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 · 07.11.2026, 00:23:54 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

Themenübersicht

Klickbare Navigation

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 Detailansicht. 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.

01 MANAGEMENT SUMMARY

Executive Summary

ALLGEMEINE EINLEITUNG

Der folgende Bericht beginnt mit einer allgemeinen technischen Einordnung. Treelogy 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

23

vollständiger Befundindex

RELEVANTE BEFUNDE

9

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-015** · Passwort in ausgeliefertem JavaScript simuliert · KRITISCH Details im Abschnitt „Hauptbefunde“.
- **DEMO-SYN-016** · Secret in öffentlicher JSON-Datei simuliert · HOCH Details im Abschnitt „Hauptbefunde“.
- **DEMO-SYN-013** · Kritischer Sicherheitszustand simuliert · KRITISCH Details im Abschnitt „Hauptbefunde“.
- **DEMO-SYN-005** · Tracking vor Einwilligung an US-Signal simuliert · HOCH Details im Abschnitt „Hauptbefunde“.
- **DEMO-SYN-006** · Veraltete beziehungsweise kritische jQuery-Version simuliert · ERHÖHT Details im Abschnitt „Hauptbefunde“.
- **DEMO-SYN-007** · Widersprüchliche Rechtspassage simuliert · ERHÖHT Details im Abschnitt „Hauptbefunde“.
- **DEMO-SYN-008** · Mouseflow im Bewerberbereich simuliert · ERHÖHT Details im Abschnitt „Hauptbefunde“.

Priorität 100 / 100

HOHER PRÜFBEDARF

Rohsumme 313; Familienkorrelation und unabhängige Gruppen werden separat ausgewiesen; Final vor Begrenzung 156.

Befundverteilung: Kritisch: 2 · Hoch: 3 · Erhöht: 4 · Hinweis: 11 · Niedrig: 2

Score-Kalibrierung: Evidence-Faktoren und Familienkappen wurden angewendet; direkt beobachtete Kritisch-Befunde bleiben im hohen Prüfband.

Prüfpriorität 0-100: Je qualifiziertem Grundbefund werden Schweregrad, Evidence-Qualität und beobachteter Kontext kombiniert. Heuristische oder nicht verifizierte Signale erhalten einen reduzierten Faktor; Risikofamilien und Root-Korrelationen begrenzen Doppelzählung. Der Wert ist kein Geldwert, kein Compliance-Prozentsatz und kein Beweis eines Rechtsverstoßes.

LESART DER SKALA

- **0–19** Kein erhöhter automatischer Prüfhinweis. Geringe oder keine qualifizierten Signale; normale fachliche Kontrolle bleibt sinnvoll.
- **20–49** Erhöhter Prüfbedarf. Mindestens ein qualifiziertes Signal sollte manuell reproduziert und eingeordnet werden.
- **50–100** Hoher Prüfbedarf. Mehrere oder besonders gewichtete qualifizierte Signale sollten zuerst geprüft werden.

DEMO-SYN-001 **+0**

Abweichende Verantwortlichenadresse

Roh +22; Familie Sonstige; Final +0; Korrelation -22; Evidence-Faktor 1.00

Kein zusätzlicher Score: Die Risikofamilie ist bereits durch einen stärkeren oder gleichartigen Befund abgedeckt.

Technische Referenz: ROOT-DEMO-DEMO-SYN-001

DEMO-SYN-002 **+18**

Cookie- und Consent-Verstoß simuliert

Roh +43; Familie Speicher/Consent; Final +18; Korrelation -25; Evidence-Faktor 1.00

Der Beitrag wurde wegen Root-/Familienkorrelation begrenzt, damit dieselbe Beobachtung nicht mehrfach voll gezählt wird.

Technische Referenz: ROOT-DEMO-DEMO-SYN-002

DEMO-SYN-005 **+39**

Tracking vor Einwilligung an US-Signal simuliert

Roh +39; Familie Consent/Tracking; Final +39; Korrelation -0; Evidence-Faktor 1.00

Eigenständiger Beitrag zur Prüfpriorität auf Basis von Schweregrad, Evidence und beobachtetem Kontext.

Technische Referenz: ROOT-DEMO-DEMO-SYN-005

DEMO-SYN-006 **+0**

Veraltete beziehungsweise kritische jQuery-Version simuliert

Roh +22; Familie Sonstige; Final +0; Korrelation -22; Evidence-Faktor 1.00

Kein zusätzlicher Score: Die Risikofamilie ist bereits durch einen stärkeren oder gleichartigen Befund abgedeckt.

Technische Referenz: ROOT-DEMO-DEMO-SYN-006

DEMO-SYN-007 **+0**

Widersprüchliche Rechtspassage simuliert

Roh +22; Familie Sonstige; Final +0; Korrelation -22; Evidence-Faktor 1.00

Kein zusätzlicher Score: Die Risikofamilie ist bereits durch einen stärkeren oder gleichartigen Befund abgedeckt.

Technische Referenz: ROOT-DEMO-DEMO-SYN-007

DEMO-SYN-008 **+0**

Mouseflow im Bewerberbereich simuliert

Roh +17; Familie Sonstige; Final +0; Korrelation -17; Evidence-Faktor 1.00

Kein zusätzlicher Score: Die Risikofamilie ist bereits durch einen stärkeren oder gleichartigen Befund abgedeckt.

Technische Referenz: ROOT-DEMO-DEMO-SYN-008

DEMO-SYN-013 **+35**

Kritischer Sicherheitszustand simuliert

Roh +50; Familie Sonstige; Final +35; Korrelation -15; Evidence-Faktor 1.00

Der Beitrag wurde wegen Root-/Familienkorrelation begrenzt, damit dieselbe Beobachtung nicht mehrfach voll gezählt wird.

Technische Referenz: ROOT-DEMO-DEMO-SYN-013

DEMO-SYN-015 **+50**

Passwort in ausgeliefertem JavaScript simuliert

Roh +50; Familie Secrets/Zugangsdaten; Final +50; Korrelation -0; Evidence-Faktor 1.00

Eigenständiger Beitrag zur Prüfpriorität auf Basis von Schweregrad, Evidence und beobachtetem Kontext.

Technische Referenz: ROOT-DEMO-DEMO-SYN-015

DEMO-SYN-016 **+10**

Secret in öffentlicher JSON-Datei simuliert

Roh +35; Familie Secrets/Zugangsdaten; Final +10; Korrelation -25; Evidence-Faktor 1.00

Der Beitrag wurde wegen Root-/Familienkorrelation begrenzt, damit dieselbe Beobachtung nicht mehrfach voll gezählt wird.

Technische Referenz: ROOT-DEMO-DEMO-SYN-016

IMP-002 **+0**

Anbieterkennzeichnung nicht eindeutig zuordenbar

Roh +8; Familie Sonstige; Final +0; Korrelation -8; Evidence-Faktor 0.85

Kein zusätzlicher Score: Die Risikofamilie ist bereits durch einen stärkeren oder gleichartigen Befund abgedeckt.

Technische Referenz: ROOT-imprint-availability

PA-F-0002 **+0**

Ablehnen weniger prominent

Roh +5; Familie Sonstige; Final +0; Korrelation -5; Evidence-Faktor 0.55

Kein zusätzlicher Score: Die Risikofamilie ist bereits durch einen stärkeren oder gleichartigen Befund abgedeckt.

Technische Referenz: ROOT-ablehnen-weniger-prominent

Unabhängigkeitsbonus **+4**

Fachlich getrennte Gruppen

Unabhängige Fachgruppen +4: Sonstige, Privacy/Consent, Security

Kleine Zusatzwertung für fachlich getrennte Risikogruppen; sie ersetzt keinen eigenen Befund.

Zusammenführung gleicher Grundbeobachtungen: Mehrfachdarstellungen derselben Beobachtung werden nur einmal gewertet.

Seitensignale und Scanumfang

MERKMAL	BEOBACHTUNG
Meta-Description	Nicht aufgezeichnet
CMS / Technologie	Nicht eindeutig erkannt
Frontend-Bibliothekskatalog	frontend-libraries-8.7-1
Globaler Signalkatalog	global-signals-8.7-1
Native-Klassifikator	native-technology-rules-8.7-1
Finale Ziel-URL	https://www.demo-report.de/
Vorgeschaltete Seiten	0
PDF-Seiten	Noch nicht bestimmt

Meta-Description, CMS- und Technologieangaben sind technische Seitensignale. Sie bestätigen weder Betreiberidentität noch eine rechtliche Einordnung.

Vergleich zum letzten Lauf

Kein echter Vorbericht; Varianten werden ausschließlich simuliert.

ART	SIGNAL	BEOBACHTUNG
simuliert	Vor Einwilligung	Marketing-Request
simuliert	Nach Ablehnen	Marketing blockiert
simuliert	Nach Akzeptieren	Marketing aktiviert

Prüfstatus

- ! **Gesamtstatus:** Teilweise · Teilbereiche separat bewerten.
- ✓ **Ablehnung:** Nach Ablehnen
- ✓ **Akzeptanz:** Nach Akzeptieren
- ✓ **Verantwortlicher:** nicht aufgelöst

Leitplanken der Einordnung

Relevant = mindestens ein Befund der Stufe Erhöht/Hoch oder ein juristisch bzw. inhaltlich relevanter Hinweis mit ausdrücklichem manuellem Prüfbedarf; technische Hinweise sind keine bewiesenen Rechtsverstöße.

Die Skala unterstützt nur die Reihenfolge der manuellen Prüfung. Sie ist kein Compliance-Prozentsatz, kein Geldwert und kein Nachweis eines Rechtsverstoßes.

02 METHODIK

Prüfmethodik und Grenzen

Technischer Ablauf

1. Passiver Abruf der Zielseite im gebündelten Chromium-Renderer.
2. Erfassung von Netzwerk, Cookies, Speicher, Ereignissen, Formularen und Sicherheits-Headern.
3. Getrennte Consent-Szenarien; keine Anmeldung, kein Versand und keine offensiven Interaktionen.
4. Zusammenführung der Befunde mit Belegverweisen und Integritätsnachweisen.

Rahmenbedingungen

MERKMAL	AUFGEZEICHNETER WERT
Browser	Chromium · nicht ausgeführt, nur simuliert
Scanmodus	Passiver Lauf
Export	Anwaltsbericht · Kompakt
Schema	2
Scanengine	Playwright/Chromium · synthetische Fixture
Rechtsregeln	8.7-demo · nicht live verifiziert
Exporter	8.7-demo
Module	Keine Modulliste aufgezeichnet.
Frische Sitzung pro Zustand	Nicht aufgezeichnet
Technische Handlungshinweise	Deaktiviert
Zeitpunkt	07.11.2026, 00:23:54 UTC

Grenzen der automatischen Einordnung: Dieser Bericht ist eine technische Beobachtung und keine gerichtsfeste Rechtsentscheidung oder abschließende Rechtsberatung. Nicht automatisch geprüft werden insbesondere Rechtsgrundlagen je Verarbeitung, Auftragsverarbeitungsverträge, Vollständigkeit und Richtigkeit der Datenschutzerklärung, Drittlandgarantien, die Erforderlichkeit einzelner Endgerätezugriffe sowie die tatsächliche Empfänger- und Betreiberrolle. Nicht bestätigte Consent-Aktionen werden nicht als ausgeführte Ablehnung oder Akzeptanz ausgegeben. Ein Befund der Stufe „Erhöht“ beschreibt konkreten manuellen Prüfbedarf bzw. ein starkes Indiz; er beweist allein keinen Rechtsverstoß.

Seitenerfassung

Status AUSREICHEND

Synthetische Fixture mit vollständig vorbereiteten Zuständen; keine Live-Erreichbarkeit.

Auswirkung auf Negativbefunde

Negativbefunde zu nicht auffindbaren Links werden bei unvollständiger Seitenerfassung nicht als belastbare Fehlbefunde gewertet.

Footer-/Navigationsprüfung und Prüfung desselben Hosts werden separat als Abdeckungssignale gespeichert.

03 QUALITÄTSSICHERUNG

Prüfvollständigkeit

Gesamtstatus TEILWEISE

Die Vollständigkeit trennt technische Beobachtungen von nicht abschließend verifizierten Teilbereichen. Konkrete Befunde bleiben auch bei einem partiellen Scan sichtbar.

TEILBEREICH	STATUS	BEGRÜNDUNG
Rechtsprüfung	OFFEN	Mindestens eine aktivierte offizielle aktuelle Rechtsquelle wurde nicht vollständig verifiziert.

Offene Prüfgründe

Mindestens eine aktivierte offizielle aktuelle Rechtsquelle wurde nicht vollständig verifiziert.

04 VERANTWORTUNG

Verantwortlichkeit und Zuständigkeit

IDENTITÄTSAUFLÖSUNG

NICHT BESTÄTIGT

Demo Report GmbH (fiktiv)

Geprüfte URL: https://www.demo-report.de/
Geprüfte Domain: www.demo-report.de

ANSCHRIFT

Demoweg 7 · 38350 Helmstedt · Deutschland

Veröffentlichter Impressumskontakt: max.mustermann@example.invalid

ROLLE	ERGEBNIS	STATUS
Verantwortlicher	Demo Report GmbH (fiktiv)	Bestätigt
Impressumsanbieter	Demo Report GmbH (fiktiv)	Bestätigt
Technischer Betreiber	Nicht angegeben	Nicht bestätigt
Technische Umsetzung	Nicht angegeben	Nicht angegeben
Datenschutzbeauftragter	Daniela Datenschutz (fiktiv) +49 5351 000000 (fiktiv) daniela.datenschutz@example.invalid	Externer DSB-Dienstleister
Aufsichtsbehörde	Fiktive Datenschutzaufsicht Niedersachsen – Demo	Nicht bestätigt / nicht automatisch bestimmbar

Zuständige Behörde

Fiktive Datenschutzaufsicht Niedersachsen – Demo

Anschrift: Behördenweg 1, 38350 Helmstedt (fiktiv)
E-Mail: aufsicht-niedersachsen@example.invalid
Offizielle Website: https://aufsicht-niedersachsen.example.invalid/

Bei möglicher Datenverletzung: Sachverhalt und Evidence sichern, Verantwortliche und Datenschutzbeauftragte einbeziehen und die Melde- und Informationspflichten nach Art. 33 und 34 DSGVO einschließlich der 72-Stunden-Frist fallbezogen prüfen und dokumentieren.

