תיקון 13 לחוק הגנת הפרטיות
רשימת תיוג למפתחים

1. איסוף מידע (Data Collection)

[ ] נאסף **רק** המידע הדרוש לפעילות הפיצ'ר(Data Minimization)

[ ] הוגדרה **מטרה ברורה** לכל סוג מידע

[ ] אין איסוף מידע "ליתר ביטחון"

[ ] אין איסוף מידע רגיש ללא צורך עסקי מובהק

[ ] כל איסוף מידע תועד במסמךData Mapping

2. שקיפות למשתמש

[ ] כל איסוף מידע מופיע במדיניות הפרטיות

[ ] בקשות הרשאה (Location, Camera, Contacts) כוללות הסבר ברור

[ ] המשתמש יכול לראות איזה מידע נאסף עליו

[ ] קיימת אפשרות למחיקת חשבון ומידע

3. אבטחת מידע (Security by Design)

[ ] כל מידע רגיש מוצפן **במעבר** (TLS)

[ ] כל מידע רגיש מוצפן **במנוחה** (DB Encryption)

[ ] אין מפתחות API בקוד

[ ] שימוש ב-Environment Variables

[ ] הרשאות לפי Least Privilege

[ ] אין חשיפת מידע מיותר ב-API Responses

[ ] טיפול בשגיאות לא חושף מידע פנימי

[ ] לוגים לא מכילים מידע אישי רגיש

4. פיתוח API בהתאם לתיקון 13

[ ] API מחזיר רק את המידע הנדרש

[ ] קיימת אפשרות למחיקת מידע (DELETE /user/data)

[ ] קיימת אפשרות לעיון במידע (GET /user/data)

ליצירת קשר: 053-565-9056 או במייל info@qac.co.il

[ ] קיימת אפשרות לתיקון מידע (PUT /user/data)

[ ] קיימת תמיכה בהגבלת עיבוד (Data Restriction)

5. עבודה עם בסיס נתונים

[ ] מידע אישי מסומן בבירור בטבלאות

[ ] מידע רגיש מוצפן ברמת שדה (Field Level Encryption)

[ ] קיימים לוגים של גישה ל-DB

[ ] אין גישה ישירה ל- DBללא הרשאות

[ ] אין שאילתות שמחזירות מידע עודף

6. עבודה עם צד שלישי (Third Parties)

[ ] כל ספק עבר בדיקת פרטיות (Privacy Assessment)

[ ] יש הסכם עיבוד מידע (DPA)

[ ] המידע לא מועבר למדינות ללא הגנה מספקת

[ ] לא מועבר מידע רגיש ללא צורך

[ ] קיימת אפשרות למחוק מידע גם אצל הספק

7. תיעוד

[ ] תיעוד של כל סוגי המידע שנאספים

[ ] תיעוד של זרימת מידע במערכת

[ ] תיעוד של תהליכי מחיקה

[ ] תיעוד של תהליכי גיבוי ושחזור

[ ] תיעוד של הרשאות גישה