

DATENSCHUTZ · WEB-SICHERHEIT · EVIDENZ

Datenschutz- und Web-Sicherheitsprüfung

Demo Report GmbH (fiktiv) · www.demo-report.de
<https://www.demo-report.de/>

Fallreferenz	Ziel / Scanzeit	Status / Vollständigkeit	Technik / Consent
PA-DEMO-20261011-HELMSTEDT-001	www.demo-report.de · 24.10.2026, 20:04:38 UTC	Technisch fertig · mit Einschränkungen ·	Vollständig · Verifiziert
Profil / Priorität / Schema			
Kompakt · 100/100 · v2			

00 GLOSSAR · THEMENINDEX

Hauptpunkte des Berichts

Diese Übersicht führt zu den zentralen Themen des Prüfdossiers. Klicken Sie auf einen Punkt, um im PDF direkt zum entsprechenden Abschnitt zu springen. Die ausführlichen Definitionen stehen im Glossar am Ende des Berichts.

GLOSSAR · THEMENINDEX		Klickbare Navigation
Themenübersicht		
	01 Übersicht & Prüfstatus Fallreferenz, Ziel-URL, Weiterleitungen, Scanzeit, Prüfprofil und technischer Status bilden den festen Rahmen. Kennzahlen und Coverage zeigen, welche Teile des Auftrags abgeschlossen, eingeschränkt oder noch offen sind.	
	02 Methodik & Grenzen Der passive Browserlauf bildet den normalen Aufruf mit Consent-, Request-, Storage- und DOM-Beobachtung ab. Grenzen, nicht ausgeführte aktive Tests und offene manuelle Fragen werden ausdrücklich getrennt dokumentiert.	
	03 Vollständigkeit Quellen, Seitensichten, Zustände, Rechtstexte und Evidence werden auf Verfügbarkeit und Konsistenz geprüft. Nicht erreichbare Pfade, fehlende Dokumente und unvollständige Abdeckung erscheinen als eigene Einschränkung.	
	04 Verantwortlichkeit & Zuständigkeit Verantwortliche Stelle, DSB, Behördenbezug und erkennbare Zuständigkeiten werden aus den erfassten Quellen zusammengeführt. Widersprüche, abweichende Adressen und unsichere Ableitungen bleiben ausdrücklich markiert.	
	05 Hauptbefunde Die wichtigsten technischen Beobachtungen stehen mit Priorität, Feststellung, Quelle und Evidence-Bezug im Mittelpunkt. Jeder Befund führt zu einem nachvollziehbaren manuellen Prüfschritt oder einer konkreten Maßnahme.	
	06 Consent-Prüfung Einwilligungsoberfläche, Zustandswechsel, Cookies und Tracking-Signale werden getrennt betrachtet. Vor-, Ablehnungs- und Akzeptanzzustände werden nur verglichen, wenn die jeweilige Aktion und ihre technische Wirkung bestätigt wurden.	
	07 Datenfluss & Rechtstexte Requests, Speicher, Drittanbieter sowie Impressum und Datenschutz werden in Beziehung gesetzt. Der Abgleich zeigt, ob beobachtete technische Signale in den erfassten Rechtstexten nachvollziehbar beschrieben oder offen gelassen werden.	
	08 Web-Sicherheit Header, TLS, Skripte, Bibliotheken, Formulare und weitere Härtungssignale werden technisch dokumentiert. Der Abschnitt beschreibt konkrete Hinweise, Schutzlücken und Prüfgrenzen, ersetzt aber keinen vollständigen Penetrationstest.	
	09 Portal- und Seitenerfassung Interne Seiten, Weiterleitungen, externe Portale und eingebettete Dienste werden getrennt erfasst. Nicht klassifizierte Bewerbungs- oder Portalpfade werden nicht durch allgemeine Template-Texte ersetzt.	
	10 Rechtskontext & Folgen Technische Hinweise werden mit Normbezügen, offenen Fragen und möglichen Folgen in einen Prüfkontext gestellt. Die Einordnung unterstützt die Fachprüfung und macht Klärungsbedarf sichtbar, ist aber keine Rechtsberatung oder verbindliche Subsumtion.	
	11 Mögliche Rechtsfolgen Mögliche behördliche, gesetzliche oder private Folgen werden nur als fallabhängige Prüffragen beschrieben. Der Bericht nennt keine automatische Sanktion und leitet keinen festen Geldbetrag aus einem technischen Signal ab.	
	12 Maßnahmen & Empfehlungen Aus den bestätigten technischen Beobachtungen werden priorisierte nächste Schritte abgeleitet. Jede Empfehlung trennt Auslöser, Begrenzung, Umsetzung, zuständige Rolle und erneute Verifikation.	
	13 Evidence & Integrität Screenshots, HAR, Evidence-IDs, Manifest und Integritätsstatus verknüpfen Beobachtung und Bericht. Strukturierte Report-Nachweise werden zusätzlich kenntlich gemacht, wenn kein eigenes Dateiartefakt existiert.	
	14 Vergleichsrechtsprechung Vergleichsentscheidungen und offizielle Quellen dienen als Einordnungsrahmen. Sie ersetzen keine fallbezogene juristische Prüfung und werden mit ihrem Verifikationsstatus ausgewiesen.	
	15 Technischer Anhang Der vollständige Befundindex, die Zustandszusammenfassung und die technischen Verweise bündeln die Detailsicht. Rohdaten bleiben im Evidence Package und werden nicht als ungeprüfte Kundenaussage ausgegeben.	
	16 Kommunikationsentwürfe Kommunikationsentwürfe für DSB, Aufsicht oder Fachpartner liegen getrennt und ausdrücklich als nicht automatisch versendbare Entwürfe vor. Empfänger, Zuständigkeit und Sachverhalt sind vor Versand manuell zu prüfen.	
	17 Glossar & Definitionen Zentrale technische, organisatorische und rechtliche Fachbegriffe werden verständlich erklärt und voneinander abgegrenzt. Das Glossar erleichtert die gemeinsame Arbeit von Technik, Datenschutz, Rechtsabteilung und Fachpartnern.	
Technische Sicht Quelltext, DOM, Browser, Requests und Speicher werden als beobachtbare Primärsignale getrennt erfasst.	Einordnung Befunde, Verantwortlichkeiten und Rechtstexte werden miteinander abgeglichen und mit ihren Grenzen ausgewiesen.	Nachweis Evidence, IDs und Integritätsinformationen verbinden die technische Beobachtung mit dem jeweiligen Berichtsteil.