Identitätskonflikte

Keine Identitätskonflikte aufgezeichnet.

Einordnung: Ein Domainname entscheidet nicht automatisch, welche Stelle rechtlich verantwortlich ist. Widersprechende Quellen werden deshalb getrennt ausgewiesen und nicht stillschweigend zusammengeführt.

Nächster Schritt: Zur Auflösung: Impressum und Datenschutzerklärung im Original öffnen, Betreibername, Anschrift, Kontakt und gegebenenfalls Portal-/Arbeitgeberrolle vergleichen und das Ergebnis manuell bestätigen.

Adress- und Personenabgleich

Die Anreicherung gruppiert nur quellengebundene Kandidaten und Schreibvarianten. Primärquelle, Evidence und menschliche Prüfung bleiben maßgeblich. Keine lokale KI wurde automatisch ausgeführt; es wurden keine Daten an einen externen KI-Dienst gesendet.

ROLLE	NAME / ORGANISATION	ANSCHRIFT	QUELLE / STATUS
Keine quellengebundenen Adress- oder Personenkandidaten ermittelt.			

Quellen: 0 · **Manuelle Prüfung:** nicht erforderlich auf Basis der erfassten Quellen

05 BEFUNDE

Hauptbefunde

Die folgenden Karten zeigen die Befunde mit konkretem manuellem Prüfbedarf. Jede Karte führt technische Feststellung, rechtlichen Prüfkontext, offene Fragen, Empfehlung und Evidence zusammen.

01 DEMO-SYN-001 · Synthetischer Demo-Befund

ERHÖHT

Abweichende Verantwortlichenadresse

FESTSTELLUNG
DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Im fiktiven Anbietertext steht Demoweg 7, 38350 Helmstedt; der ebenfalls fiktive Policy-Text nennt Demoallee 12, 30159 Hannover.

TECHNISCHE BEDEUTUNG
Synthetischer Demo-Befund

OFFENE FRAGEN
Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE
`nicht separat aufgezeichnet`

THEMATISCHE EINORDNUNG
Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

RECHTLICHER PRÜFKONTEXT
Kernnormen: Keine konkrete Normzuordnung im automatischen Lauf. · Mappingstatus: Keine konkrete Normzuordnung

EMPFEHLUNG
Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT
`E-LAW-001`

02 DEMO-SYN-002 · Synthetischer Demo-Befund

HOCH

Cookie- und Consent-Verstoß simuliert

FESTSTELLUNG
DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Vor einer Entscheidung wird im synthetischen Lauf ein Marketing-Cookie gesetzt; Ablehnen und Akzeptieren sind als getrennte Zustände dokumentiert.

TECHNISCHE BEDEUTUNG
Vor der Consent-Entscheidung wurden Browser-Speichereinträge beobachtet. Die Auswertung verwendet nur Namen, Anzahl und technische Metadaten; Werte und konkrete Zwecke wurden nicht ausgegeben. Ob ein Eintrag unbedingt erforderlich ist oder erst durch die geprüfte Seite angelegt wurde, ist separat zu prüfen.

OFFENE FRAGEN
Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE
`01_vor_einwilligung.har; E-STORAGE-001`

THEMATISCHE EINORDNUNG
Das Thema betrifft Zugriffe auf Informationen im Endgerät. Zweck, Erforderlichkeit, Lebensdauer und Einwilligungsabhängigkeit müssen je Eintrag im konkreten Kontext geprüft werden.

RECHTLICHER PRÜFKONTEXT
Kernnormen: Keine konkrete Normzuordnung im automatischen Lauf. · Mappingstatus: Keine konkrete Normzuordnung

EMPFEHLUNG
Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT
`E-LAW-002`

03 DEMO-SYN-015 · Synthetischer Demo-Befund

KRITISCH

Passwort in ausgeliefertem JavaScript simuliert

FESTSTELLUNG
DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. In einem fiktiven JavaScript-Bundle wird ein redigierter Passwortwert mit der synthetischen Fundstelle `assets/app.demo.js:42` markiert. Es wird kein Rohwert gespeichert.

TECHNISCHE BEDEUTUNG
Synthetischer Demo-Befund

OFFENE FRAGEN
Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE
`nicht separat aufgezeichnet`

THEMATISCHE EINORDNUNG
Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

RECHTLICHER PRÜFKONTEXT
Kernnormen: Art. 32 DSGVO · Ergänzend: Art. 5 DSGVO; Art. 25 DSGVO; Art. 33/34 DSGVO (nur bei bestätigter Verletzung) · Mappingstatus: Manuelle Prüfung

EMPFEHLUNG
Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT
`E-LAW-004`

04 DEMO-SYN-016 · Synthetischer Demo-Befund

Secret in öffentlicher JSON-Datei simuliert

HOCH

FESTSTELLUNG

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Eine fiktive `config.demo.json` enthält ein redigiertes, nicht öffentlich gedachtes Secret-Signal. Die Demo speichert weder Rohwert noch nutzbares Credential.

TECHNISCHE BEDEUTUNG

Synthetischer Demo-Befund

OFFENE FRAGEN

Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE

nicht separat aufgezeichnet

THEMATISCHE EINORDNUNG

Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

RECHTLICHER PRÜFKONTEXT

Kernnormen: Art. 32 DSGVO · Ergänzend: Art. 5 DSGVO; Art. 25 DSGVO; Art. 33/34 DSGVO (nur bei bestätigter Verletzung) · Mappingstatus: Manuelle Prüfung

EMPFEHLUNG

Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT

E-LAW-005

05 DEMO-SYN-013 · Synthetischer Demo-Befund

Kritischer Sicherheitszustand simuliert

KRITISCH

FESTSTELLUNG

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Die Demo stellt absichtlich einen kritischen technischen Zustand dar, bei dem eine zentrale Schutzkontrolle als unwirksam markiert ist. Es handelt sich um eine synthetische Ausprägung ohne reale Zielseite, Verbindung oder ausnutzbares System.

TECHNISCHE BEDEUTUNG

Synthetischer Demo-Befund

OFFENE FRAGEN

Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE

nicht separat aufgezeichnet

THEMATISCHE EINORDNUNG

Das Thema betrifft die technische Absicherung der Auslieferung. Ein einzelner Header ist nur im Zusammenspiel mit HTTPS, Ressourcenpfaden, Browserverhalten und Serverkonfiguration zu bewerten.

RECHTLICHER PRÜFKONTEXT

Kernnormen: Keine konkrete Normzuordnung im automatischen Lauf. · Mappingstatus: Keine konkrete Normzuordnung

EMPFEHLUNG

Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT

E-LAW-007

06 DEMO-SYN-005 · Synthetischer Demo-Befund

Tracking vor Einwilligung an US-Signal simuliert

HOCH

FESTSTELLUNG

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Vor Einwilligung wird ein synthetischer Request an `analytics-us.demo-report.example` mit US-Anbieter-Signal dokumentiert.

TECHNISCHE BEDEUTUNG

Der Zielhost oder Request passt zu einer bekannten Analyse-/Tracking-Signatur. Das ist ein technischer Hinweis auf einen Datenfluss; die Signatur allein beweist weder die übertragenen Daten noch deren Personenbezug oder die rechtliche Zulässigkeit.

OFFENE FRAGEN

Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE

E-NET-001

THEMATISCHE EINORDNUNG

Das Thema betrifft beobachtete Analyse- oder Identifikatorsignale. Hostname und Parametername belegen einen technischen Datenfluss, aber allein weder Personenbezug noch zulässige Rechtsgrundlage.

RECHTLICHER PRÜFKONTEXT

Kernnormen: Art. 12 DSGVO; Art. 13 DSGVO · Ergänzend: Art. 28 DSGVO; Art. 44 ff. DSGVO · Mappingstatus: Manuelle Prüfung

EMPFEHLUNG

Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT

E-LAW-009

07 DEMO-SYN-006 · Synthetischer Demo-Befund

Veraltete beziehungsweise kritische jQuery-Version simuliert

ERHÖHT

FESTSTELLUNG

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Das Demo-Frontend lädt synthetisch jQuery 1.11.2 und markiert die Version als veraltet.

TECHNISCHE BEDEUTUNG

Synthetischer Demo-Befund

OFFENE FRAGEN

Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE

nicht separat aufgezeichnet

THEMATISCHE EINORDNUNG

Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

RECHTLICHER PRÜFKONTEXT

Kernnormen: Keine konkrete Normzuordnung im automatischen Lauf. · Mappingstatus: Keine konkrete Normzuordnung

EMPFEHLUNG

Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT

E-LAW-010

DEMO-SYN-007 · Synthetischer Demo-Befund

08 Widersprüchliche Rechtspassage simuliert

ERHÖHT

FESTSTELLUNG

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Der fiktive Policy-Text nennt für denselben Dienst gleichzeitig Einwilligung und berechtigtes Interesse als alleinige Grundlage.

TECHNISCHE BEDEUTUNG

Synthetischer Demo-Befund

OFFENE FRAGEN

Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE

`nicht separat aufgezeichnet`

THEMATISCHE EINORDNUNG

Das Thema betrifft die technische Wirkung einer Einwilligungsentscheidung. Eine angezeigte Schaltfläche und ein API-Aufruf sind erst bei beobachtbarer Zustandsänderung ein belastbarer Nachweis.

RECHTLICHER PRÜFKONTEXT

Kernnormen: Keine konkrete Normzuordnung im automatischen Lauf. · Mappingstatus: Keine konkrete Normzuordnung

EMPFEHLUNG

Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT

`E-LAW-011`

DEMO-SYN-008 · Synthetischer Demo-Befund

09 Mouseflow im Bewerberbereich simuliert

ERHÖHT

FESTSTELLUNG

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Auf dem fiktiven Karriere- und Bewerberpfad wird ein synthetischer Mouseflow-Aufruf vor einer Consent-Entscheidung geführt.

TECHNISCHE BEDEUTUNG

Synthetischer Demo-Befund

OFFENE FRAGEN

Zweck, Erforderlichkeit und konkrete Verarbeitung manuell abgleichen.

TECHNISCHE BELEGE

`nicht separat aufgezeichnet`

THEMATISCHE EINORDNUNG

Das Thema betrifft die technische Wirkung einer Einwilligungsentscheidung. Eine angezeigte Schaltfläche und ein API-Aufruf sind erst bei beobachtbarer Zustandsänderung ein belastbarer Nachweis.

RECHTLICHER PRÜFKONTEXT

Kernnormen: Keine konkrete Normzuordnung im automatischen Lauf. · Mappingstatus: Keine konkrete Normzuordnung

EMPFEHLUNG

Befund im Originalsystem reproduzieren, Zweck und Rechtsgrundlage dokumentieren und die technische Umsetzung gezielt nachschärfen.

RECHTSKONTEXT

`E-LAW-012`

05 CONSENT

Consent-Prüfung

Zustandsvergleich

Tracking neu nur nach Akzeptieren	1
Tracking nach Ablehnen	0
Akzeptanz technisch bestätigt	Ja
Ablehnung technisch bestätigt	Ja

Interpretation

Consent-Diff nur zwischen tatsächlich bestätigten Zuständen belastbar.

Cookies gesamt je Zustand: vor Consent 2 · nach Ablehnen 1 · nach Akzeptieren 1. Zusätzlich nur nach Akzeptieren: 0.

Browser-Storage gesamt je Zustand: vor Consent 0 · nach Ablehnen 0 · nach Akzeptieren 0. Zusätzlich nur nach Akzeptieren: 0.

Delta je Zustand gegenüber dem frischen Ausgangszustand

Einträge werden anhand der vollständigen technischen Identität verglichen. Bei Cookies zählen Name, Domain, Pfad, Secure, HttpOnly und SameSite; Storage wird nach Speicherart und Schlüssel verglichen. Werte werden nicht ausgegeben.

BEREICH / ZUSTAND	NEU	ENTFALLEN	UNVERÄNDERT
Keine bestätigte Zustandsdifferenz aufgezeichnet.			

Getrennte Netzwerk-Skopen

CMP-Skripte und CMP-Infrastruktur, Preconnect-/DNS-Prefetch-Hinweise und echte beobachtete Tracking-Transfers werden getrennt gezählt. Ein Preconnect ist kein Transfernachweis.

ZUSTAND	TRACKING-TRANSFERS	CMP-SKRIPTE	CMP-INFRASTRUKTUR	PRECONNECT-HINWEISE	SONSTIGE REQUESTS
Keine getrennten Netzwerk-Skopen aufgezeichnet.					

Cookie- und Storage-Einordnung

Technisch notwendige, CMP-/Sicherheits- und potenziell optionale Cookies werden getrennt ausgewiesen. Die technische Katalogeinordnung ersetzt keine Prüfung von Zweck, Erforderlichkeit oder Rechtsgrundlage.

ZUSTAND	COOKIES GESAMT	TECHNISCH/CMP/SICHERHEIT	POTENZIELL OPTIONAL	UNBEKANNT	STORAGE-EINTRÄGE
Keine Cookie-/Storage-Klassifikation aufgezeichnet.					

