



TAKIN // תקין

מערך בדיקת תאימות לחוקים ותקנות, איתור ליקויים וייעול האתר

דוח ביקורת תאימות וייעול – לשימוש הנהלת האתר

Takin // ביקורת תאימות לחוקים, תקנות ואיכות דיגיטלית

דוח ביקורת תאימות מקיף לחוקים ותקנות וצמצום חשיפה לתביעות

איתור מקיף של ליקויים לפי דיני הנגישות (תקן 5568), הגנת הפרטיות (תיקון 13), הגנת הצרכן וחוק הספאם – לצד המלצות לשיפור וייעול האתר.

תאריך סריקה: 17.9.2026

כתובת האתר הנבדק: <https://demostore.co.il>

הופעל פרוטוקול בדיקה מחמיר לזיהוי עילות תביעה פוטנציאליות (ציון מקסימלי 55)

בסריקת האתר אותרה לפחות עבירה סטטוטורית אחת ברמת חומרה קריטית (כגון דליפת מספרי תעודת זהות גולמיים או אי-עמידה בחובת יידוע לפי תיקון 13). על פי מודל הסיכונים הסטטוטורי, האתר חשוף להליכי אכיפה מנהליים ודרישות פיצויים ללא הוכחת נזק.



ציון מחמיר (STRICT)

100 / 55

10 חשיפות פעילות

ציון בסיס רגולטורי

100 / 55

3 ליקויים גלויים

חשיפה סטטוטורית

175,000 ₪

ללא הוכחת נזק

שער בטיחות התיקון

Turnkey

קוד מאושר לבדיקה

דוח ביקורת עומק מחמיר (סטנדרט תובעים)

100 / 55

אותרו 10 חשיפות וליקויי קוד מעמיקים

דוח תאימות רגיל (עמידה בסיסית בחוק)

100 / 55

אותרו 3 ליקויים גלויים ברף הבסיס

סטטוס חשיפה כולל: לקוי קריטי (חשיפה משפטית פעילה ועילות תביעה ישירות). בדיקת העומק איתרה סך של 10 חשיפות פעילות (מתוכן 3 ליקויים גלויים בדוח הרגיל ו-7 חשיפות עומק טכנולוגיות ייחודיות לדוח זה).

הערכת חשיפה כספית מקסימלית: 175,000 ₪

ממצאי בדיקות היסוד (מתוך הדוח הרגיל)

בדיקת יסוד בסיסית	חקיקה ישראלית רלוונטית	דרישת החוק הסטטוטורית	ממצא בדוח הרגיל
חוק הספאם (טפסים)	סעיף 30א לחוק התקשורת	איסור תיבות סימון שיווקיות מסומנות מראש	✓ עומד ברף הבסיסי
הגנת הצרכן (ביטול עסקה)	סעיף 14ג לחוק הגנת הצרכן	קישור ייעודי ונפרד לביטול עסקה בדף הראשי	✗ חסר קישור ביטול עסקה
הצהרת נגישות בסיסית	תקנה 35 לתקנות שוויון זכויות	פרסום הצהרת נגישות מקושרת מכל עמוד	✓ הצהרת נגישות אותרה

בדיקת יסוד בסיסית	חקיקה ישראלית רלוונטית	דרישת החוק הסטטוטורית	מצא בדוח הרגיל
אבטחת תעבורה (HTTPS)	תקנות הגנת הפרטיות (אבטחת מידע)	הצפנת תעבורה בסיסית בפרוטוקול SSL/TLS	✓ תעבורה מוצפנת ב-HTTPS

התפלגות ציונים לפי 5 אדני הרגולציה בישראל

עמוד רגולטורי	ציון (0-100)	סטנדרט החוק הנבדק	סטטוס סיכון
הגנת הפרטיות (תיקון 13)	0/100	סעיף 11 לחוק הגנת הפרטיות (חובת יידוע וגילוי טראקרים)	סיכון גבוה (הפרה פעילה)
נגישות דיגיטלית (ת"י 5568)	70/100	תקנות שוויון זכויות לאנשים עם מוגבלות (רמת AA)	סיכון גבוה (הפרה פעילה)
חוק הספאם (סעיף 30א)	100/100	סעיף 30א לחוק התקשורת (איסור תיבות מסומנות מראש)	תקין כחוק ✓
הגנת הצרכן (סעיף 14ג)	70/100	חובת קישור ביטול עסקה נפרד ונגיש בדף הראשי	סיכון גבוה (הפרה פעילה)
הגנת פרטיות ופרטי זיהוי (PII)	85/100	הגנה על מספרי תעודת זהות ואשראי (תקנות מאגרי מידע)	טעון שיפור (ליקוי פעיל)

מעקבי צד-שלישי פעילים שאותרו בתעבורת הרשת 🔍

סעיף 11 לחוק הגנת הפרטיות (תיקון 13) מחייב גילוי מדויק של כל גורם חיצוני המקבל מידע מהאתר. אי-התאמה בין המעקבים הפועלים בפועל לבין הפירוט במדיניות מהווה עילה לסנקציות מנהליות ותביעות.

