

נספח ב': שאלון להערכת סיכוני פרטיות (PIA) לאישור כלי דיגיטלי במוסדות חינוך

פרק 1: מאפייני המידע, האוכלוסייה והיקף העיבוד

מספר	נושא / שאלת בחינה	פירוט והנחיות למענה	מענה ספק/גורם מקצועי
1.1	פרטי המידע	אילו פריטי מידע נאספים? האם נאסף מידע בעל רגישות מיוחדת (מידע רפואי, נפשי, ציונים, התנהגות, מידע ביומטרי, דעות פוליטיות וכד')? יש לכתוב באופן מפורט ברמת שדות המידע (כגון: שם, כתובת, שם ביה"ס, גיל וכיוצ"ב).	
1.2	סוגי נשואי המידע	על מי המידע מעובד? האם מדובר באוכלוסייה רגישה (קטינים, תלמידי חינוך מיוחד, אנשי צוות)?	
1.3	מקורות איסוף המידע	מהו מקור המידע? (ישירות מהתלמיד/הורה, הזנה ידנית ע"י המורה, או משיכה אוטומטית ממערכת אחרת)?	
1.4	ממשקים למערכות ארגוניות	האם נדרש ממשק למערכות משרד החינוך? אם כן, אילו נתונים נמשכים (יש לפרט ברמת שדות, לאיזו מטרה? והאם יש אישור טכנולוגי לממשק)?	
1.5	כמות נשאי המידע	מהו היקף המשתמשים הפוטנציאלי? (נתון קריטי לקביעת רמת האבטחה בתקנות).	

מספר	נושא / שאלת בחינה	פירוט והנחיות למענה	מענה ספק/גורם מקצועי
1.6	משך שמירת המידע	לכמה זמן נשמר המידע בכלי? מהו נוהל מחיקת המידע בתום פעילות/ שנת הלימודים/אחר?	
1.7	העברת מידע לחו"ל	האם המידע מעובד בשרתי ענן מחוץ לגבולות ישראל? באילו מדינות?	
1.8	ספקים חיצוניים DPA-1	האם הכלי משתמש בספקי משנה (למשל, שירותי ענן של AWS/Google, כלי אנליטיקה)? האם קיים הסכם עיבוד נתונים (DPA)?	
1.9	הרשאות גישה	למי יש גישה למידע בתוך ביה"ס (מנהל, מחנך, מורה מקצועי, יועצת) ומחוץ לו (תמיכה טכנית של הספק)? כמה מורשי גישה צפויים להיות?	
1.10	מזעור מידע (Data Minimization)	האם ניתן להפעיל את הכלי באמצעות שימוש טכניקות מגבירות פרטיות (כגון: פסאודונימיזציה/ השמטה של שדות מזהים[מ.ס/ שם מלא וכיוצ"ב])?	

פרק 2: מטרות האיסוף והשימושים במידע

מספר	נושא / שאלת בחינה	פירוט והנחיות למענה	מענה ספק/גורם מקצועי
2.1	הגדרת מטרות איסוף המידע	מהם המטרות והשימושים שבגינם נאסף המידע. יש לכתוב באופן ברור ומפורש (למשל: מטרה כגון: "ניהול שוטף של פעילות בית הספר" היא כללית מידי) מהו התוצר המבוקש מהשימוש בכלי?	
2.2	השפעה על נושא המידע	כיצד השימוש בכלי משפיע על התלמיד? האם מופק ממנו ציון, אבחון, קביעת הקבצה, או מניעת הטבה כלשהי?	
2.3	מחלוקת או עניין ציבורי	האם השימוש בכלי או איסוף המידע מעלים סוגיות רגישות מבחינה ציבורית או אתית (למשל: זיהוי פנים, מעקב אחר מיקום, ניתוח רגשות)?	
2.4	שימוש בטכנולוגיות חדשות (AI)	האם הכלי מבוסס על בינה מלאכותית? אם כן, האם המידע של התלמידים משמש לאימון מודל ה-AI של החברה? האם מתבצע פרופילינג (Profiling)?	

פרק 3: בסיס חוקי וזכויות נושאי המידע

מספר	נושא / שאלת בחינה	פירוט והנחיות למענה	מענה ספק/גורם מקצועי
3.1	בסיס חוקי לעיבוד	מכוח מה מעובד המידע? (הסמכה חוקית/הסכמה)?	
3.2	מימוש זכות העיון והתיקון	האם לנושא המידע קיימת שליטה על המידע וגישה אליו באמצעות הכלי לצורך צפייה/ שינוי/ מחיקה? ככל שלא כיצד ניתן יהיה לתמוך בזכותם של נושאי המידע לעיין במידע על אודותיהם ולבקש לתקנו אם המידע אינו נכון, שלם, ברור ומעודכן?	
3.3	רגולציה מגזרית נוספת	האם חלה חקיקה או רגולציה מגזרית נוספת בעניין הגנת מידע, פרטיות או סודיות (בנוסף לחוק הגנת הפרטיות והתקנות שהותקנו מכוחו) בקשר עם השימושים שהוגדרו?	
3.4	ניהול הסכמות הורים	במידה ונדרשת הסכמת הורים ספציפית (לקטינים), כיצד ביה"ס אוסף ומנהל את ההסכמות הללו? האם המערכת מאפשרת להחריג תלמיד שהוריו סירבו?	
3.5	ניידות המידע (Portability)	האם בתום העבודה עם הכלי, בית הספר יכול לייצא את כל המידע שנאסף בצורה מרוכזת וסטנדרטית (למשל קובץ Excel/CSV)?	

פרק 4: אבטחת מידע וניהול סיכונים

מספר	נושא / שאלת בחינה	פירוט והנחיות למענה	מענה ספק/גורם מקצועי
4.1	עמידה בתקן אבטחת מידע של מוסדות חינוך	האם הכלי עומד בתקן אבטחת מידע של מוסדות חינוך?	
4.2	ניסיון קודם ואירועי עבר	האם ידוע על פרצות אבטחה, אירועי סייבר או דליפות מידע בעבר הקשורים לכלי זה או לטכנולוגיה זו?	
4.3	תוצרי ניהול סיכונים	האם נבחנו תרחישי קיצון ופגיעות בנושאי המידע כתוצאה מהעיבוד? (כגון: אפליה אלגוריתמית, גניבת זהות של קטינים, חשיפת מידע רגיש להורים אחרים, זיהוי מחדש של מידע אנונימי).	