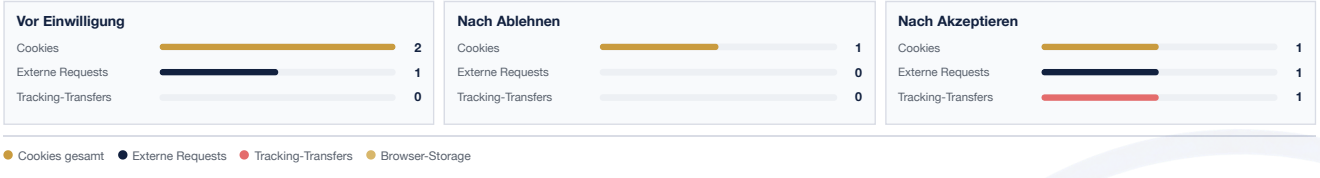
Reload-Prüfung

AKTION	RELOAD	STATUS	NACH RELOAD BESTÄTIGT	EINORDNUNG
Keine Reload-Prüfung aufgezeichnet.				

ZUSTANDSVERGLEICH

Cookies und Consent-Signale

Die Balken zeigen beobachtete Mengen je frischem Browserzustand. Sie sind keine rechtliche Bewertung; Namen, Werte und Payloads bleiben in den Tabellen und Evidence-Belegen getrennt.



ZUSTAND

Vor Einwilligung

VOR EINWILLIGUNG

2	1	2	0
Requests	externer Netzwerk-Request	Cookies	registrierte DOM-Event-Listener

Ausgangszustand vor Consent-Entscheidung.

ZUSTAND

Nach Ablehnen

NACH ABLEHNEN

1	0	1	0
Request	externe Netzwerk-Requests	Cookie	registrierte DOM-Event-Listener

Nicht angegeben Beobachtungsfenster nach Aktion: 0 Requests, davon 0 signaturbekannte Tracking-/Analyse-Requests.

ZUSTAND

Nach Akzeptieren

NACH AKZEPTIEREN

1	1	3	0
Request	externer Netzwerk-Request	Cookies	registrierte DOM-Event-Listener

Nicht angegeben Beobachtungsfenster nach Aktion: 0 Requests, davon 0 signaturbekannte Tracking-/Analyse-Requests.

Cookie-/Consent-Banner: Inhaltliche Kurzprüfung

Der sichtbare öffentliche Bannertext wird separat vom technischen Netzwerkvergleich ausgewertet. Die Markierungen sind Heuristiken; sie ersetzen keine rechtliche Prüfung von Zweck, Rechtsgrundlage oder Gestaltung.

ZUSTAND	SICHTBARER BANNERTEXT	AUTOMATISCHE INHALTSMERKMALE
Kein sichtbarer Cookie-/Consent-Bannertext aufgezeichnet.		

Consent-Verlauf und Kontextisolierung

Die Prüfung startet je Szenario in einem neuen Browser-Kontext. Aus Cookie-/Storage-Namen und sichtbarer UI wird nur der beobachtbare Vorzustand abgeleitet; Werte und serverseitige Profile werden nicht behauptet. Ein frischer Kontext ist ein Isolationsnachweis, aber kein Beweis für eine vollständig leere serverseitige Historie.

ZUSTAND	FRISCHER KONTEXT	VOR-AKTION-STATUS	BEOBACHTETE INDIKATOREN	ABLEITUNG
Kein Consent-Verlaufsnachweis im Datensatz vorhanden.				

Technische Consent-Oberfläche

Erfasst werden die beobachteten CMP-Globals, Shadow-DOM-Wurzeln und iframe-Controls. Die Spalten „Shadow Roots“ und „iframes / Controls“ zeigen Erfassungstiefe, nicht automatisch einen Rechtsverstoß.

ZUSTAND	CMP-GLOBALS	SHADOW ROOTS / DAVON GESCHLOSSEN	IFRAMES / CONTROLS	AKTIVE API
Vor Einwilligung	keine CMP-Globals	0 / 0	0 / 0	Keine aktive CMP-API bestätigt
Nach Ablehnen	keine CMP-Globals	0 / 0	0 / 0	Keine aktive CMP-API bestätigt
Nach Akzeptieren	keine CMP-Globals	0 / 0	0 / 0	Keine aktive CMP-API bestätigt

Erkannte CMP-Integrationen

SYSTEM	AKTIONSUNTERSTÜTZUNG	ERKENNUNGSMARKER
Keine CMP-Integration im geladenen Quelltext erkannt.		

Deklarative Consent- und Tracking-Signale

SYSTEM/DIENST	HOST BZW. SETTINGS-ID	TECHNISCHER STATUS
Keine deklarative Consent-Blockierung im HTML erkannt.		

Ein blockiertes Script mit dem MIME-Typ `text/plain` ist eine Einbindung, kein ausgeführter Netzwerk-Transfer. dataLayer-Werte werden auf dokumentierte, nicht-sensitive Kontextfelder begrenzt.

dataLayer-Events

EVENT	SICHERE KONTEXTWERTE
Keine dataLayer-Events aufgezeichnet.	

Tracking-Konfiguration

ZUSTAND	AUSGABESICHERE KONFIGURATION
Keine ausgabesichere Tracking-Konfiguration erkannt.	

Forensische Zusatzsignale

Diese Signale werden aus der passiven Browserbeobachtung abgeleitet. Sie sind keine automatische Feststellung eines Rechtsverstoßes und kein Nachweis einer wirksamen Einwilligung.

IAB TCF / CMP

ZUSTAND	TCF VERFÜGBAR	CMP-ID	VENDOR-EINWILLIGUNGEN	ZWECK-EINWILLIGUNGEN
Vor Einwilligung	Ja	42	1	0

GVL-Abgleich: verifiziert · Keine TCF-Erläuterung aufgezeichnet.

VENDOR-SIGNAL	ZUSTAND	BEOBACHTETER HOST	HINWEIS
Analyse-/Messdienst	Vor Einwilligung	Host nicht verifiziert (Rohwert im Evidence Package)	Signal und Host manuell prüfen.

Fingerprinting-Indizien

API	AUFRUFE
Canvas.toDataURL	1

Indizien sind keine Identifizierung.

Consent-Design-Heuristik

SIGNAL	EINORDNUNG
Ablehnen weniger prominent	Visuelle Gewichtung des Dialogs manuell prüfen.

Gestaltung, Sprache, Klicktiefe und Gesamtzusammenhang manuell prüfen.

07 DATENFLUSS

Datenschutz und Datenfluss

TECHNISCH BEOBACHTETE WEGE

Die Zahl „×“ zählt beobachtete Requests bzw. DOM-Einbindungen über alle aufgeführten Prüfzustände. Jeder Zielhost erscheint einmal; mehrere technische Kanäle werden innerhalb dieser Zeile ausgewiesen. Das ist keine Zahl der betroffenen Personen.

www.demo-report.de → **Host nicht verifiziert (Rohwert im Evidence Package)**
Unbekannt, Unbekannt (Bibliotheksabruf 1×, Tracking-Beacon 1×) · Gesamt 2× · Nach Akzeptieren; Vor Einwilligung

Verbindliche Zählskopen

METRIK	SCOPE	WERT
Tracking-/Analyse-Transfers	Alle erfassten Prüfzustände	1
Tracking-/Analyse-Transfers	Stärkster einzelner Prüfzustand	1
Signaturbekannte Tracking-Hosts	Eindeutig über alle Zustände	1
Externe Netzwerk-Hosts	Eindeutig über alle Zustände	1
Externe Netzwerk-Requests	Summe über alle Zustände	2

Transfers, Requests und eindeutige Hosts sind unterschiedliche Metriken. Wiederholungen in mehreren Consent-Zuständen werden nur in der ausdrücklich als Summe bezeichneten Scope addiert.

Formular- und Eingabeflächen

Zusammenfassung: Nicht angegeben

Die Prüfung erfasst nur sichtbare Formularmerkmale. Es wurden keine Eingaben vorgenommen, ausgelesen oder abgesendet. 'Methode' beschreibt die technische Übertragungsart, 'Zieladresse' das erkannte Formularziel und 'Position' die Stelle im HTML-Dokument.

ÜBERTRAGUNGSART	ZIELADRESSE	POSITION IM FORMULAR	FELDER UND ERLÄUTERUNG
Keine Formularmetadaten aufgezeichnet.			

Datensparsame Browser-Speicherklassifikation

Es werden keine Storage-Werte im Report ausgegeben. Die Einordnung nutzt nur Schlüsselname, Länge und eine grobe Wertform; sie ist ein technisches Signal, keine Inhalts- oder Personenbewertung.

ZUSTAND	SPEICHER	SCHLÜSSEL	DATENSPARSAME KATEGORIE	LÄNGE	WERTFORM
Keine localStorage-/sessionStorage-Schlüssel aufgezeichnet.					

Einzelne Cookie-Evidence

Die Tabelle nennt ausschließlich Namen, Domain und eine erklärbare technische Klassifikation. Cookie-Werte werden nicht ausgegeben. Zweck, Anbieter und Konfidenz sind technische Hinweise; sie ersetzen keine rechtliche Einzelfallprüfung.

ZUSTAND	NAME	DOMAIN	PFAD	SECURE	HTTPONLY	SAMESITE	TECHNISCHE EINORDNUNG	VERMUTETER ZWECK	KONFIDENZ	GRUNDLAGE
Vor Einwilligung	session	Host nicht verifiziert (Rohwert im Evidence Package)	/	Ja	Ja	Lax	Technisch erforderlich – technische Einordnung	Session-, Sicherheits- oder technische Funktionsspur; Erforderlichkeit bleibt kontextabhängig.	Niedrig	Technischer Marker im Namen; Funktion nicht verifiziert.
Vor Einwilligung	_analytics	Host nicht verifiziert (Rohwert im Evidence Package)	/	Ja	Nein	None	Zweck aus dem Namen nicht eindeutig ableitbar	Aus dem Namen allein nicht belastbar bestimmbar; manuelle Prüfung erforderlich.	Niedrig	Cookie-Name und Domain liefern keine eindeutige Zwecksignatur.
Nach Ablehnen	session	Host nicht verifiziert (Rohwert im Evidence Package)	/	Ja	Ja	Lax	Technisch erforderlich – technische Einordnung	Session-, Sicherheits- oder technische Funktionsspur; Erforderlichkeit bleibt kontextabhängig.	Niedrig	Technischer Marker im Namen; Funktion nicht verifiziert.
Nach Akzeptieren	_analytics	Host nicht verifiziert (Rohwert im Evidence Package)	/	Ja	Nein	None	Zweck aus dem Namen nicht eindeutig ableitbar	Aus dem Namen allein nicht belastbar bestimmbar; manuelle Prüfung erforderlich.	Niedrig	Cookie-Name und Domain liefern keine eindeutige Zwecksignatur.

Browser-Storage gesamt je Zustand: vor Consent 0 · nach Ablehnen 0 · nach Akzeptieren 0. Zusätzlich nur nach Akzeptieren: 0. Ein technischer Datenfluss ist noch keine abschließende Aussage über Verantwortlichkeit oder Rechtsgrundlage.

Abgleich mit Datenschutzerklärung / USA-Signal

Nur simulierte Dokumentdaten; kein echter Rechtstexte-Abgleich.

USA-Signal: Vor Einwilligung 0 Anbieter mit US-Jurisdiktionssignal, davon 0 mit Identifier-artigem Query-Signal. Keine konkrete Drittlandübermittlung automatisch bestätigt.

Quelltext-/DOM-Abgleich der Rechtstexte

Bei dynamischen Rechtstexten bleibt der sichtbare DOM-Inhalt die maßgebliche Analysesicht, sofern er nicht leer oder deutlich unvollständig ist. Der Quelltext-Fallback wird deshalb separat ausgewiesen und ist kein eigener Rechtsverstoß.

DOKUMENT	URL	FORMAT	QUELLTEXTZEICHEN	DOM-ZEICHEN	VERGLEICH	ANALYSESICHT
Datenschutz	https://www.demo-report.de/datenschutz	HTML	0	0	Nicht ermittelt	nicht ermittelt
Impressum	https://www.demo-report.de/impressum	HTML	0	0	Nicht ermittelt	nicht ermittelt

Analyse-/Messdienst

NICHT ERMITTELT

Host: Host nicht verifiziert (Rohwert im Evidence Package) · **Anbieter:** nicht aufgelöst
Ländersignal: unbekannt · **Basis:** Nicht ermittelt
Vor Einwilligung: nein · Nicht ermittelt
Request-Evidenz: Nicht ermittelt
Datenschutz-Abgleich: Anbieter nein · Zweck nein · Drittland nein · Transfermechanismus nein

Konkreter Empfänger, tatsächliches Empfängerland, Payload-Inhalt und Personenbezug sind nicht aus dem Hostnamen allein verifiziert. Request-IDs: nicht aufgezeichnet

Ergebnis des Rechtstext-Inhaltsabgleichs

Quellenabdeckung des passiven Laufs

Die Übersicht zeigt nur tatsächlich erfasste Quellen. Ein nicht erreichbarer Pfad wird nicht als vorhandene oder fehlende Rechtsgrundlage behauptet.

QUELLFAMILIE	STATUS	ERFASSTE EINTRÄGE
Robots / Sitemap	nicht bestätigt	0
Rechtstext-Varianten	nicht bestätigt	0
Karriere / Bewerbung	nicht bestätigt	0
Shop / Commerce	nicht bestätigt	0
Sprachvarianten	nicht bestätigt	0

Consent-Erkennung über mehrere Signalarten

PRÜFPUNKT	ERGEBNIS
Gesamtbewertung	nicht ermittelt
Konfidenz	nicht quantifiziert
CMP-/Provider-Signale	keine
Quelle allein	Kontakt-/Rechtstexte werden nicht als Banner gewertet

Getrennte Datenschutzerklärungen

Datenschutzerklärungen verbundener, aber rechtlich getrennt behandelter Gesellschaften werden nicht zu einer gemeinsamen Erklärung zusammengezogen. Die Hauptseite und ein Group-/Karriere-Dokument bleiben als eigene Quellen sichtbar.