ספק מעקב	קטגוריה	דומיין מפעיל	סטטוס במדיניות
Google Analytics 4	ANALYTICS	https://googletagmanager.com/gtag/js	מפורט כחוק
Meta Pixel (Facebook)	ADVERTISING	https://connect.facebook.net/en_US/fbevents.j	לא גלוי במדיניות
TikTok Pixel	ADVERTISING	https://analytics.tiktok.com/i18n/pixel/event	לא גלוי במדיניות
Microsoft Clarity	SESSION_RECORDING	https://www.clarity.ms/tag/demo	לא גלוי במדיניות

ממצאי חשיפה בפרטיות (תיקון 13)

חומרה גבוהה

נכלל גם בדוח הרגיל ✓

סעיפים 13 ו-14 לחוק הגנת הפרטיות, התשמ"א-1981 (תיקון 13)

שלב 1 מה הבעיה והסיכון המשפטי?

היעדר מנגנון מפורש למימוש זכות עיון ומחיקת מידע (תיקון 13)

במדיניות הפרטיות חסרה כתובת דוא"ל ייעודית ונוהל ברור המאפשר לגולשים לפנות ולדרוש את מחיקת המידע שנאסף עליהם.

⚠ חשיפה כספית סטטוטורית: עד 120,000 ₪ לפי סעיף 31ב(א)(2)

לשון החוק: "סעיפים 13 ו-14 לחוק הגנת הפרטיות: 13. (א) כל אדם זכאי לעיין, בעצמו או על ידי בא-כוחו... במידע שעליו המוחזק במאגר מידע... 14. (א) אדם שעיין במידע שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות אל בעל מאגר המידע בבקשה לתקן את המידע או למוחקו."

שלב 2 ההוכחה הדיגיטלית (מתוך האתר שלך)

אותרה עדות ברמת פרוטוקול רשת ומדיניות האתר.

שלב 3 הנחיית יישום מילולית זהירה (תכנון בלבד)

⚠ ציון בטיחות פתרון: 75/100 – זהירות: נדרשת התאמה מילולית ובדיקת Staging

הנחיה כללית: יש להוסיף סעיף מפורש המציין כתובת דוא"ל ישירה לפנייה לצורך עיון ומחיקת מידע אישי ממאגרי העסק.

💡 הצעה מילולית תמציתית לפתרון (ללא קוד ביצוע אוטומטי):

הנחיה עקרונית: יש להוסיף סעיף מפורש המציין כתובת דוא"ל ישירה לפנייה לצורך עיון ומחיקת מידע אישי ממאגרי העסק.. יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור.

⚠ **מדיניות בטיחות תקין:** בשל תלות ברכיבי שרת או לוגיקת טפסים, לא מסופק פרומפט ביצוע אוטומטי. יש ליישם את ההנחיה המילולית באופן מבוקר בסביבת בדיקות (Staging).

חומרה קריטית

חשיפת עומק (מחמיר בלבד)

סעיף 11 לחוק הגנת הפרטיות (תיקון 13)

מה הבעיה והסיכון המשפטי? שלב 1

שיגור מעקבי רשת ופרסום ללא הסכמה מוקדמת (עקיפת באנר קוקיז)

אותרו 3 מעקבי פרסום וריגול צד-שלישי (Meta Pixel (Facebook), TikTok Pixel, Microsoft Clarity) ששיגרו נתונים עוד בטרם ניתנה הסכמת הגולש (הפרת חובת יידוע מוקדמת לפי תיקון 13 לחוק הגנת הפרטיות).

⚠ **חשיפה כספית סטטוטורית: עד 5% ממחזור העסקאות השנתי לפי סעיף 31ב(ב); עיצום מנהלי כספי חמור**

לשון החוק: "סעיף 11 לחוק הגנת הפרטיות (תיקון 13): איסור שיגור נתוני מעקב ופרסום לצדדים שלישיים בטרם הוצגה גולש הודעה מפורשת וניתנה הסכמתו."