01MANAGEMENT SUMMARY

Executive Summary

ALLGEMEINE EINLEITUNG

Der folgende Bericht beginnt mit einer allgemeinen technischen Einordnung. Treeology PA beobachtet öffentlich erreichbare Browserpfade und beschreibt sichtbare Datenflüsse, Einwilligungszustände, Speicher, Rechtshinweise und Sicherheitsmerkmale. Die Darstellung unterstützt die fachliche Prüfung; sie ersetzt weder Rechtsberatung noch eine vollständige Prüfung nicht erreichbarer oder serverseitiger Verarbeitung.

AUTOMATISCHE SEITENKLASSIFIZIERUNG

Nicht abschließend klassifiziert

Die automatische Klassifizierung ist nicht abschließend: Es lagen keine ausreichenden Klassifizierungssignale vor.
Weitere erkannte Signale: Keine zusätzlichen Kategorien

STATUS	KONFIDENZ	SEITEN
Nicht abschließend klassifiziert	0 %	0

Quelle: Kategorie-Modul · Methode: regelbasiertes Ensemble · Die Kategorie ist ein technischer Hinweis und keine Betreiber-, Branchen- oder Rechtsfeststellung.

Getrennte Klassifikationsdimensionen

Betreiber, Branche, technische Plattform und Seitentyp werden getrennt bewertet. Ein CMS-Signal wird nicht als Betreiber- oder Branchenbeweis verwendet.

DIMENSION	ERGEBNIS	STATUS	KONFIDENZ	BELEGBASIS
Betreiber	Nicht verifiziert	nicht abschließend	nicht quantifiziert	Keine Basis aufgezeichnet
Branche	Nicht verifiziert	nicht abschließend	nicht quantifiziert	Keine Basis aufgezeichnet
Technologie	Nicht verifiziert	nicht abschließend	nicht quantifiziert	Keine Basis aufgezeichnet
Seitentyp	Nicht verifiziert	nicht abschließend	nicht quantifiziert	Keine Basis aufgezeichnet

PRÜFGEGENSTAND

Demo Report GmbH (fiktiv)

<https://www.demo-report.de/>

TECHNISCH FERTIG · MIT EINSCHRÄNKUNGEN

Fallpriorität Hoher Prüfbedarf

BEFUNDE GESAMT

21

vollständiger Befundindex

RELEVANTE BEFUNDE

10

manueller Prüfbedarf

PRÜFPRIORITÄT

100

/ 100 · Hoher Prüfbedarf

VOLLSTÄNDIGKEIT

TEILWEISE

technischer Reportstatus



TEILBEREICHE NICHT ABSCHLIESSEND VERIFIZIERT

Der Scan ist technisch verwertbar. Die folgenden Punkte begrenzen jedoch die Aussagekraft einzelner Teilvergleiche.

- Mindestens eine aktivierte offizielle aktuelle Rechtsquelle wurde nicht vollständig verifiziert.

Wichtigste Befunde – Kurzfassung

- DEMO-SYN-001 · Abweichende Verantwortlichenadresse · **ERHÖHT** Details im Abschnitt „Hauptbefunde“.
- DEMO-SYN-002 · Cookie- und Consent-Verstoß simuliert · **HOCH** Details im Abschnitt „Hauptbefunde“.
- DEMO-SYN-003 · Passwort im Local Storage simuliert · **HOCH** Details im Abschnitt „Hauptbefunde“.
- DEMO-SYN-004 · API-Key im JavaScript simuliert · **HOCH** Details im Abschnitt „Hauptbefunde“.
- DEMO-SYN-014 · Passwortfund im JavaScript simuliert · **HOCH** Details im Abschnitt „Hauptbefunde“.