QUELLE	HOST	HERKUNFT	ZEICHEN	TEXTSIGNALE
Keine getrennten Datenschutzerklärungen aufgezeichnet.				

Inhaltlicher Rechtstext-Check

PRÜFPUNKT	SIGNAL
Keine inhaltlichen Rechtstext-Signale aufgezeichnet.	

Transparenzsignale

THEMA	SIGNAL
Consent Management Platform	erkannt
Drittanbieter erwähnt	nicht erkannt

Aktualität und interne Konsistenz der Rechtsreferenzen

REFERENZ	STATUS	EINORDNUNG
Keine datierten oder auffälligen Rechtsreferenzen erkannt.		

Dokumentenstatus: Datenschutzerklärung nicht erfasst · Datenschutzhinweis nicht gefunden · AGB/Nutzungsbedingungen nicht gefunden.

Nicht verfolgte externe Rechtstext-Links

DOKUMENT	URL	GRUND
Keine externen Rechtstext-Links als nicht verfolgt aufgezeichnet.		

TCF-Signal technisch erkannt; keine Aussage über wirksame Einwilligung.

08 HÄRTUNG

Web-Sicherheit

Gesamteinstufung	HINWEIS

Passiver Web-Sicherheitscheck: Es werden nur Header, DOM-Elemente und Netzwerkvorgänge ausgewertet, die beim ohnehin ausgeführten Browseraufruf beobachtet wurden. Keine Exploit-Payloads, kein Fuzzing, kein Portscan und keine zusätzlichen Angriffstests.

Risikobezogener Kontext

HTTPS ist aktuell aktiv, aber HSTS fehlt: relevant für künftige Aufrufe und Downgrade-Schutz, nicht automatisch ein Beweis einer unsicheren aktuellen Verbindung.

KONTROLLE	STATUS	WERT	EINORDNUNG
HTTPS/TLS	OK	HTTPS	Die Zielseite war im passiven Lauf über HTTPS erreichbar.
Content-Security-Policy	FEHLT	Nicht angegeben	Keine erzwingende CSP erkannt.
Strict-Transport-Security	FEHLT	Nicht angegeben	HTTPS vorhanden, aber kein HSTS-Header erkannt.
TLS-Protokoll	INFO	nicht verfügbar	Browser lieferte keine TLS-Detailangabe.
Clickjacking-Schutz	FEHLT	Nicht angegeben	Weder frame-ancestors noch X-Frame-Options erkannt.
CSP Frame-Quellen	INFO	Nicht angegeben	Keine externen IFrames im Scan beobachtet.
X-Content-Type-Options	FEHLT	Nicht angegeben	Optionale, aber verbreitete Härtung fehlt.
Referrer-Policy	INFO	Browser-Standard	Kein Header erkannt; moderne Browser verwenden einen restriktiveren Standard. Kein automatischer Mangel.
Permissions-Policy	INFO	Nicht angegeben	Nicht zwingend erforderlich; kann Browser-Funktionen zusätzlich einschränken.
Cross-Origin-Opener-Policy	INFO	Nicht angegeben	Optionale Isolation; nicht für jede Anwendung geeignet.
Cross-Origin-Embedder-Policy	INFO	Nicht angegeben	Optionale Isolation; kann Drittanbieter-Einbindungen brechen.
Cross-Origin-Resource-Policy	INFO	Nicht angegeben	Optionale Ressourcen-Isolation.

Lesart der Header: CSP frame-ancestors und X-Frame-Options verfolgen denselben Schutzzweck, sind aber getrennte Header. Ein positiver CSP-Befund bedeutet daher nicht automatisch, dass X-Frame-Options zusätzlich gesetzt ist. Der HSTS-Wert wird als beobachteter Headerwert und zum Abrufzeitpunkt bewertet.

Security-Befunde

Keine hervorgehobenen Security-Befunde.

Zusätzliche technische Security-Signale

Die folgenden Details ergänzen die Befundkarten. Schlüsselwerte und sensible URL-Werte werden nicht ausgegeben; die Tabellen zeigen ausschließlich redigierte technische Signale.

Browser-API-Key-Signale

ANBIETER	PARAMETER	FUNDSTELLE	BEOBACHTUNG
Keine öffentlich sichtbaren Browser-API-Key-Signale aufgezeichnet.			

Auffällige URL-Parameter

ZUSTAND	URL	PARAMETERNAMEN	HEURISTISCHE KLASSE	DRITTANBIETER
Keine auffälligen URL-Parameternamen aufgezeichnet.				

Neue Fenster ohne Opener-Schutz

ELEMENT	ZIEL	REL	LINKTEXT
Keine target=_blank-Elemente ohne noopener/noreferrer aufgezeichnet.			

Secrets, Passwörter und mögliche Zugangsdaten – zeilenweise Fundstellen

Jeder Eintrag wird als eigener Befund mit Bezeichner, Script-Position und Zeile ausgegeben. Bezeichner wie **Password / Passwort**, **Passphrase**, **Secret / Geheimnis**, **Token**, **Bearer-Token**, **API-Key** oder **Privater Schlüssel** beschreiben das erkannte Feld bzw. Muster. Rohwerte werden aus Sicherheitsgründen weder gespeichert noch ausgegeben; der Wertauszug bleibt maskiert.

BEFUND-ID	BEFUND	BEZEICHNER	SCRIPT-POSITION	ZEILE	WERTAUSZUG	BEOBACHTUNGEN	ZUSTÄNDE
Keine clientseitigen Secret- oder Kontaktadressensignale aufgezeichnet.							

Kontextbewertung und Maßnahme

Öffentliche Kontaktadressen, Provider-Search-Keys, Tracking-IDs und tatsächliche Zugangsdaten werden nicht gleich behandelt. Rohwerte bleiben redigiert.

BEFUND-ID	KONTEXTKLASSE	EMPFEHLUNG
Keine kontextbezogenen Secret-Signale aufgezeichnet.		

Öffentliche Konfigurations-, Backup- und Diagnosepfade

Keine feste Exposure-Pfadprüfung aufgezeichnet.

PFAD	HTTP	ZUSTAND	MARKER	BEWERTUNG
Keine feste Exposure-Pfadprüfung aufgezeichnet.				

Source Maps (.js.map) in Production

Keine Source-Map-Prüfung aufgezeichnet. Die Prüfung erfolgt nur für tatsächlich geladene same-origin JavaScript-Dateien, begrenzt auf 30 Kandidaten und 256 KiB je Map. Empfehlung: Source Maps in Production deaktivieren oder ohne `sourcesContent` und ohne sensible Konfiguration ausliefern.

SCRIPT	SOURCE MAP	HTTP	ZUSTAND	QUELLEN	MARKER	BEWERTUNG
Keine same-origin Source-Map-Kandidaten aufgezeichnet.						

llms.txt – maschinenlesbarer Seitenhinweis

Die bekannte Datei wird nur per begrenztem GET auf dem Zielhost geprüft. Ihr Inhalt wird nicht in den Report übernommen; dokumentiert werden ausschließlich Status und technische Metadaten.

MERKMAL	BEOBACHTUNG
Status	PRESENT
URL	https://www.demo-report.de/llms.txt
HTTP-Status	200
Content-Type	text/plain
Zeilen / Zeichen	12 / 684

TLS-Verbindungsdaten

MERKMAL	BEOBACHTUNG
Protokoll	Nicht aufgezeichnet
Zertifikat / Subject	Nicht aufgezeichnet
Aussteller	Nicht aufgezeichnet
Gültig bis	Nicht aufgezeichnet

Barrierefreiheit

Gesamtstatus NICHT ANGEGEBEN

Prüfumfang: Automatisierte technische Vorprüfung auf Basis des passiven DOM-Snapshots; kein Konformitätsnachweis. · Ziel: https://www.demo-report.de/

Technische Quelle: states[*].security.dom.accessibility

Ergebnis: 0 unauffällig · 21 Hinweis(e) · 1 nicht ermittelbar · 22 Prüfpunkte.

PRÜFPUNKT	STATUS	BEOBACHTUNG	TECHNISCHE REFERENZ
Dokumentsprache	PRÜFEN	Keine html-lang-Angabe erkannt.	WCAG 3.1.1
Seitentitel	PRÜFEN	Kein aussagekräftiger Seitentitel erkannt.	WCAG 2.4.2
Überschriftenstruktur	PRÜFEN	2 Überschrift(en), h1=1, Ebenensprünge=1.	WCAG 1.3.1, WCAG 2.4.6
Alternativtexte	PRÜFEN	1 von 2 Bild-/SVG-Elementen ohne erkennbare Alternative.	WCAG 1.1.1
Link-Namen	PRÜFEN	1 von 2 Links ohne erkennbaren zugänglichen Namen.	WCAG 2.4.4
Button-Namen	PRÜFEN	1 von 2 Schaltflächen ohne erkennbaren zugänglichen Namen.	WCAG 4.1.2
Formularbeschriftungen	PRÜFEN	1 von 2 relevanten Eingabefeldern ohne explizite Beschriftung.	WCAG 1.3.1, WCAG 3.3.2
IFrame-Titel	PRÜFEN	1 von 1 IFrames ohne erkennbaren Titel.	WCAG 4.1.2
Landmarken	PRÜFEN	3 semantische Bereiche, main=0.	WCAG 1.3.1
Tastatur-/Fokusgrundlage	TECHNISCHER HINWEIS	2 Element(e) mit negativem tabindex; vollständige Tastaturführung nicht passiv verifiziert.	WCAG 2.1.1, WCAG 2.4.7
Farbkontrast	PRÜFEN	2 von 4 Kontrastprobe(n) unter dem technischen AA-Schwellenwert.	WCAG 1.4.3, WCAG 1.4.11
Eingabezweck	PRÜFEN	1 von 2 erkannten Eingabefeldern ohne autocomplete-Zweck.	WCAG 1.3.5
Eindeutige IDs	PRÜFEN	1 doppelte ID-Gruppe(n), 2 betroffene Vorkommen.	WCAG 1.3.1, WCAG 4.1.2
Sprung zum Inhalt	TECHNISCHER HINWEIS	0 Skip-Link(s) mit Ziel auf einen Seitenbereich erkannt.	WCAG 2.4.1
Tab-Reihenfolge	PRÜFEN	1 Element(e) mit positivem tabindex.	WCAG 2.4.3
ARIA-Zustände	PRÜFEN	1 von 1 erfassten interaktiven Elementen mit möglichem fehlendem Zustandsattribut.	WCAG 4.1.2
Statusmeldungen	NICHT ERMITTELBAR	0 Live-/Statusbereich(e) erkannt.	WCAG 4.1.3
Medien und Untertitel	PRÜFEN	1 Autoplay-Element(e) ohne erkennbare Stummschaltung/Kontrolle; 1 Video(s) ohne erkannte Untertitelspur.	WCAG 1.2.2, WCAG 1.2.5, WCAG 1.4.2
Dialoge und Fokus	PRÜFEN	1 von 1 Dialog(en) ohne Namen oder erkennbare fokussierbare Inhalte.	WCAG 2.1.2, WCAG 4.1.2
Zielgröße	PRÜFEN	1 von 2 sichtbaren Schaltflächen unter 24×24 CSS-Pixel.	WCAG 2.5.8
Passwort-Eingabe	PRÜFEN	1 von 1 Passwortfeldern mit erkennbarem Paste-/Input-Handler.	WCAG 3.3.8
Zoom und Reflow	PRÜFEN	width=device-width, initial-scale=1, user-scalable=no, maximum-scale=1	WCAG 1.4.4, WCAG 1.4.10

Manuelle Anschlussprüfung

Die markierten technischen Hinweise an den betroffenen Komponenten reproduzieren und nach der Korrektur erneut prüfen.
Tastaturbedienung, Fokusreihenfolge, Dialoge und dynamische Zustände mit Tastatur und assistiver Technologie prüfen.
Kontrast, Zoom/Reflow, Textabstände, Fokus bei Sticky-Headern, Hover-/Fokus-Inhalte und mobile Darstellung in allen relevanten Zuständen prüfen.
Medienuntertitel, Audiodeskription, Autoplay, Captcha-Alternativen, Drag-/Ziehbedienung und Fehlermeldungen mit realen Nutzungsszenarien prüfen.
Bestell-, Login-, Captcha- und Zahlungsstrecken einschließlich Passwortmanager, Checkout-Fehlern und Drittanbieter-Widgets separat prüfen.
Konsistente Hilfe, Navigation, Sprachwechsel, Orientierung und redundante Eingaben über mehrere Seiten und Zustände vergleichen.
Anwendbarkeit von BFSG/BITV und gegebenenfalls weitere Verpflichtungen anhand Anbieter, Dienst, Zielgruppe und Ausnahmen rechtlich bewerten.

Technische und rechtliche Referenzen

W3C – Web Content Accessibility Guidelines (WCAG) 2.2 · Technische Referenz für wahrnehmbare, bedienbare, verständliche und robuste Webinhalte.
Gesetze im Internet – Barrierefreiheitsstärkungsgesetz · Anwendbarkeit hängt insbesondere von Dienst, Anbieter, Ausnahme und Einzelfall ab.
Gesetze im Internet – BITV 2.0 · Besonders für die Zugänglichkeit informationstechnischer Angebote öffentlicher Stellen relevant.
MLBF – Marktüberwachungsstelle der Länder · Gemeinsame Marktüberwachungsstelle für BFSG-relevante Produkte und Dienstleistungen.
Abgrenzung: Die Ergebnisse sind technische Indizien. Sie bestätigen oder widerlegen weder eine vollständige WCAG-Konformität noch die Anwendbarkeit oder Erfüllung eines Gesetzes.