ההוכחה הדיגיטלית (מתוך האתר שלך) שלב 2

ראיה דיגיטלית בקוד ה-DOM:

Meta Pixel (Facebook) (ADVERTISING), TikTok Pixel (ADVERTISING), Microsoft Clarity (SESSION_RECORDING)

הנחיית יישום מילולית זהירה (תכנון בלבד) שלב 3

⚠ **ציון בטיחות פתרון: 75/100 – זהירות: נדרשת התאמה מילולית ובדיקת Staging**

הנחיה כללית: יש להגדיר את מערכת ניהול התגיות (GTM) כך שפיקסלים של צדדים שלישיים ייטענו אך ורק לאחר לחיצה פעילה על כפתור האישור בבאנר.

💡 **הצעה מילולית תמציתית לפתרון (ללא קוד ביצוע אוטומטי):**

הנחיה עקרונית: יש להגדיר את מערכת ניהול התגיות (GTM) כך שפיקסלים של צדדים שלישיים ייטענו אך ורק לאחר לחיצה פעילה על כפתור האישור בבאנר.. יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור.

⚠ **מדיניות בטיחות תקין:** בשל תלות ברכיבי שרת או לוגיקת טפסים, לא מסופק פרומפט ביצוע אוטומטי. יש ליישם את ההנחיה המילולית באופן מבוקר בסביבת בדיקות (Staging).

חומרה קריטית

חשיפת עומק (מחמיר בלבד)

תיקון 13 לחוק הגנת הפרטיות (חובת יידוע ושקיפות)

מה הבעיה והסיכון המשפטי? שלב 1

מעקב לא מוצהר: Meta Pixel (Facebook)

פיקסל Meta פועל ברשת האתר ומבצע איסוף מידע עקיף ופילוח שיווקי, ללא גילוי נאות במדיניות הפרטיות בניגוד לתיקון 13.

⚠ חשיפה כספית סטטוטורית: עד 150,000 ₪ לפי סעיף 31ב(א)(1)

לשון החוק: "סעיף 11(ב) לחוק הגנת הפרטיות (תיקון 13): "נאסף מידע אודות אדם שלא מנושא המידע במישרין (לרבות באמצעות עוגיות, פיקסלים של מעקב ורשתות שיווק דיגיטלי), חלה על בעל המאגר החובה להביא לידיעת נושא המידע את ההודעה לפי סעיף קטן (א) בהזדמנות הראשונה."

ההוכחה הדיגיטלית (מתוך האתר שלך) שלב 2

ראה דיגיטלית בקוד ה-DOM:

Meta Pixel (Facebook)

שלב 3 הפתרון האוטומטי חסום – סיכון ארכיטקטוני גבוה

● ציון בטיחות פתרון: 65/100 – סיכון ארכיטקטוני גבוה – הפתרון האוטומטי חסום

● מדיניות הגנה על מערכות האתר:

מדיניות בטיחות תקין: תיקון זה כרוך בסיכון ארכיטקטוני גבוה ונוגע בלוגיקת שרת רגישה / טפסים פעילים / מסדי נתונים. כדי למנוע שיבוש של פעילות האתר, מערכות הסליקה או נתוני משתמשים - המערכת אינה מנפקת קוד או פרומפט אוטומטי. חובה להעביר את פרטי הליקוי למפתח האתר לבדיקה ותיקון מותאם אישית בסביבת פיתוח.

🔒 **חובת התערבות מפתח:** תיקון ליקוי זה מחייב בדיקה ידנית של מתכנת בסביבת פיתוח מבודדת כדי למנוע שיבוש של פעילות האתר או מסדי הנתונים.

חומרה קריטית

חשיפת עומק (מחמיר בלבד)

תיקון 13 לחוק הגנת הפרטיות (חובת יידוע ושקיפות)

מה הבעיה והסיכון המשפטי? שלב 1

מעקב לא מוצהר: TikTok Pixel

פיקסל TikTok מופעל ברשת האתר ללא אזכור במדיניות הפרטיות כנדרש בסעיף 11(ב) לחוק הגנת הפרטיות.

⚠ חשיפה כספית סטטוטורית: עד 150,000 ₪ לפי סעיף 31ב(א)(1)

לשון החוק: "סעיף 11(ב) לחוק הגנת הפרטיות (תיקון 13): "נאסף מידע אודות אדם שלא מנושא המידע במישרין (לרבות באמצעות עוגיות, פיקסלים של מעקב ורשתות שיווק דיגיטלי), חלה על בעל המאגר החובה להביא לידיעת נושא המידע את ההודעה לפי סעיף קטן (א) בהזדמנות הראשונה."

