

SITE CONTROL

Benutzerhandbuch von A bis Z

Deutsch | Version 4.2.27

Deine Website sicher und selbstständig verwalten.

Installation, Seiten, Inhalte, SEO, Links, Formulare, Consent, Datenschutz, Styling, Barrierefreiheit, Tracking, Search Console, Übersetzungen, Backups und AI-Auswertungen.

Mit WordPress-Verwaltung, Stelleninseraten, Bewerbungen, Agentur-Zentrale, White Label, aktuellen Preisen und sieben Tagen kostenloser Testphase.

Für Administratoren, Mitarbeiter, Agenturen und technische Betreiber.
Stand 08.09.2026

So verwendest du dieses Handbuch

Deutsch | Site Control 4.2.27 | Stand 08.09.2026

Dieses Handbuch führt durch Installation, tägliche Website-Pflege und Erweiterungen. Die vorhandenen Kapitel bleiben als Nachschlagewerk erhalten. Überarbeitete Abläufe ersetzen die alten Anleitungen direkt im jeweiligen Kapitel; zusätzliche Themen stehen ab Kapitel 67.

Was gegenüber 3.5.0 ergänzt oder überarbeitet wurde

- WordPress-Modul: Core, Plugins, Themes, Sammelaktionen, ZIP-Updates und Wiederherstellung.
- Stelleninserate mit Unternehmen, Bewerbungen, Anhängen, CSV und einstellbaren Farben.
- Agentur mit zentraler Kundenverwaltung, White Label, WordPress und getrennten Lizenzkontingenten.
- Normale ZIP-Backups, Versionshistorie und Freigabe der Wiederherstellung.
- Sieben Tage kostenlos testen, aktuelle Modulpreise und WordPress für 49,99 USD pro Jahr.
- Hosting-Statistikordner beim Scan, WordPress-SEO-Import und Hinweise zur SQLite-Diagnose.

Bezeichnungen und Abbildungen

Administrator bedeutet vollständiger Zugang. Mitarbeiter erhalten nur ausgewählte Rechte. Runtime bezeichnet die Einbindung auf öffentlichen Website-Seiten; Modulfreischaltung die bestätigte Lizenz. Die erhaltenen Abbildungen zeigen neutrale Beispielinstallationen: Positionen und Beschriftungen können je nach Version, Sprache, Rolle und Website abweichen.

Vor größeren Änderungen

Sichere Website und Datenbank extern und prüfe die Sicherung. Bei Wiederherstellung und WordPress-Updates zählt der tatsächliche Sicherungsumfang; eine Programmsicherung ist kein vollständiges Website-Backup.

Inhaltsverzeichnis

So verwendest du dieses Handbuch	2
1. Schnellstart in sieben Schritten	6
2. Produktmodell: Free und Erweiterungen	7
3. Systemvoraussetzungen	8
4. Ordnerstruktur und richtiger Installationsort	9
5. Installation über FTP, SFTP oder Dateimanager	10
6. WordPress-Installation	11
7. Installer-Felder und Erstkonto	12
8. Anmeldung, Sitzung und Kontosicherheit	13
9. Navigation, Sprachen und lesbare URLs	14
10. Übersicht und Statuskarten	15
11. Kostenloses Website-Datenblatt	16
12. Website-Scan und Runtime-Verbindung	17
13. Seitenübersicht	18
14. SEO pro Seite	19
15. Inhalte bearbeiten	20
16. Linkprüfung	21
17. Weiterleitungen	22
18. Formulare erkennen	23
19. Forms & Schutz	24
20. Formularfunnel und Quellen	25
21. Spam Protection	26
22. Consent-Modi	27
23. Cookie-Banner und zentrale Skripte	28
24. JavaScript-Scanner und CSV	29
25. Externe Inhalte und Iframes	30