09 SITE COMPLIANCE

Portal und Impressum

BEWERBUNGSPORTAL-STATUS

NEIN

NEIN

Konkretes Bewerbungsziel bzw. Bewerbungsportal erkannt: Bewerbungsportal (fiktiv) · https://bewerbung.demo-report.example/portal, Fiktives Portal · https://bewerbung.demo-report.example/portal

Karriere- und Bewerbungsweg

Expliziter Karriere-/Bewerbungspfad erkannt; verlinkte Portal- und Rechtstexte werden getrennt bewertet.

TYP	LINKTEXT	ZIEL	ENTDECKT AUF	KONFIDENZ
Karriere-/Bewerbungspfad	Karriere (fiktiv)	https://www.demo-report.de/karriere	nicht angegeben	nicht angegeben
Karriere-/Bewerbungspfad	Bewerbungsportal (fiktiv)	https://bewerbung.demo-report.example/portal	nicht angegeben	nicht angegeben

Sichtbare Arbeitgeberidentität im Bewerbungsweg

PRÜFUNG	SEITE	URL	TECHNISCHE EINBINDUNG	ANBIETERHINWEIS
Keine erreichbare Bewerbungsseite für die Identitätsprüfung erfasst.				

Rechtstext-Abdeckung im Karriereweg

Mindestens ein erreichter Karriere-/Bewerbungspfad hat keine vollständige eigene Rechtstextabdeckung.

Bei einem konkreten Stellen- oder Bewerbungsziel werden Impressum und Datenschutz ausschließlich mit den direkt auf diesem Ziel erkannten Links und gelesenen Dokumenten korreliert. Nur Links im selben registrierbaren Root-Domain-Scope erfüllen die eigene Rechtstextabdeckung. Ein externer Anbieterlink, etwa zu Heroes, wird separat ausgewiesen und nicht als Arbeitgeber-Impressum gewertet. Ein Anbieterhinweis wie „Provided by …“ ist nur ein technisches Signal und kein Nachweis des rechtlichen Betreibers.

PRÜFBEREICH	STATUS	TYP	SEITENTITEL	SEITE	EIGENES IMPRESSUM	DATENSCHUTZ-LINK	EXTERNER IMPRESSUMSLINK	IMPRESSUM GELESEN	DATENSCHUTZ GELESEN	ARB IM QU
Karriere-/Portalseite	nicht gefunden	CAREER_PAGE	Fiktives Portal	https://bewerbung.demo-report.example/portal	nein	nein	nein	nein	nein	nic

Microsoft Bookings – gezielter Folgelauf

Explizit verlinkte Microsoft-Bookings-Ziele werden separat nachgeladen. Sie zählen weder als Bewerbungsportal noch automatisch als aktiver Tracking-Transfer. Rechtstexte des Zielsystems werden nur als eigene technische Quelle ausgewiesen.

VERLINKTES ZIEL	WEITERGELEITETE URL	HTTP	SEITENTITEL	TEXTZEICHEN	RECHTSLINKS	ERGEBNIS
Kein explizites Microsoft-Bookings-Ziel erkannt oder erreichbar.						

Domain-Abgleich: Zielhost nicht angegeben · Root-Domain-Scope nicht bestimmt · Root-Domain bzw. kein Subdomain-Zusatz.

Externe Bewerbungs-Hosts werden als eigene technische Betreiber-/Dienstleisterquelle ausgewiesen und nicht automatisch der Hauptdomain zugerechnet.

Interne Seitenabdeckung

0 interne HTML-Seite(n) geprüft; Limit 25, fehlgeschlagen: 0. Der Crawl folgt ausschließlich demselben autorisierten Host und ersetzt keine vollständige Webarchivierung.

URL	HTTP	TEXTZEICHEN	INTERNE LINKS	RECHTSLINKS	ERGEBNIS
Keine intern verlinkten HTML-Seiten erfasst.					

Eingebettete Bewerberportale

HOST	HTTPS	SENSIBLE FORMULARE	EIGENE RECHTSQUELLEN IM IFRAME	DIREKTER GET-AUFRUF	HAUPT-DATENSCHUTZ / VERWEIS	ENTDECKT AUF	EINORDNUNG
Kein externes IFrame-Portal erkannt.							

Prüfhinweise

IMP-002 · Anbieterkennzeichnung nicht eindeutig zuordenbar

HINWEIS

Hoststruktur des Impressums weicht ab.

Kernnormen: § 5 DDG · Ergänzend: § 33 DDG · Mappingstatus: Manuelle Prüfung

Eingebettete Dienste

HOST	KATEGORIE	AKTIVITÄT	HTTPS	SENSIBLE FORMULARE	DATENSCHUTZTEXT / VERWEIS
Keine externen Dienste automatisch eindeutig klassifiziert.					

„Externer Datenschutzverweis“ bedeutet: Der Host selbst wurde nicht mit einem eigenen Rechtstext-Link erkannt, die Seite verweist aber auf eine Datenschutzquelle eines anderen Hosts. Das ist nicht dasselbe wie ein fehlender Datenschutztext.

Aktivität bedeutet hier: Ein aktiver Tracking-/Analyse-Transfer wurde im Netzwerk beobachtet. Ein geladener Dienst, eine Consent-Komponente oder ein blockiertes Script ist dadurch nicht automatisch ein aktiver Tracking-Empfänger.

Zahlungsdienste und Bezahlstrecken

Hinweis: Zahlungsdienste werden im passiven Lauf nur anhand beobachteter externer Hosts oder IFrames technisch eingeordnet. Wenn im passiven Lauf kein Zahlungsdienst beobachtet wurde, bedeutet das nur „nicht beobachtet“ und nicht „nicht vorhanden“. Ein abgeschlossener Zahlungsvorgang und konkrete Zahlungs-Payloads werden nicht geprüft.

Weitere öffentliche Transparenz- und Technologieindizien

Native Erkennung (Primärquelle): CMS-, Framework- und Bibliotheksklassifikation stammt aus den eigenen passiven Treelogy-Regeln. Diese Ergebnisse bleiben für die technische Klassifikation maßgeblich. Wappalyzer-Ergänzung (Kandidaten): Magento 2.4.x, PayPal. Diese Shadow-Treffer werden separat gespeichert, nicht automatisch in die native Klassifikation übernommen und erst nach manueller Gegenprüfung als mögliche Ergänzung bewertet. Frontend-Indizien: Alpine.js (Hoch). CMS-Indizien: Magento (Mittel). Frontend-Bibliotheken: jQuery (1.11.2 · Wartungsprüfung erforderlich). Ein Bibliotheksfund ist ein technischer Hinweis und kein automatischer Sicherheitsverstoß.

Globale Quellsignale · global-signals-8.7-1

Diese versionierte, seitenunabhängige Inventur wird auf jede geprüfte Seite angewendet. Sie beschreibt nur passive Quelltext-Indizien; sie beweist weder einen Netzwerktransfer, ein Secret noch einen Rechtsverstoß.

CODE	FAMILIE	SIGNAL	KONFIDENZ	ANZAHL	TECHNISCHE EINORDNUNG
HTML_FORM_SURFACE	forms	Formularoberfläche	Mittel	1	Synthetisches Demo-Signal: HTML-Formulare im Quelltext.
SENSITIVE_FORM_CONTROL_SURFACE	forms	Sensible Formularfelder	Mittel	1	Synthetisches Demo-Signal: Passwort-, E-Mail-, Datei- oder Autocomplete-Feld.
CLIENT_STORAGE_SURFACE	storage	Clientseitiger Speicherzugriff	Mittel	1	Synthetisches Demo-Signal: localStorage-, sessionStorage-, Cookie- oder IndexedDB-Marker.
EMBEDDED_CONTENT_SURFACE	embedding	Eingebettete Inhalte	Mittel	1	Synthetisches Demo-Signal: iframe-, embed- oder object-Elemente.
STRUCTURED_DATA_SURFACE	metadata	Strukturierte Daten	Hoch	1	Synthetisches Demo-Signal: JSON-LD-Block.
EXTERNAL_SCRIPT_SURFACE	resources	Externe Script-Ressourcen	Mittel	1	Synthetisches Demo-Signal: absolute Script-Quelle.
API_ENDPOINT_SURFACE	requests	API-/Request-Oberfläche	Mittel	1	Synthetisches Demo-Signal: Fetch-, XHR-, API- oder GraphQL-Marker.

Beobachtete externe Verbindungen/Hosts (1; 1 Konzern-/Betreibergruppen; nicht alle sind datenschutzrechtliche Empfänger): Host nicht verifiziert (Rohwert im Evidence Package)

Hostsignal nicht abschließend verifiziert; für die Einordnung wurde der Host der beobachteten URL bevorzugt: Host nicht verifiziert (Rohwert im Evidence Package)

Betreibergruppen-Aufschlüsselung: analytics.demo-report.example: Host nicht verifiziert (Rohwert im Evidence Package)

Analyse-/Messdienst (1): Host nicht verifiziert (Rohwert im Evidence Package)

1 relevanter Tracking-/Analyse-Transfer gegenüber 1 beobachtetem externen Host; Zählung aus dem repräsentativen Einzelzustand, Hosts aus dem Site-Compliance-Modul.

Noch nicht eindeutig klassifizierte externe Hosts: Host nicht verifiziert (Rohwert im Evidence Package)

10 RECHTSCHECK

Rechtskontext

Automatischer Rechtscheck HINWEIS **Priorität 100 / 100**

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Keine Rechtsberatung und keine echte Behördenbewertung.

Verifikationsstatus: DEMO_SIMULIERT. Die technische Befundstufe bleibt Hinweis; lediglich die aktuelle Live-Rechtsquelle konnte nicht vollständig verifiziert werden.

Ampel: Sehr hoch · **Begründung:** Hoher Prüfbedarf; 5 relevante Grundbefunde; 4 Risikofamilien; Familienkorrelation berücksichtigt; Unabhängigkeitsbonus +4 für 3 fachlich getrennte Gruppen; Manueller Prüfbedarf; Unsicherheit nicht als Risikobonus gewertet

DEMO-SYN-001 · Abweichende Verantwortlichenadresse

ERHÖHT

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-002 · Cookie- und Consent-Verstoß simuliert

HOCH

Thema: Das Thema betrifft Zugriffe auf Informationen im Endgerät. Zweck, Erforderlichkeit, Lebensdauer und Einwilligungsabhängigkeit müssen je Eintrag im konkreten Kontext geprüft werden.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-003 · Unbestätigtes Secret-Signal simuliert

HINWEIS

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Art. 32 DSGVO · Ergänzend: Art. 5 DSGVO; Art. 25 DSGVO; Art. 33/34 DSGVO (nur bei bestätigter Verletzung) · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-015 · Passwort in ausgeliefertem JavaScript simuliert

KRITISCH

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Art. 32 DSGVO · Ergänzend: Art. 5 DSGVO; Art. 25 DSGVO; Art. 33/34 DSGVO (nur bei bestätigter Verletzung) · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-016 · Secret in öffentlicher JSON-Datei simuliert

HOCH

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Art. 32 DSGVO · Ergänzend: Art. 5 DSGVO; Art. 25 DSGVO; Art. 33/34 DSGVO (nur bei bestätigter Verletzung) · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-017 · Öffentliche Kontaktadresse in ausgelieferter Datei simuliert

HINWEIS

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Art. 32 DSGVO · Ergänzend: Art. 5 DSGVO; Art. 25 DSGVO; Art. 33/34 DSGVO (nur bei bestätigter Verletzung) · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-013 · Kritischer Sicherheitszustand simuliert

KRITISCH

Thema: Das Thema betrifft die technische Absicherung der Auslieferung. Ein einzelner Header ist nur im Zusammenspiel mit HTTPS, Ressourcenpfaden, Browserverhalten und Serverkonfiguration zu bewerten.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-014 · Befund nicht automatisch bewertet

NICHT BEWERTET

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-005 · Tracking vor Einwilligung an US-Signal simuliert

HOCH

Thema: Das Thema betrifft beobachtete Analyse- oder Identifikatorsignale. Hostname und Parametername belegen einen technischen Datenfluss, aber allein weder Personenbezug noch zulässige Rechtsgrundlage.

Rechtskontext: Kernnormen: Art. 12 DSGVO; Art. 13 DSGVO · Ergänzend: Art. 28 DSGVO; Art. 44 ff. DSGVO · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-006 · Veraltete beziehungsweise kritische jQuery-Version simuliert

ERHÖHT

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-007 · Widersprüchliche Rechtspassage simuliert

ERHÖHT

Thema: Das Thema betrifft die technische Wirkung einer Einwilligungsentscheidung. Eine angezeigte Schaltfläche und ein API-Aufruf sind erst bei beobachtbarer Zustandsänderung ein belastbarer Nachweis.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-008 · Mouseflow im Bewerberbereich simuliert

ERHÖHT

Thema: Das Thema betrifft die technische Wirkung einer Einwilligungsentscheidung. Eine angezeigte Schaltfläche und ein API-Aufruf sind erst bei beobachtbarer Zustandsänderung ein belastbarer Nachweis.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-009 · Content-Security-Policy fehlt simuliert

NIEDRIG

Thema: Das Thema betrifft die technische Absicherung der Auslieferung. Ein einzelner Header ist nur im Zusammenspiel mit HTTPS, Ressourcenpfaden, Browserverhalten und Serverkonfiguration zu bewerten.

Rechtskontext: Kernnormen: Art. 32 DSGVO · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-010 · HSTS fehlt simuliert

NIEDRIG

Thema: Das Thema betrifft die technische Absicherung der Auslieferung. Ein einzelner Header ist nur im Zusammenspiel mit HTTPS, Ressourcenpfaden, Browserverhalten und Serverkonfiguration zu bewerten.