ההוכחה הדיגיטלית (מתוך האתר שלך) שלב 2

ראה דיגיטלית בקוד ה-DOM:

TikTok Pixel

שלב 3 הפתרון האוטומטי חסום – סיכון ארכיטקטוני גבוה

● ציון בטיחות פתרון: 65/100 – סיכון ארכיטקטוני גבוה – הפתרון האוטומטי חסום

מדיניות הגנה על מערכות האתר: ●

מדיניות בטיחות תקין: תיקון זה כרוך בסיכון ארכיטקטוני גבוה ונוגע בלוגיקת שרת רגישה / טפסים פעילים / מסדי נתונים. כדי למנוע שיבוש של פעילות האתר, מערכות הסליקה או נתוני משתמשים - המערכת אינה מנפקת קוד או פרומפט אוטומטי. חובה להעביר את פרטי הליקוי למפתח האתר לבדיקה ותיקון מותאם אישית בסביבת פיתוח.

🔒 **חובת התערבות מפתח:** תיקון ליקוי זה מחייב בדיקה ידנית של מתכנת בסביבת פיתוח מבודדת כדי למנוע שיבוש של פעילות האתר או מסדי הנתונים.

חומרה גבוהה

חשיפת עומק (מחמיר בלבד)

תיקון 13 לחוק הגנת הפרטיות (חובת יידוע ושקיפות)

מה הבעיה והסיכון המשפטי? שלב 1

מעקב לא מוצהר: Microsoft Clarity

כלי הקלטת מסך והתנהגות גלישה (Session Recording) פועל ללא יידוע מפורש במדיניות.

⚠ חשיפה כספית סטטוטורית: עד 150,000 ₪ לפי סעיף 31ב(א)(1)

לשון החוק: "סעיף 11(ב) לחוק הגנת הפרטיות (תיקון 13): "נאסף מידע אודות אדם שלא מנושא המידע במישרין (לרבות באמצעות עוגיות, פיקסלים של מעקב ורשתות שיווק דיגיטלי), חלה על בעל המאגר החובה להביא לידיעת נושא המידע את ההודעה לפי סעיף קטן (א) בהזדמנות הראשונה."

ההוכחה הדיגיטלית (מתוך האתר שלך) שלב 2

ראה דיגיטלית בקוד ה-DOM:

Microsoft Clarity

שלב 3 הפתרון האוטומטי חסום – סיכון ארכיטקטוני גבוה

● ציון בטיחות פתרון: 65/100 – סיכון ארכיטקטוני גבוה – הפתרון האוטומטי חסום

● מדיניות הגנה על מערכות האתר:

מדיניות בטיחות תקין: תיקון זה כרוך בסיכון ארכיטקטוני גבוה ונוגע בלוגיקת שרת רגישה / טפסים פעילים / מסדי נתונים. כדי למנוע שיבוש של פעילות האתר, מערכות הסליקה או נתוני משתמשים - המערכת אינה מנפקת קוד או פרומפט אוטומטי. חובה להעביר את פרטי הליקוי למפתח האתר לבדיקה ותיקון מותאם אישית בסביבת פיתוח.

🔒 **חובת התערבות מפתח:** תיקון ליקוי זה מחייב בדיקה ידנית של מתכנת בסביבת פיתוח מבודדת כדי למנוע שיבוש של פעילות האתר או מסדי הנתונים.

סריקת קוד מקור ו-DOM

פרק ב': ביקורת הגנת פרטיות ופרטי זיהוי (PII AUDIT)

איתור חשיפת מספרי תעודת זהות וכרטיסי אשראי 🔍

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, מחייבות כל עסק המנהל מאגר מידע ליישם הצפנה ומיסוך מלא של נתוני זיהוי. חשיפה של מספר תעודת זהות תקין בקוד ה-HTML או בבקשות רשת מהווה הפרה חמורה של הדין.

סוג מידע אישי מוגן	בדיקה מתמטית	ממצאים באתר הנבדק	סטטוס סיכון
מספרי תעודת זהות ישראלים	אימות ספרת ביקורת Modulo 10 מלא	לא אותרו ת"ז חשופות	תקין
כרטיסי אשראי	אימות אלגוריתם Luhn	לא אותרו כרטיסי אשראי	תקין

ראיות דיגיטליות לדליפת מידע

✓ לא אותרו ליקויים פתוחים בפרק זה.

ליקויי קוד נגישות ברמת ה-DOM (Axe-Core / WCAG 2.1 AA)

סריקת עץ ה-DOM לאיתור אלמנטים שאינם עומדים בדרישות הניגודיות (Contrast), חסרי תוויות ARIA או תגיות חלופיות לתמונות:

חומרה קריטית

חשיפת עומק (מחמיר בלבד)

תקן ישראלי ת"י 5568 / WCAG 2.1 AA

שלב 1 מה הבעיה והסיכון המשפטי?

