיס חוקי לגיטימי המצויין בתקנות. תצטרכו לשקול ולהחליט מהו הבסיס החוקי לאיסוף כל רכיב מידע ולתעד זאת.

.6 קבלת הסכמה לפי ה-GDPR

אם בחרתם בהסכמה כבסיס לאיסוף המידע, תצטרכו לבחון מחדש את תהליכי קבלת ההסכמה. חובה שההסכמה תהיה: מיודעת, כוללת פרטים נכונים, חופשית, לא מסומנת מראש, ללא התניה, חד משמעית, ברורה, הסכמה לכל אחד מהרכיבים הנאספים, בולטת, מדוייקת וניתנת לביטול. לכל אחד ממונחים אלו משמעות ייחודית שיש להקפיד עליה. יש לתעד את ההסכמות בצורה חד משמעית, ניתנת להוכחה ולאחזור.

7. ומה עם ילדים?

תצטרכו לבחון האם אתם אוספים מידע על או מ - ילדים. כשהמידע הנאסף ומעובד מתייחס לילדים, מוטלות על האוסף חובות מוגברות. ילדים שלא רשאים כלל לתת הסכמה בעצמם, אלא באמצעות אפוטרופוס, נחשבים כאלו בטווח הגילאים שמתחת לגיל 16 (או גיל אחר שייקבע בכל מדינה).

8. פעולות עיבוד ספציפיות

תצטרכו לבחון את מגוון פעילויות העיבוד שאתם מבצעים לגבי המידע. פעולות עיבוד מסויימות מחייבות התייחסות מפורטת. לדוגמא, פעולות של ניטור גולשים ברשת, "profiling" (קטלוג אנשים לפי מאפייני ייחוס) ועיבוד אוטומטי של החלטות ללא מגע יד אדם; כולן כוללות כללים ייחודיים שיש להקפיד עליהם.

9. זכויות הפרט לאור הרגולציה ועמידה בהן

לב תקנות הגנת המידע והפרטיות האירופיות הוא העברת השליטה במידע האישי מידי העסק האוסף לידי נשוא המידע. הוגדרו מספר לא מבוטל של זכויות פרט, המגלמות שליטה של אדם במידע האישי אודותיו. ביניהן נמצא גם את "הזכות להשכח" והזכות להורות על העברת המידע מספק אחד לספק אחר בצורה נאותה טכנולוגית. תצטרכו לבחון את הזכויות הללו ולוודא, כי העסק שלכם ערוך ומוכן למימושן.

10. הסדרת האופן בו מטופלות בקשות הקשורות בזכויות

מאחר והרגולציה קבעה לוח זמנים מחייב, ומחייבת את העסקים השונים לטפל בפניות באופן זריז ויעיל, תצטרכו להתכונן מראש ולהכין פתרונות לבקשות ודרישות שונות שיגיעו אליכם.

11. אבטחת מידע ופרטיות

עליכם לבדוק את מערך אבטחת המידע והפרטיות בעסק ואת התאמתו להוראות החדשות. ישנם מספר סוגי אבטחה נדרשים. ביניהם אבטחה, אבטחה ארגונית, אבטחה פיזית ואבטחה דיגיטלית ומקוונת. יש להקפיד על כולן.

12. פרצות אבטחת מידע

תצטרכו לבחון את נושא הטיפול של העסק בפרצות אבטחת מידע. הרגולציה מחייבת במקרים מסויימים הודעה לרשויות המפקחות או לפרטים נשואי המידע על פרצות אבטחה. חובת הדיווח תבחן לאור נסיבות כל מקרה ומקרה.
ה-GDPR אף מחייבת קביעת נהלים לאיתור וטיפול בפרצות אבטחת מידע וכן תיעוד שוטף של כל פרצות אבטחת המידע.

13. הגנת מידע משולבת בתכנון והערכת השפעת סיכונים על הפרטיות (DPIA)

ה GDPR קובעת כי יש לשקול שיקולי פרטיות והגנת מידע בלב ליבם של התהליכים הארגוניים והפיתוחיים, כבר משלב התכנון.
כמו כן, הרגולציה מחייבת ביצוע הערכות השפעות סיכוני אבטחה על הפרטיות הן מלכתחילה, והן בכל שלב בו נוצר מצב שעשוי לשנות את ההערכה.

14. הגנת מידע ופרטיות כברירת מחדל

כחלק משיקולי הפרטיות והגנת מידע בשלבי התכנון, תצטרכו לוודא שברירת המחדל של כל שירות או מוצר תהיה כי ההגדרות יהיו מכוונות להגנת הפרטיות. ככל שלקוח יבקש לשנות מצב זה, כמובן שיוכל לעשות כך לבחירתו.

15. קציני הגנת מידע (DPO)

תצטרכו לבחון האם מוטלת עליכם חובה למנות קצין הגנת מידע. זוהי פונקציה ניהולית חדשה שלעיתים נדרשת על פי ה-GDPR, וגם אם אינה מחוייבת – היא מומלצת, שכן מינוייה יעזור לארגון להוכיח ציות ופעולה כנדרש.
על הקצין להיות מנהל בכיר, כפוף לשדרה הניהולית הגבוהה ביותר בחברה, עצמאי, בעל השכלה ויכולת לפעול. על העסק לספק לו משאבים מספקים לבצע את תפקידו, לא להנחות אותו כיצד לפעול, לא להעמידו בניגוד עניינים ולאפשר לכל עובדי החברה, לקוחותיה, הרשות המפקחת ואנשים מהציבור גישה ישירה אליו.

16. העברות מידע בינלאומיות

הרגולציה באירופה הציבה מגבלות על הוצאת מידע אישי מחוץ לגבולות האיחוד. דרישת הבסיס הוא קיומה של "החלטת נאותות" ביחס למדינה או לתחום העיסוק, ובכל מקרה - יש לדאוג לאמצעי הגנה ואבטחה מספיקים ולציות מקבל המידע לרגולציה.
כיום, ישראל נהנית מהחלטת נאותות, אך קיים סיכון שהחלטה זו תתבטל עם כניסת הרגולציה לתוקף. מכיוון שהחלטה זו נבחנת מחדש כל כמה שנים, מומלץ לבדוק את קיומה במועד הרלוונטי אליכם.

נשמח אם תצרו עמנו קשר בכל נושא כדי שנוכל לעזור:

יורם ליכטנשטיין, עו"ד, CIPP/E טלפון: 03-6133333, דוא"ל: Yoram@y-law.co.il
טל פרנקל, עו"ד טלפון: 03-6243611, דוא"ל: Tal@fglaw.co.il