Rechtskontext: Kernnormen: Art. 32 DSGVO · Mappingstatus: Manuelle Prüfung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-011 · Externe Links ohne sichere Fensterbeziehung simuliert

HINWEIS

Thema: Das Thema betrifft eine externe Einbindung oder einen externen Empfänger. Die technische Zieladresse ist nicht automatisch mit der rechtlichen Betreiber- oder Empfängerrolle gleichzusetzen.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

DEMO-SYN-012 · Tastatur- und Beschriftungslücke simuliert

HINWEIS

Thema: Das Thema beschreibt ein technisches Signal aus dem beobachteten Prüfpfad. Für eine belastbare Bewertung sind Originalquelle, Zweck, konkrete Verarbeitung, Abdeckung und – soweit erforderlich – die zuständige Fachstelle gemeinsam zu prüfen.

Rechtskontext: Kernnormen: Keine konkrete Normzuordnung · Mappingstatus: Keine konkrete Normzuordnung

Offener Prüfschritt: Technischen Befund im Original und im konkreten Verarbeitungskontext prüfen.

Die vollständige technische Feststellung steht einmalig unter „Hauptbefunde“; diese Karte ist nur der rechtliche Querverweis.

Quellen und Status

QUELLE	STATUS	ABRUF	FASSUNG	OFFIZIELLE URL
BDSG	Status nicht angegeben	nicht angegeben	nicht angegeben	https://www.gesetze-im-internet.de/bdsg_2018/

11 FOLGEN

Mögliche Rechtsfolgen

Die Darstellung trennt behördliche/gesetzliche Folgen von privatem Schadensersatz. Sie enthält keine Prognose eines persönlichen Geldbetrags und ersetzt keine Rechtsberatung. Ein fixer Geldbetrag ist aus einem technischen Scan nicht ableitbar; mögliche Ansprüche und Maßnahmen hängen vom Einzelfall ab.

Cookie- und Consent-Verstoß simuliert

PRÜFUNG OFFEN

GESETZLICHE / BEHÖRDLICHE FOLGE
Aktuelle Rechtsfolge nicht verifiziert
Kernnormen: nicht angegeben · Ergänzend: keine

PRIVATER SCHADENSERSATZ
Aktuelle Rechtsfolge nicht verifiziert

Nicht abschließend; manuelle rechtliche Prüfung erforderlich.

Tracking vor Einwilligung an US-Signal simuliert

PRÜFUNG OFFEN

GESETZLICHE / BEHÖRDLICHE FOLGE
Aktuelle Rechtsfolge nicht verifiziert
Kernnormen: Art. 12 DSGVO; Art. 13 DSGVO · Ergänzend: Art. 28 DSGVO; Art. 44 ff. DSGVO

PRIVATER SCHADENSERSATZ
Aktuelle Rechtsfolge nicht verifiziert

Nicht abschließend; manuelle rechtliche Prüfung erforderlich.

Widersprüchliche Rechtspassage simuliert

PRÜFUNG OFFEN

GESETZLICHE / BEHÖRDLICHE FOLGE
Aktuelle Rechtsfolge nicht verifiziert
Kernnormen: nicht angegeben · Ergänzend: keine

PRIVATER SCHADENSERSATZ
Aktuelle Rechtsfolge nicht verifiziert

Nicht abschließend; manuelle rechtliche Prüfung erforderlich.

Mouseflow im Bewerberbereich simuliert

PRÜFUNG OFFEN

GESETZLICHE / BEHÖRDLICHE FOLGE
Aktuelle Rechtsfolge nicht verifiziert
Kernnormen: nicht angegeben · Ergänzend: keine

PRIVATER SCHADENSERSATZ
Aktuelle Rechtsfolge nicht verifiziert

Nicht abschließend; manuelle rechtliche Prüfung erforderlich.

Vorgehen bei bestätigtem Verstoß oder ernsthaftem Verdacht: Befund und Evidence sichern, die betroffene Verarbeitung vorläufig bewerten, Ursache und Reichweite klären, Abhilfe dokumentieren und Verantwortliche bzw. Datenschutzbeauftragte einbeziehen. Eine Meldung an Fiktive Datenschutzaufsicht Niedersachsen – Demo ist nicht allein aufgrund eines automatischen Hinweises geschuldet; sie ist nach Sachverhalt und Rolle zu prüfen. Bei einer möglichen Verletzung des Schutzes personenbezogener Daten sind insbesondere die Melde- und Dokumentationspflichten nach Art. 33 und 34 DSGVO sowie interne Fristen zu bewerten. Der Bericht ersetzt diese Einzelfallprüfung nicht.

Fiktive Datenschutzaufsicht Niedersachsen – Demo

Anschrift: Behördenweg 1, 38350 Helmstedt (fiktiv)
E-Mail: aufsicht-niedersachsen@example.invalid
Offizielle Website: https://aufsicht-niedersachsen.example.invalid/

Bei möglicher Datenverletzung: Sachverhalt und Evidence sichern, Verantwortliche und Datenschutzbeauftragte einbeziehen und die Melde- und Informationspflichten nach Art. 33 und 34 DSGVO einschließlich der 72-Stunden-Frist fallbezogen prüfen und dokumentieren.

11A

UMSETZUNG

Technische Empfehlungen für Seitenbetreiber

PRIORISIERTE TO-DO-LISTE

AKTIV

Die Handlungshinweise leiten sich aus den aufgezeichneten technischen Befunden ab. Sie sind Umsetzungshinweise für Seitenbetreiber und keine abschließende Rechtsbewertung.

Reihenfolge: Hoch vor Erhöht vor Hinweis · **Empfehlungen nach Priorität:** Kritisch: 1 · Hoch: 1 · Erhöht: 2 · Hinweis: 2

Die Hinweise sind technische Umsetzungsvorschläge und keine abschließende Rechtsbewertung.

Passwort- und Zugangsdatenkontrolle bei kritischem Befund

KRITISCH

Sofortmaßnahme: Kritischen Passwortbefund sofort absichern und die betroffenen Zugänge kontrollieren.

Dauerhafte Umsetzung: Passwort-/Credential-Inventar, Session-Invalidierung, MFA, Rotation und Alarmprüfung nachvollziehbar durchführen.

Zuständige Rolle: Anwendungsbetrieb, Informationssicherheit und Account-Verantwortliche

Nachtest: Nach Rotation: alter Wert abgewiesen, aktive Sessions geprüft, Logs ausgewertet und neuer Scan ohne Klartextwert dokumentiert.

Technischer Kontext: Bei einem kritischen Passwort- oder Zugangsdatenbefund sofort prüfen, ob der Wert produktiv verwendbar ist. Betroffene Konten, Sessions, API-Zugänge und Testzugänge sperren oder rotieren, MFA und Nutzungsprotokolle kontrollieren und den Nachtest ohne Klartextwerte dokumentieren.

Ableitung: Mindestens ein kritischer Passwort-/Credential-Befund erfordert eine sofortige Zugangskontrolle und einen dokumentierten Nachtest.

Auslöser: Passwort in ausgeliefertem JavaScript simuliert · **Evidence:** DEMO-SYN-015; E-LAW-004

Clientseitiges Secret verifizieren und danach absichern

HOCH

Sofortmaßnahme: Fundstelle und Credential-Bedeutung verifizieren; bei Bestätigung betroffene Zugangsdaten unmittelbar widerrufen/rotieren und Nutzungs- sowie Authentisierungslogs prüfen.

Dauerhafte Umsetzung: Secrets serverseitig verwalten, Proxy mit Minimalrechten und dokumentierte Rotation einsetzen.

Zuständige Rolle: Anwendungsbetrieb, Informationssicherheit und API-Verantwortliche

Nachtest: Quelltext-, Bundle- und HAR-Nachtest ohne Klartext-Secret; alte Credentials müssen scheitern.

Technischer Kontext: Zuerst die exakte Fundstelle, den Werttyp, die Gültigkeit und die Berechtigungen fachlich und technisch verifizieren. Bestätigt sich ein produktives Passwort, Bearer-/Basic-Auth-Datum, privater Schlüssel oder nicht öffentlich bestimmtes Token, ist es unmittelbar zu widerrufen oder zu rotieren und die Nutzungslogs sind zu prüfen. Künftige privilegierte Aufrufe über einen serverseitigen Proxy mit minimalen, kurzlebigen Berechtigungen ausführen; die konkrete Fundstelle nicht erneut als Klartext in einen Bericht oder ein Beweispaket übernehmen.

Ableitung: Ein clientseitig erreichbarer Zugangsdaten- oder Secret-Hinweis wurde im Quelltext-/Bundle-Befund erfasst.

Auslöser: Passwort in ausgeliefertem JavaScript simuliert · **Evidence:** DEMO-SYN-015; E-LAW-004

Browser-Speicher vor Consent klassifizieren und minimieren

ERHÖHT

Sofortmaßnahme: Nicht erforderliche Cookies und Storage-Einträge vor Einwilligung unterbinden.

Dauerhafte Umsetzung: Inventar mit Zweck, Lebensdauer, Kategorie und Löschverhalten pflegen.

Zuständige Rolle: Frontend-/CMP-Verantwortliche und Datenschutzkoordination

Nachtest: Automatisierter Diff in leerem Kontext nach Laden, Ablehnen, Akzeptieren und Reload.

Technischer Kontext: Jeden Cookie- und Storage-Eintrag Zweck, Erforderlichkeit, Lebensdauer und Consent-Kategorie zuordnen. Nicht erforderliche Einträge erst nach Einwilligung setzen und den Ausgangszustand regelmäßig mit einem leeren Browserkontext prüfen.

Ableitung: Im Ausgangskontext wurden 2 Cookies-/Storage-Indikatoren aufgezeichnet; Zweck und Erforderlichkeit müssen je Eintrag geprüft werden.

Auslöser: Vor Einwilligung; 2 Speicherindikator(en) · **Evidence:** nicht separat zugeordnet

Fehlende oder schwache Security-Header gezielt härten

ERHÖHT

Sofortmaßnahme: Fehlende Header am tatsächlichen HTTPS-Endpunkt bestätigen und Basisschutz ergänzen.

Dauerhafte Umsetzung: CSP schrittweise mit Nonces/Hashes aufbauen; HSTS, MIME-, Referrer-, Frame- und Permissions-Schutz setzen.

Zuständige Rolle: Server-/DevOps-Verantwortliche und Webentwicklung

Nachtest: Response-Header, Redirects, Assets, Browserkonsole und CSP-Reports nach Rollout kontrollieren.

Technischer Kontext: HSTS, Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy und Clickjacking-Schutz anhand des konkreten Deployment-Modells prüfen. Eine CSP schrittweise im Report-Only-Modus einführen, danach Ausnahmen reduzieren und erst anschließend erzwingen.

Ableitung: Mindestens ein Security-Header wurde als fehlend, schwach oder nicht nachgewiesen erfasst.

Auslöser: Content-Security-Policy fehlt simuliert; HSTS fehlt simuliert · **Evidence:** DEMO-SYN-009; E-LAW-013; DEMO-SYN-010; E-LAW-014

Beobachtbares Secret manuell verifizieren

HINWEIS

Sofortmaßnahme: Das beobachtete Signal vor einer Rotation fachlich und technisch verifizieren.

Dauerhafte Umsetzung: Fundstelle, Kontext, Provider, Berechtigungen und Wertform getrennt bewerten; öffentliche Konfiguration von echten Credentials unterscheiden.

Zuständige Rolle: Webentwicklung, API-Verantwortliche und Informationssicherheit

Nachtest: Exakte Script-/DOM-Fundstelle reproduzieren, Rohwert nicht speichern und Einstufung mit Belegverweis dokumentieren.

Technischer Kontext: Das beobachtete Secret-Signal zunächst an der exakten Fundstelle prüfen: Feldname, Werttyp, Script-Eigentümer, Berechtigungen, Gültigkeit und Providerkontext abgleichen. Öffentliche Client-Keys, UI-Texte, Selektoren und Parserfragmente nicht als Passwort behandeln; Rohwerte bleiben redigiert.

Ableitung: Ein Secret-Signal ist beobachtbar, aber seine tatsächliche Credential-Bedeutung muss an der Fundstelle getrennt verifiziert werden.

Auslöser: Passwort in ausgeliefertem JavaScript simuliert · **Evidence:** DEMO-SYN-015; E-LAW-004

Öffentliche Kontaktadresse in Quelltext und Dateien einordnen

HINWEIS

Sofortmaßnahme: Die Kontaktadresse redigiert erfassen und ihre beabsichtigte öffentliche Veröffentlichung bestätigen.

Dauerhafte Umsetzung: Kontaktadressen von Zugangsdaten trennen; unbeabsichtigte Kopien in Bundles, JSON und Dateien entfernen.

Zuständige Rolle: Web-/Kommunikationsverantwortliche und Datenschutzkoordination

Nachtest: Quelltext, statische Dateien und öffentliche Downloadpfade nach der Änderung erneut durchsuchen.

Technischer Kontext: Eine ausgelieferte Kontakt-E-Mail redigiert dokumentieren und prüfen, ob ihre Veröffentlichung in HTML, JavaScript, JSON oder Dateien beabsichtigt ist. Sie ist nicht automatisch ein Passwort oder Secret; bei unbeabsichtigter Veröffentlichung entfernen oder ersetzen und anschließend den öffentlichen Pfad erneut prüfen.

Ableitung: Eine Kontaktadresse wurde in einem öffentlich ausgelieferten Quelltext-/Dateipfad dokumentiert und muss von Zugangsdaten getrennt eingeordnet werden.