ליקוי נגישות בקוד האתר (color-contrast)

ניגודיות צבעים לקויה בכפתורי רכישה (3.1:1 לעומת מינימום 4.5:1)

חשיפה כספית סטטוטורית: פיצוי ללא הוכחת נזק עד 50,000 ₪ לפי סעיף 19ד לחוק שוויון זכויות לאנשים עם מוגבלות

לשון החוק: "סעיף 19ד לחוק שוויון זכויות לאנשים עם מוגבלות: בית המשפט רשאי לחייב בתשלום פיצויים בסכום שלא יעלה על 50,000 ₪ בלא הוכחת נזק בשל הפרת הוראות הנגישות."

שלב 2 ההוכחה הדיגיטלית (מתוך האתר שלך)

ראיה דיגיטלית בקוד ה-DOM:

```
<button class="btn-add-to-cart">הוסף לסל הקניות</button>
```

שלב 3 הנחיית יישום מילולית זהירה (תכנון בלבד)

ציון בטיחות פתרון: 78/100 – זהירות: נדרשת התאמה מילולית ובדיקת Staging

הנחיה כללית: בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C: <https://dequeuniversity.com/rules/axe/4.4/color-contrast>

שלב 4 הצעה מילולית תמציתית לפתרון (ללא קוד ביצוע אוטומטי):

יש לבצע בדיקת ניגודיות צבעים (יחס 4.5:1 לפחות) ולהכחות את גוון הטקסט או להבהיר את הרקע בהגדרות ה-CSS, מבלי לפגוע בפלטת שפת המותג.

מדיניות בטיחות תקין: בשל תלות ברכיבי שרת או לוגיקת טפסים, לא מסופק פרומפט ביצוע אוטומטי. יש ליישם את ההנחיה המילולית באופן מבוקר בסביבת בדיקות (Staging).

חומרה גבוהה

חשיפת עומק (מחמיר בלבד)

תקן ישראלי ת"י 5568 / WCAG 2.1 AA

מה הבעיה והסיכון המשפטי? שלב 1

ליקוי נגישות בקוד האתר (image-alt)

תמונות מוצרים ללא תגית טקסט חלופי (Alt Text) לקוראי מסך

חשיפה כספית סטטוטורית: פיצוי ללא הוכחת נזק עד 50,000 ₪ לפי סעיף 19 לחוק שוויון זכויות לאנשים עם מוגבלות ⚠️

לשון החוק: "סעיף 19 לחוק שוויון זכויות לאנשים עם מוגבלות: בית המשפט רשאי לחייב בתשלום פיצויים בסכום שלא יעלה על 50,000 ₪ בלא הוכחת נזק בשל הפרת הוראות הנגישות."

ההוכחה הדיגיטלית (מתוך האתר שלך) שלב 2

ראיה דיגיטלית בקוד ה-DOM:

```

```

הפתרון המעשי המוכן להטמעה שלב 3

ציון בטיחות פתרון: 94/100 – בטוח ליישום מיידי

הנחיה טכנית לתיקון: בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C
<https://dequeuniversity.com/rules/axe/4.4/image-alt>

● חומרה בינונית

🔗 חשיפת עומק (מחמיר בלבד)

תקן ישראלי ת"י 5568 / WCAG 2.1 AA

● שלב 1 מה הבעיה והסיכון המשפטי?

ליקוי נגישות בקוד האתר (focus-visible)

ביטול מסגרת פוקוס מקלדת באמצעות outline:none ללא חלופה

חשיפה כספית סטטוטורית: פיצוי ללא הוכחת נזק עד 50,000 ₪ לפי סעיף 19 יד לחוק שוויון זכויות לאנשים עם מוגבלות ⚠️

לשון החוק: "סעיף 19 יד לחוק שוויון זכויות לאנשים עם מוגבלות: בית המשפט רשאי לחייב בתשלום פיצויים בסכום שלא יעלה על 50,000 ₪ בלא הוכחת נזק בשל הפרת הוראות הנגישות."

🔍 שלב 2 ההוכחה הדיגיטלית (מתוך האתר שלך)

ראיה דיגיטלית בקוד ה-DOM:

```
<a href="/catalog" style="outline: none;">קטלוג מוצרים</a>
```

● שלב 3 הנחיית יישום מילולית זהירה (תכנון בלבד)

⚠️ **ציון בטיחות פתרון: 75/100 – זהירות:** נדרשת התאמה מילולית ובדיקת Staging

הנחיה כללית: בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C: <https://dequeuniversity.com/rules/axe/4.4/focus-visible>

💡 **הצעה מילולית תמציתית לפתרון (ללא קוד ביצוע אוטומטי):**

הנחיה עקרונית: בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C: <https://dequeuniversity.com/rules/axe/4.4/focus-visible>. יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור.