Auslöser: Öffentliche Kontaktadresse in ausgelieferter Datei simuliert · **Evidence:** DEMO-SYN-017; E-LAW-006

09 INTEGRITÄT

Evidence und Integrität

Evidence Package

Package-ID	EP-demo-2026101
Session-ID	demo-20261011-helmstedt
Manifest-Fingerprint	`730c7caa7a1b952b81a847948ee730d38f93d716cef9285da50f889f6d08aa93`
Qualifizierter Zeitstempel	Nicht angehängt

Integritätsnotiz

Die Hashes machen nachträgliche Änderungen an den aufgeführten Dateien erkennbar, solange der ursprüngliche Manifest-Fingerprint separat aufbewahrt wird. Ein qualifizierter eIDAS-Zeitstempel wurde in diesem Lauf nicht angehängt. Das Manifest ist daher keine elektronische Signatur und keine Garantie gerichtlicher Beweiswürdigung.

Nicht angehängt: In diesem Lauf wurde kein qualifizierter elektronischer Zeitstempel angehängt. Ein qualifizierter eIDAS-Zeitstempel wurde in diesem Lauf nicht angehängt. Ein externer RFC-3161-TSA-Nachweis muss separat beschafft, verifiziert und als Token im Evidence Package abgelegt werden.
Automatische Fallablage: Vollständig/kompakt: Vollständig, Kompakt und Vorschau · im Fallordner
ZIP-Beweispaket: ZIP-Beweispaket · im Fallordner (im Fallordner)

Validierung der Report-Artefakte

Status: nicht aufgezeichnet · Existenz, Lesbarkeit und PDF-Signatur wurden je Profil geprüft.

PROFIL	STATUS	GRÖSSE	SEITEN
Vollbericht	nicht geprüft	0 Bytes	–
Kompaktbericht	nicht geprüft	0 Bytes	–
Vorschau	nicht geprüft	0 Bytes	–
Maßnahmenkatalog	nicht geprüft	0 Bytes	–

Validierung der visuellen Evidence

PRÜFUNG	ERGEBNIS
Gültige visuelle Belege	0
Doppelte Dateien	0
Nicht nutzbare Dateien	0
Evidence-IDs vollständig	Nein / nicht aufgezeichnet
Nicht zugeordnete Pfade	0

identical bytes represented once by kind and SHA-256

ID	TYP	ZUSTAND	REFERENZ	SHA-256
E-HAR-001	HAR	Vor Einwilligung	evidence/01_vor_einwilligung.har	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
E-HAR-002	HAR	Nach Ablehnen	evidence/02_nach_ablehnen.har	bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
E-HAR-003	HAR	Nach Akzeptieren	evidence/03_nach_akzeptieren.har	ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
E-LAW-001	Strukturierter Report-Nachweis	DEMO-SYN-001	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-002	Strukturierter Report-Nachweis	DEMO-SYN-002	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-STORAGE-001	Strukturierter Report-Nachweis	DEMO-SYN-002	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-003	Strukturierter Report-Nachweis	DEMO-SYN-003	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-004	Strukturierter Report-Nachweis	DEMO-SYN-015	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-005	Strukturierter Report-Nachweis	DEMO-SYN-016	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-006	Strukturierter Report-Nachweis	DEMO-SYN-017	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-007	Strukturierter Report-Nachweis	DEMO-SYN-013	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt

ID	TYP	ZUSTAND	REFERENZ	SHA-256
E-LAW-008	Strukturierter Report-Nachweis	DEMO-SYN-014	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-009	Strukturierter Report-Nachweis	DEMO-SYN-005	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-NET-001	Strukturierter Report-Nachweis	DEMO-SYN-005	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-010	Strukturierter Report-Nachweis	DEMO-SYN-006	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-011	Strukturierter Report-Nachweis	DEMO-SYN-007	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-012	Strukturierter Report-Nachweis	DEMO-SYN-008	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-013	Strukturierter Report-Nachweis	DEMO-SYN-009	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-014	Strukturierter Report-Nachweis	DEMO-SYN-010	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-015	Strukturierter Report-Nachweis	DEMO-SYN-011	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-NET-002	Strukturierter Report-Nachweis	DEMO-SYN-011	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-LAW-016	Strukturierter Report-Nachweis	DEMO-SYN-012	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-OBS-001	Strukturierter Report-Nachweis	PA-F-0001	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-DOM-001	Strukturierter Report-Nachweis	IMP-002	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-OBS-002	Strukturierter Report-Nachweis	PA-F-0002	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-OBS-003	Strukturierter Report-Nachweis	PA-F-0003	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-OBS-004	Strukturierter Report-Nachweis	PA-F-0017	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-OBS-005	Strukturierter Report-Nachweis	PA-F-0004	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-OBS-006	Strukturierter Report-Nachweis	PA-F-0005	Report-JSON	nicht anwendbar – kein eigenes Dateiartefakt
E-MANIFEST	Manifest	Gesamtpaket	evidence/evidence_manifest.json	730c7caa7a1b952b81a847948ee730d38f93d716cef9285da50f889f6d08aa93

13 VERGLEICHSRAHMEN

Vergleichsrechtsprechung

DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung.

Nicht angegeben · Nicht angegeben

Nicht angegeben

Kernaussage: Nicht angegeben

Warum vergleichbar: Nicht angegeben

Grenze: Nicht angegeben

Gericht: nicht angegeben · **Aktenzeichen:** nicht angegeben · **Entscheidungsdatum:** nicht angegeben · **ECLI:** nicht angegeben · **Offizielle Quelle:** Nicht angegeben · **Verifikationsstatus:** Nicht verifiziert
Offizielle URL: nicht angegeben · Quelle im automatischen Lauf nicht verifiziert.

Nicht angegeben · Nicht angegeben

Nicht angegeben

Kernaussage: Nicht angegeben

Warum vergleichbar: Nicht angegeben

Grenze: Nicht angegeben

Gericht: nicht angegeben · **Aktenzeichen:** nicht angegeben · **Entscheidungsdatum:** nicht angegeben · **ECLI:** nicht angegeben · **Offizielle Quelle:** Nicht angegeben · **Verifikationsstatus:** Nicht verifiziert
Offizielle URL: nicht angegeben · Quelle im automatischen Lauf nicht verifiziert.

Nicht angegeben · Nicht angegeben

Nicht angegeben

Kernaussage: Nicht angegeben

Warum vergleichbar: Nicht angegeben

Grenze: Nicht angegeben

Gericht: nicht angegeben · **Aktenzeichen:** nicht angegeben · **Entscheidungsdatum:** nicht angegeben · **ECLI:** nicht angegeben · **Offizielle Quelle:** Nicht angegeben · **Verifikationsstatus:** Nicht verifiziert
Offizielle URL: nicht angegeben · Quelle im automatischen Lauf nicht verifiziert.

14 ANHANG

Technischer Anhang

Vollständiger Befundindex und kompakte Zustandszusammenfassung. Evidence wird nach Primär-, Unterstützungs-, Kontext- und Rechtsrolle getrennt ausgewiesen. Der Rohzeitstrahl bleibt im HTML-Technikanhang sowie im Evidence Package und wird nicht in die Standard-PDF gedruckt.

Vollständiger Befundindex

ID	STATUS UND QUELLE	TITEL / FESTSTELLUNG	BELEGROLLEN
DEMO-SYN-001	Erhöht · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Abweichende Verantwortlichenadresse** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Im fiktiven Anbietertext steht Demoweg 7, 38350 Helmstedt; der ebenfalls fiktive Policy-Text nennt Demoallee 12, 30159 Hannover.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-001
DEMO-SYN-002	Hoch · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Cookie- und Consent-Verstoß simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Vor einer Entscheidung wird im synthetischen Lauf ein Marketing-Cookie gesetzt; Ablehnen und Akzeptieren sind als getrennte Zustände dokumentiert.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-002
DEMO-SYN-003	Hinweis · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Unbestätigtes Secret-Signal simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Die Demo zeigt ausschließlich ein redigiertes, synthetisches Signal. Feldname, Werttyp, Script-Eigentümer und Providerkontext reichen nicht für die Einstufung als Passwort oder Secret; es wird kein Credential gespeichert.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-003
DEMO-SYN-015	Kritisch · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Passwort in ausgeliefertem JavaScript simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. In einem fiktiven JavaScript-Bundle wird ein redigierter Passwortwert mit der synthetischen Fundstelle `assets/app.demo.js:42` markiert. Es wird kein Rohwert gespeichert.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-004
DEMO-SYN-016	Hoch · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Secret in öffentlicher JSON-Datei simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Eine fiktive `config.demo.json` enthält ein redigiertes, nicht öffentlich gedachtes Secret-Signal. Die Demo speichert weder Rohwert noch nutzbares Credential.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-005
DEMO-SYN-017	Hinweis · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Öffentliche Kontaktadresse in ausgelieferter Datei simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Eine fiktive Kontakt-E-Mail ist redigiert in `assets/contact.demo.js` sichtbar. Das Signal ist ausdrücklich kein Passwort und kein Secret.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-006
DEMO-SYN-013	Kritisch · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Kritischer Sicherheitszustand simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Die Demo stellt absichtlich einen kritischen technischen Zustand dar, bei dem eine zentrale Schutzkontrolle als unwirksam markiert ist. Es handelt sich um eine synthetische Ausprägung ohne reale Zielseite, Verbindung oder ausnutzbares System.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-007
DEMO-SYN-014	Nicht bewertet · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Befund nicht automatisch bewertet** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Für dieses synthetische Teilmodul fehlen belastbare Vergleichsdaten. Eine automatische Einstufung wäre nicht nachvollziehbar.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-008
DEMO-SYN-005	Hoch · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Tracking vor Einwilligung an US-Signal simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Vor Einwilligung wird ein synthetischer Request an `analytics-us.demo-report.example` mit US-Anbieter-Signal dokumentiert.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-009
DEMO-SYN-006	Erhöht · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Veraltete beziehungsweise kritische jQuery-Version simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Das Demo-Frontend lädt synthetisch jQuery 1.11.2 und markiert die Version als veraltet.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-010
DEMO-SYN-007	Erhöht · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Widersprüchliche Rechtspassage simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Der fiktive Policy-Text nennt für denselben Dienst gleichzeitig Einwilligung und berechtigtes Interesse als alleinige Grundlage.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-011
DEMO-SYN-008	Erhöht · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Mouseflow im Bewerberbereich simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Auf dem fiktiven Karriere- und Bewerberpfad wird ein synthetischer Mouseflow-Aufruf vor einer Consent-Entscheidung geführt.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-012
DEMO-SYN-009	Niedrig · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Content-Security-Policy fehlt simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Die synthetische Header-Kontrolle enthält keine aktive CSP.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-013
DEMO-SYN-010	Niedrig · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**HSTS fehlt simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Die synthetische HTTPS-Antwort enthält keinen Strict-Transport-Security-Header.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-014
DEMO-SYN-011	Hinweis · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Externe Links ohne sichere Fensterbeziehung simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Ein fiktiver externer Link verwendet `target=_blank` ohne `rel=noopener noreferrer`.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-015
DEMO-SYN-012	Hinweis · Synthetische Fixture-Evidence · synthetisch Quelle: Rechtscheck	**Tastatur- und Beschriftungslücke simuliert** DEMO / FIKTIVE DATEN – keine Live-Prüfung, keine echte Behörde, keine echte Person und keine echte Meldung. Ein fiktives Bewerbungsfeld besitzt absichtlich keine vollständige programmatische Beschriftung.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** E-LAW-016
PA-F-0001	Hinweis · Heuristik · mittel Quelle: Erklärungs-Abgleich	**Analyse-Dienst** Bezeichnung im Dokument nicht eindeutig.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet
IMP-002	Hinweis · Stark indiziert · mittel Quelle: Impressum/Portal	**Anbieterkennzeichnung nicht eindeutig zuordenbar** Hoststruktur des Impressums weicht ab.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet
PA-F-0002	Hinweis · Heuristik · mittel Quelle: Consent-Design	**Ablehnen weniger prominent** Visuelle Gewichtung des Dialogs manuell prüfen.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet
PA-F-0003	Hinweis · Heuristik · niedrig Quelle: IAB-TCF	**IAB-TCF-Signalabweichung: Analytics** Signal und Host manuell prüfen.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet
PA-F-0017	Hinweis · Stark indiziert · mittel Quelle: Zustandsvergleich	**Tracking vor Einwilligung** Technische Beobachtung.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet
PA-F-0004	Hinweis · Stark indiziert · mittel Quelle: Zustandsvergleich	**Ablehnen nicht wirksam** Technische Beobachtung.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet
PA-F-0005	Hinweis · Stark indiziert · mittel Quelle: Zustandsvergleich	**Portal separat prüfen** Technische Beobachtung.	**Primär:** nicht zugeordnet · **Unterstützend:** nicht zugeordnet · **Kontext:** nicht zugeordnet · **Recht:** nicht zugeordnet

Zustandszusammenfassung

ZUSTAND	STATUS	NETZWERK / TRACKING	DOM-LISTENER
Vor Einwilligung	Vor der Consent-Entscheidung	2 Requests · 1 externer Netzwerk-Request · 0 Tracking-/Analyse-Transfers	0 registrierte DOM-Event-Listener
Nach Ablehnen	Ablehnung bestätigt	1 Request · 0 externe Netzwerk-Requests · 0 Tracking-/Analyse-Transfers	0 registrierte DOM-Event-Listener

ZUSTAND	STATUS	NETZWERK / TRACKING	DOM-LISTENER
Nach Akzeptieren	Akzeptanz bestätigt	1 Request · 1 externer Netzwerk-Request · 1 Tracking-/Analyse-Transfer	0 registrierte DOM-Event-Listener

15 HANDLUNG

Kommunikationsentwürfe verfügbar

ENTWÜRFE NICHT IM STANDARDREPORT AUSGEGEBEN
Die vollständigen, kontextsensitiven Entwürfe liegen separat als TXT/JSON in der Fallakte vor. Vor Versand sind Empfänger, Zuständigkeit und Sachverhalt manuell zu prüfen.