⚠️ **מדיניות בטיחות תקין:** בשל תלות ברכיבי שרת או לוגיקת טפסים, לא מסופק פרומפט ביצוע אוטומטי. יש ליישם את ההנחיה המילולית באופן מבוקר בסביבת בדיקות (Staging).

VISUAL & MODAL AUDIT

פרק ד': ביקורת שפת עיצוב, מיתוג ואחידות חלונות קופצים

ניתוח עקביות ויזואלית ושפת עיצוב המותג

בדיקה זו בוחנת האם האתר פועל עם שפת עיצוב אחידה ויוקרתית, או שמא שילוב של תוספים, ווידג'טים ופופאפים חיצוניים שוברים את ארון הלקוחות ויוצרים רושם מפוצל.

תקין ✓

התאמת מובייל

1

פופאפים / ווידג'טים

2

גופנים שזוהו

82/100

ציון אחידות עיצוב

ממצאי ביקורת העיצוב והפופאפים:

- עיצוב עקבי בשפת המותג העיקרית.
- הפופאפ שומר על גופן המותג אך מומלץ להוסיף כפתור סגירה נגיש.

ליקויי צרכנות, ספאם ואיכות דיגיטלית נוספים

חומרה קריטית ●

נכלל גם בדוח הרגיל ✓

סעיף 1ג14 לחוק הגנת הצרכן

מה הבעיה והסיכון המשפטי? שלב 1 ●

היעדר קישור ייעודי לביטול עסקה באתר מכר מרחוק

אתר המבצע מכר מרחוק מחויב להציג קישור ייעודי ונפרד ששמו ביטול עסקה.

חשיפה כספית סטטוטורית: עד 10,000 ₪ פיצוי לדוגמה ללא הוכחת נזק לפי סעיף 31א; עיצום כספי מינהלי של הרשות להגנת הצרכן עד כ-46,000 ₪ ⚠

לשון החוק: "סעיף 1ג14(ג) לחוק הגנת הצרכן: "עוסק שהתקשרות עמו נעשתה באמצעות אתר אינטרנט, יציג באתר: (1) קישור ייעודי ונפרד ששמו 'ביטול עסקה'; (2) הקישור יוצג באופן בולט וברור בדף הבית של האתר וכן בתחתית כל דף באתר (Footer); (3) לחיצה על הקישור תוביל אל טופס מקוון ייעודי לביטול עסקה..."

ההוכחה הדיגיטלית (מתוך האתר שלך) שלב 2 🔍

אותרה עדות ברמת פרוטוקול רשת ומדיניות האתר.

הפתרון המעשי המוכן להטמעה שלב 3 ●

ציון בטיחות פתרון: 90/100 – בטוח ליישום מיידי 🛡

הנחיה טכנית לתיקון: הוסף קישור בשם ביטול עסקה בפוסטר ובעמוד הבית.

חומרה גבוהה

נכלל גם בדוח הרגיל ✓

הנחיות מערך הסייבר הלאומי

שלב 1 מה הבעיה והסיכון המשפטי?

היעדר כותרת אבטחה (HSTS) Strict-Transport-Security

האתר אינו אוכף תקשורת מוצפנת קשיחה.

חשיפה כספית סטטוטורית: הפרת חובת אבטחת מידע לפי סעיף 17 לחוק הגנת הפרטיות - חשיפה לסנקציות מנהליות ⚠️

לשון החוק: "סעיף 17 לחוק הגנת הפרטיות: בעל מאגר מידע אחראי לאבטחת המידע שבמאגר. שידור נתונים ללא הצפנה מלאה חושף את המידע לציטוט וירוס."

שלב 2 ההוכחה הדיגיטלית (מתוך האתר שלך)

אותרה עדות ברמת פרוטוקול רשת ומדיניות האתר.

שלב 3 הנחיית יישום מילולית זהירה (תכנון בלבד)

⚠️ ציון בטיחות פתרון: 75/100 – זהירות: נדרשת התאמה מילולית ובדיקת Staging

הנחיה כללית: הגדר בשרת כותרת HSTS: Strict-Transport-Security: max-age=31536000.

💡 **הצעה מילולית תמציתית לפתרון (ללא קוד ביצוע אוטומטי):**

הנחיה עקרונית: הגדר בשרת כותרת HSTS: Strict-Transport-Security: max-age=31536000.. יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור.

⚠️ **מדיניות בטיחות תקין:** בשל תלות ברכיבי שרת או לוגיקת טפסים, לא מסופק פרומפט ביצוע אוטומטי. יש ליישם את ההנחיה המילולית באופן מבוקר בסביבת בדיקות (Staging).

נחתם דיגיטלית // תקין (TAKIN)

פרוטוקול ביקורת תאימות מס' TK-2026 // גרסה 3.8 Strict
דוח זה נחתם טכנולוגית ומכיל ממצאים מבוססי קוד DOM ופרוטוקול רשת.



🚧 **הבהרה משפטית (סעיף 20 לחוק לשכת עורכי הדין, התשכ"א-1961):** דוח ביקורת עומק זה מופק באמצעות מערכת טכנולוגית אוטונומית ונועד להערכת סיכונים טכנולוגית בלבד. אין באמור משום ייעוץ משפטי, חוות דעת משפטית מחייבת או תחליף לייעוץ משפטי פרטני.

ספר הפרומפטים לתיקון מלא (The AI Master)

(Playbook)

סה"כ משימות ממוספרות:

10

הנחיות שימוש להפעלה בלחיצה אחת:

- לחץ על כפתור "העתק את כל הפרומפט" בראש התיבה (או סמן והעתק ידנית).
- פתח את ה-IDE שלך (Cursor / Claude 3.7 / GitHub Copilot / ChatGPT 4o).
- הדבק את הפרומפט בחלון ה-Chat והפעל את סוכן התיקון האוטומטי.
- המערכת תבצע תיקון כירורגי נקודתי (Minimal Diff) של כל הליקויים ללא פגיעה בעיצוב.

העתק את כל הפרומפט

10 משימות מובנות

פרומפט מאסטר מרוכז (Master Remediation Prompt)

```
# Takin AI Master Remediation Playbook (ספר הפרומפטים לתיקון האתר)
אתר היעד: https://demostore.co.il
סך משימות לביצוע: 10 משימות מדורגות לפי רמת סיכון משפטי.

## הנחיה ל-AI Assistant (Cursor / Claude / GitHub Copilot / ChatGPT):
אתה פועל כארכיטקט תוכנה בכיר ומומחה רגולציה דיגיטלית ישראלית (תקן נגישות 5568, תיקון 13 לפרטיות, חוק הגנת הצרכן וחוק הספאם).
בצע את רשימת המשימות הבאה בצורה כירורגית (Minimal Diff), ללא פגיעה בעיצוב הקיים, וללא ביצוע Refactoring בלתי נדרש.

---

### משימה 1: [קריטי] היעדר קישור ייעודי לביטול עסקה באתר מכר מרחוק (CON-14C1-LINK-001)
- **מיקום:** פوتر האתר (Footer) ודף ייעודי לביטול עסקה
- **הנחיית ביצוע:** הוסף קישור בשם ביטול עסקה בפوتر ובעמוד הבית.
- **קוד/נוסח מומלץ:**
  <a href="/cancellation" rel="nofollow" class="footer-link">ביטול עסקה</a>
  ---

### משימה 2: [קריטי] שיגור מעקבי רשת ופרסום ללא הסכמה מוקדמת (עקיפת באנר קוקיז) (PRV-CONSENT-BYPASS-001)
- **מיקום:** קוד המקור של האתר והפوتر
- **הנחיית ביצוע:** יש להגדיר את מערכת ניהול התגיות (GTM) כך שפיקסלים של צדדים שלישיים ייטענו אך ורק לאחר לחיצה פעילה על כפתור האישור בבאנר. [הנחיית תכנון מילולית בלבד (ללא כתיבת קוד אוטומטית עיוורת)]
- **קוד/נוסח מומלץ:**
  /* הנחיית תכנון מילולית בלבד (ציון בטיחות: 75/100 - ללא קוד אוטומטי) */
  /* הנחיה עקרונית: יש להגדיר את מערכת ניהול התגיות (GTM) כך שפיקסלים של צדדים שלישיים ייטענו אך ורק לאחר לחיצה פעילה על כפתור האישור בבאנר. יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור. */
  ---

### משימה 3: [קריטי] מעקב לא מוצהר (Meta Pixel (Facebook) (TRK-UNDISC-METAPIXELF)
- **מיקום:** קוד המקור של האתר והפوتر
- **הנחיית ביצוע:** [משימת תכנון ובדיקה ידנית (Manual Engineering Only) - אל תייצר קוד אוטומטי] עדכן את מדיניות
```

html``

*/ סיכון ארכיטקטוני גבוה: חובה לבצע בדיקה ידנית מותאמת אישית ע"י מפתח מוסמך בסביבת פיתוח */