Fallakte

Fallnummer	PA-DEMO-20261011-HELMSTEDT-001
Entwurfsstatus	Manuelle Prüfung erforderlich

Verfügbarkeit

Kommunikationsentwürfe verfügbar · keine automatische Versendung.

16 GLOSSAR

100 zentrale Begriffe

Dieses Glossar erklärt die wichtigsten technischen, organisatorischen und rechtlichen Begriffe dieses Berichts in kurzer, verständlicher Form. Die Definitionen sind eine Orientierung und ersetzen keine gesetzliche Begriffsprüfung im Einzelfall.

BEGRIFF	KURZ ERKLÄRT
Accessibility	Technische und gestalterische Zugänglichkeit einer Website.
Maßnahmenkatalog	Aus Befunden abgeleitete, priorisierte Arbeitsliste mit Verantwortlichkeit, Nachtest und Evidence-Bezug.
Analyse	Auswertung technischer oder nutzungsbezogener Signale.
Analyse-/Messdienst	Dienste zur statistischen Messung von Nutzung und Reichweite.
API	Programmierschnittstelle zwischen Softwarekomponenten.
Applicant Portal	Technisches Bewerbungsportal oder Bewerbungsweg.
Auftragsverarbeitung	Verarbeitung personenbezogener Daten im Auftrag.
Aufsichtsbehörde	Zuständige öffentliche Stelle für Datenschutzaufsicht.
Authentifizierung	Prüfung, ob ein Nutzer oder Dienst bekannt ist.
Passwort	Geheime Zeichenfolge zur Authentifizierung; ein Fund in öffentlich geladenem HTML, JavaScript, JSON, XML oder TXT gilt als kompromittiert zu behandeln.
Browser-Storage	Speicherbereich des Browsers für Webanwendungen.
Cache	Zwischenspeicher zur Wiederverwendung bereits geladener Daten.
Cookie	Kleine Information, die eine Website im Browser speichert.
Cookie-Laufzeit	Zeitraum, in dem ein Cookie gespeichert bleiben kann.
Cookie-Banner	Bedienelement zur Information und Einwilligungsverwaltung.
Consent	Einwilligung zu einem bestimmten Verarbeitungsvorgang.
Consent Management Platform	Software zur Verwaltung von Einwilligungen.
Content Security Policy	Header-Regelwerk zur Begrenzung erlaubter Ressourcen.
CORS	Regelung für Ressourcenabrufe von anderen Ursprüngen.
Cross-Origin	Ressource oder Anfrage aus einem anderen Ursprung.
Dataflow	Technischer Weg von Daten zwischen Quelle und Ziel.
Datenschutzbeauftragter	Benannte Kontakt- und Kontrollfunktion für Datenschutz.
Datenschutzerklärung	Information über Datenverarbeitung und Betroffenenrechte.
Drittlandtransfer	Übermittlung personenbezogener Daten außerhalb des EWR.
DNS	Namenssystem zur Auflösung von Domains in Netzwerkadressen.
Secret	Vertraulicher Schlüssel- oder Zugangswert; der Report speichert nur Bezeichner, Fundstelle und maskierte Auszüge, niemals den Rohwert.
DOM	Strukturmodell der im Browser geladenen HTML-Seite.
Domain	Adressierbarer Namensbereich im Internet.
API-Key	Zugriffsschlüssel für eine Programmierschnittstelle; öffentliche Suchschlüssel werden von echten Zugangsdaten getrennt bewertet.
Evidence	Technischer Beleg für eine beobachtete Feststellung.
Fallback	Ersatzverfahren, wenn der bevorzugte Weg nicht verfügbar ist.
Fingerprinting	Wiedererkennung anhand einer Kombination technischer Merkmale.
Form Action	Zieladresse, an die ein Formular übermittelt werden soll.
Frontend	Im Browser ausgeführter sichtbarer Teil einer Anwendung.
Geolocation	Ermittlung oder Verarbeitung eines Standortbezugs.
HSTS	Header, der Browser auf HTTPS-Nutzung festlegt.
HTML	Auszeichnungssprache für die Struktur einer Webseite.
HTTP	Protokoll zur Übertragung von Webressourcen.
HTTPS	Mit TLS geschützte Variante von HTTP.

BEGRIFF	KURZ ERKLÄRT
IAB TCF	Standard für Signale zwischen Consent-Plattformen und Partnern.
Iframe	HTML-Element zur Einbettung einer weiteren Seite.
Impressum	Anbieterkennzeichnung einer geschäftsmäßigen Website.
Integrität	Nachvollziehbarkeit und Unveränderheit eines Belegs.
JavaScript	Programmiersprache für dynamische Browserfunktionen.
JSON-LD	Strukturierte Daten im JSON-Format innerhalb einer Seite.
Klassifizierung	Technische Zuordnung zu einem Seitentyp oder Themenbereich.
Konfidenz	Maß für die Trennschärfe einer automatischen Einordnung.
LocalStorage	Dauerhafterer Schlüssel-Wert-Speicher im Browser.
Manifest	Liste von Belegen mit Pfad, Typ und Integritätswert.
Nicht bewertet	Es liegt kein belastbarer Wert oder keine ausreichende Abdeckung für eine automatische Einstufung vor.
Metadaten	Daten, die andere Daten beschreiben.
MIME-Typ	Kennzeichnung des Inhaltsformats einer Ressource.
Netzwerk-Request	Vom Browser ausgelöste Netzwerkanfrage.
Nonce	Einmaliger Wert zur Begrenzung erlaubter Script- oder Style-Ausführung.
Origin	Kombination aus Schema, Host und Port eines Ursprungs.
PDF	Festes Dokumentformat für eine layouttreue Ausgabe.
Playwright	Werkzeug zur automatisierten Browsersteuerung.
Portalbetreiber	Stelle, die ein technisches Portal bereitstellt oder betreibt.
Privacy by Design	Datenschutz als Gestaltungsprinzip technischer Systeme.
Bearer-Token	Authentifizierungswert im Authorization-Kontext; ein öffentlich ausgelieferter Wert muss als potenziell kompromittiert geprüft werden.
Rate Limit	Begrenzung der Anzahl von Anfragen in einem Zeitraum.
Redirect	Automatische Weiterleitung auf eine andere URL.
Referrer	Vorherige URL, die ein Browser bei einer Anfrage mitteilen kann.
Robots.txt	Datei mit Hinweisen für automatisierte Crawler.
SameSite	Cookie-Attribut zur Begrenzung seitenübergreifender Übermittlung.
SHA-256	Kryptografische Hashfunktion für Integritätsvergleiche.
SessionStorage	Browser-Speicher für die Dauer eines Tabs oder Fensters.
Session-Identifier	Kennung zur Zuordnung einer Browser-Sitzung.
Shadow DOM	Gekapselter DOM-Bereich eines Web Components.
Sitemap	Maschinenlesbare Liste auffindbarer Seiten.
Source Code	Quelltext, aus dem eine Seite oder Anwendung entsteht.
Storage Access	Zugriff einer Seite auf gespeicherte Browserinformationen.
Subdomain	Untergeordneter Hostname innerhalb einer Domain.
TLS	Verschlüsselungsprotokoll für Transportverbindungen.
Tracking	Beobachtung oder Zuordnung von Nutzungssignalen.
Tracking-Pixel	Kleines Element zur Messung eines Aufrufs oder Ereignisses.
Third-Party-Host	Host, der nicht zum geprüften Hauptursprung gehört.
TDDDG	Deutsches Gesetz mit Regeln für Endgerätezugriffe und Telekommunikation.
Kritisch	Höchste technische Demo- oder Befundstufe; sie verlangt sofortige Verifikation und gegebenenfalls Sperrung oder Rotation, ist aber kein automatischer Rechtsverstoß.
Timestamp	Zeitstempel eines Ereignisses oder Dokuments.
URL	Einheitliche Adresse einer Webressource.
User Agent	Kennung des abrufenden Browsers oder Clients.
Evidence-ID	Stabile Kennung, die eine technische Beobachtung mit Screenshot, HAR, DOM, Quelle oder einem anderen Beleg verknüpft.
WCAG	Technische Leitlinien für zugängliche Webinhalte; automatische Checks ersetzen keine vollständige manuelle Konformitätsprüfung.
BFSG	Deutscher Rechtsrahmen zur Barrierefreiheit bestimmter Produkte und Dienstleistungen; die Anwendbarkeit ist einzelfallabhängig.

BEGRIFF	KURZ ERKLÄRT
Privater Schlüssel	Geheimer kryptografischer Schlüssel, der niemals öffentlich ausgeliefert oder im Report im Rohformat ausgegeben werden darf.
X-Content-Type-Options	Header gegen bestimmte MIME-Typ-Fehlinterpretationen.
X-Frame-Options	Header zur Einschränkung der Einbettung in Frames.
Zweckbindung	Verarbeitung nur für festgelegte und nachvollziehbare Zwecke.
Rechtsgrundlage	Rechtliche Grundlage für einen Verarbeitungsvorgang.
Empfänger	Stelle, der Daten offengelegt oder zugänglich gemacht werden.
Speicherdauer	Zeitraum, für den Daten aufbewahrt werden.
Personenbezug	Möglichkeit, Daten einer Person zuzuordnen.
Pseudonymisierung	Ersetzung direkter Identifikatoren bei erhaltener Zuordenbarkeit.
Anonymisierung	Veränderung, durch die ein Personenbezug entfallen soll.
Betroffenenrecht	Recht einer betroffenen Person gegenüber der verantwortlichen Stelle.
Verantwortlicher	Stelle, die Zwecke und Mittel der Verarbeitung bestimmt.
Verarbeitung	Jeder Vorgang im Zusammenhang mit personenbezogenen Daten.
Abdeckung	Umfang der im Prüfpfad tatsächlich erfassten Seiten und Zustände.
Reproduzierbarkeit	Möglichkeit, eine Beobachtung unter gleichen Bedingungen nachzustellen.

ABSCHLUSSSEITE · MASSNAHMEN & NÄCHSTE SCHRITTE · FALL PA-DEMO-20261011-HELMSTEDT-001

Technik verstehen.

Maßnahmen priorisieren.

Wirkung verifizieren.

Dieses Prüfdossier dokumentiert die im Rahmen der passiven Web- und Consent-Prüfung beobachteten technischen Signale, Datenflüsse, Speicherzugriffe und Sicherheitsmerkmale. Es dient als strukturierte Arbeitsgrundlage für Betreiber, Datenschutzbeauftragte, IT-Verantwortliche und Fachabteilungen.

Die automatische Auswertung liefert Hinweise und Prioritäten. Die endgültige rechtliche und technische Bewertung bleibt eine manuelle Aufgabe.

Der Maßnahmenkatalog im Beweispaket bündelt die aus den beobachteten Signalen abgeleiteten Handlungsempfehlungen, Zuständigkeiten und Nachtests. Er unterstützt die Umsetzung, ersetzt aber weder die Primärbelege noch die fachliche Einzelfallprüfung.

KI-gestützte Analyse · menschliche Einordnung

FALL
PA-DEMO-20261011-HELMSTEDT-001

ZIEL
https://www.demo-report.de/

STATUS
Kompakt · Technisch fertig · mit Einschränkungen

SCANZEIT
07.11.2026, 00:23:54 UTC

VERSION
Treelogy | PA · Version 8.7-demo · Export 8.7-demo

RECHTSTEXTE-ABGLEICH
DEMO_SIMULIERT

ZEITPUNKT RECHTSTEXTE-ABGLEICH
Nicht separat aufgezeichnet

Erfasste Rechtstext-Dokumente: 2. Der Zeitpunkt bezeichnet den technischen Abruf/Abgleich im Prüf-Lauf und bestätigt nicht automatisch die rechtliche Aktualität oder Vollständigkeit des Textes.

KONZEPT & UMSETZUNG
Andreas Knoll · Michael Frenzel

HINWEIS

Dieser Bericht ist eine technische Beobachtung und keine abschließende Rechtsberatung. Er ersetzt weder eine rechtliche Einzelfallprüfung noch eine vollständige Prüfung serverseitiger oder nicht erreichbarer Verarbeitung. Befunde der Stufe ·Erhöht· oder ·Hinweis· beschreiben konkreten manuellen Prüfbedarf, nicht automatisch einen Rechtsverstoß.

RECHTE AN DRITTINHALTEN

Screenshots, Texte, Bilder, Logos, Marken und sonstige Inhalte der geprüften Website verbleiben bei den jeweiligen Urhebern, Rechte- und Markeninhabern. In den Prüfberichten und Belegen können geschützte Marken, Logos und Kennzeichen Dritter erscheinen. Diese dienen ausschließlich der technischen Dokumentation des beobachteten Zustands. Es wird keine Markenlizenz erteilt und keine Zustimmung zur Benutzung der abgebildeten Zeichen außerhalb des internen Prüfkontexts erklärt. Eine Weitergabe oder Veröffentlichung ist nur mit den erforderlichen Rechten, einer gesetzlichen Grundlage oder Zustimmung zulässig.

NÄCHSTE SCHRITTE

1. Befunde im Originalsystem reproduzieren.
2. Maßnahme, Verantwortlichkeit und Frist festlegen.
3. Technische Umsetzung gezielt nachschärfen.
4. Änderung im frischen Browserkontext erneut prüfen.
5. Maßnahmen, Evidence und offene Punkte dokumentieren.

Infos und Kontakt: info@treelogy.de · www.treelogy.de
© 2026 Treelogy · Andreas Knoll · Michael Frenzel · Alle Rechte vorbehalten.