- **מיקום: ** קוד המקור של האתר והפוסט

- **קוד/נוסח מומלץ: **

html``

*/ סיכון ארכיטקטוני גבוה: חובה לבצע בדיקה ידנית מותאמת אישית ע"י מפתח מוסמך בסביבת פיתוח */

- **מיקום:** אלמנט ב-`<button class="btn-add-to-cart`
DOM: `<button class="btn-add-to-cart`
לסל הקניות`>`<button/>

- **הנחיית ביצוע: ** בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C

- **קוד/נוסח מומלץ: **

```
html``
```

* / יש לבצע בדיקת ניגודיות צבעים (יחס 4.5:1 לפחות) ולהזהרות את גוון הטקסט או להבהיר את הרקע בהגדרות ה-CSS, מבלי לפגוע בפלטת שפת המותג. / *

לפגוע בפלטת שפת המותג. /*

- **מיקום: ** קוד המקור של האתר והפוסט

- **קוד/נוסח מומלץ: **

html``

```
/* הנחיה עקרונית: הגדר בשרת כותרת HSTS: Strict-Transport-Security: max-age=31536000 יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור. */
```

זו בסביבת פיתוח ובדיקות לפני העלאה לייצור. /*

- **מיקום: ** קוד המקור של האתר והפוסטר

[הנחיית תכנון מילולית בלבד (ללא כתיבת קוד אוטומטית עיוורת)]

- **קוד/נוסח מומלץ: **

html``

/ הנחיה עקרונית: יש להוסיף סעיף מפורש המציין כתובת דוא"ל ישראל לפניה לצורך עיון ומחיקת מידע אישי ממאגרי העסק. יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור. /

לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור. /*

- **מיקום: ** קוד המקור של האתר והפוסט

```

- **הנחיית ביצוע:** [משימת תכנון ובדיקה ידנית (Manual Engineering Only - אל תייצר קוד אוטומטי)] [עדכן את מדיניות הפרטיות כך שתכלול במפורש את הכלי Microsoft Clarity ומטרות השימוש בו.
- **קוד/נוסח מומלץ:**
html`
/* הסום לייצור קוד או פרומפט אוטומטי (ציון בטיחות: 65/100) */
/* סיכון ארכיטקטוני גבוה: חובה לבצע בדיקה ידנית מותאמת אישית ע"י מפתח מוסמך בסביבת פיתוח */
/* מדיניות בטיחות תקין: תיקון זה כרוך בסיכון ארכיטקטוני גבוה ונוגע בלוגיקת שרת רגישה / טפסים פעילים / מסדי נתונים. כדי למנוע שיבוש של פעילות האתר, מערכות הסליקה או נתוני משתמשים - המערכת אינה מנפקת קוד או פרומפט אוטומטי. חובה להעביר את פרטי הליקוי למפתח האתר לבדיקה ותיקון מותאם אישית בסביבת פיתוח. */
`

### משימה 9: [גבוה] ליקוי נגישות בקוד האתר (image-alt) (AXE-IMAGE-ALT)
- **מיקום:** אלמנט ב-`<img src="/assets/demo-shirt.jpg" class="product-thumbnail`
- **הנחיית ביצוע:** בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C:
https://dequeuniversity.com/rules/axe/4.4/image-alt
- **קוד/נוסח מומלץ:**
html`
<-- AXE-IMAGE-ALT עבור מותאם עבור AXE-IMAGE-ALT
<-- בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C:
<-- https://dequeuniversity.com/rules/axe/4.4/image-alt
`

### משימה 10: [בינוני] ליקוי נגישות בקוד האתר (focus-visible) (AXE-FOCUS-VISIBLE)
- **מיקום:** אלמנט ב-`<a href="/catalog" style="outline: none`
- **הנחיית ביצוע:** בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C:
https://dequeuniversity.com/rules/axe/4.4/focus-visible
[הנחיית תכנון מילולית בלבד (ללא כתיבת קוד אוטומטית עיוורת)]
- **קוד/נוסח מומלץ:**
html`
/* הנחיית תכנון מילולית בלבד (ציון בטיחות: 75/100 - ללא קוד אוטומטי) */
/* הנחיה עקרונית: בצע תיקון התאמת נגישות ברכיבי ה-DOM המסומנים לפי הנחיות ה-W3C:
https://dequeuniversity.com/rules/axe/4.4/focus-visible
יש לבצע התאמה זו בסביבת פיתוח ובדיקות לפני העלאה לייצור. */
`

- - -
**הוראה סופית:** לאחר ביצוע כל משימה, ודא שהקוד מתקמפל ללא שגיאות ושאר תכונה קיימת לא נפגעה.

```