Inhaltsverzeichnis · Fortsetzung

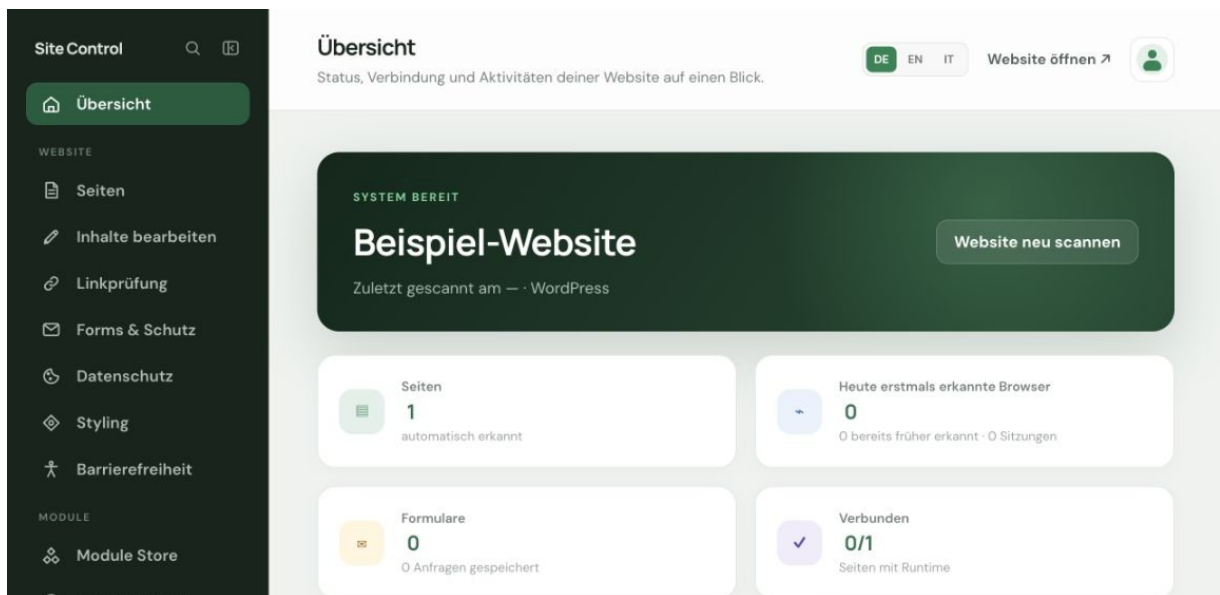
26. Datenschutz-Modul und Privacy-Profile	31
27. Aufbewahrungsfristen	32
28. Fonts scannen	33
29. Fonts lokal übernehmen	34
30. Font-Fehler und manueller Upload	35
31. Styling	36
32. Darstellung & Barrierefreiheit	37
33. Tracking aktivieren	38
34. Pageviews, Browser und Sitzungen	39
35. Tracking-Zuverlässigkeit	40
36. Tracking-Auswertungen	41
37. Audience-Speicher und Retention	42
38. Google Analytics 4	43
39. Google Search Console	44
40. Übersetzungen	45
41. Vollbackup erstellen	46
42. Backup-Inhalt und Konsistenz	47
43. Wiederherstellung und Umzug	48
44. Backup-Historie und Aufbewahrung	49
45. Module Store, Kauf und Stripe	50
46. Module und Preise	51
47. AI Website Check	52
48. AI Credits und BYOK	53
49. Agentur und White Label einrichten	54
50. Benutzer und Rollen	55
51. Einstellungen	56

Inhaltsverzeichnis · Fortsetzung

52. Updates direkt installieren	57
53. Manuelles ZIP-Update und Rückfall	58
54. Datenschutz und lokale Datenspeicherung	59
55. Sicherheitsmodell	60
56. WordPress-Besonderheiten	61
57. Klassische HTML-/PHP-Websites	62
58. Fehlerbehebung: Banner oder Werkzeuge fehlen	63
59. Fehlerbehebung: Formular nicht erkannt	64
60. Fehlerbehebung: Tracking zeigt null oder andere Werte	65
61. Fehlerbehebung: Fonts	66
62. Fehlerbehebung: Updates und Backups	67
63. Betriebskalender	68
64. Checkliste für einen sauberen Produktivstart	69
65. Glossar	70
66. Support richtig vorbereiten	71
67. WordPress, Plugins und Themes	72
68. WordPress-ZIP-Updates und Rückfall	73
69. Unternehmen für Stelleninserate	74
70. Stellen anlegen und veröffentlichen	75
71. Bewerbungen und Anhänge bearbeiten	76
72. Jobs einbetten und gestalten	77
73. Stellen und Bewerbungen als CSV	78
74. Agentur-Zentrale und Lizenzpakete	79
75. Sieben Tage kostenlos testen	80
76. AI-Auswertungen richtig lesen	81
77. Hosting-, Scan- und SQLite-Fehler	82

1. Schnellstart in sieben Schritten

Die meisten Installationen sind in wenigen Minuten betriebsbereit.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

- 1 Das vollständige Site-Control-ZIP aus der offiziellen Quelle herunterladen.
- 2 Ein externes Backup der Website und ihrer Datenbank anlegen.
- 3 Den vollständigen Ordner site-control in den Hauptordner der Website hochladen.
- 4 Im Browser `https://deine-domain.tld/site-control/install/` öffnen.
- 5 Website-Name, Administrator-E-Mail und ein starkes Passwort eintragen.
- 6 Installation abschließen, anmelden und Website neu scannen ausführen.
- 7 Website, Cookie-Einstellungen, Formulare und gegebenenfalls Tracking mit echten Tests prüfen.

Fertig

Im Dashboard erscheint System bereit. Erkannte Seiten zeigen eine Runtime-Verbindung oder einen klaren Hinweis, was noch fehlt.

2. Produktmodell: Free und Erweiterungen

Site Control ist ein Kontrollzentrum für bestehende Websites auf dem eigenen Hosting.

Bereich	Enthalten / Abrechnung
Free Core + Website Essentials	Dauerhaft kostenlos: Seiten, SEO, Inhalte, Links, Formulare, Consent, Styling, Barrierefreiheit, Benutzer und Core-Updates.
Funktionsmodule	WordPress, Tracking & Analytics, Spam Protection, Search Console, Übersetzungen, Backup & Migration, Datenschutz und Stelleninserate.
All Modules	Alle kostenpflichtigen Funktionsmodule einschließlich WordPress in einem Paket.
Agentur	White Label, zentrale Kundenverwaltung und WordPress. Eigenes Jahresabo; getrennt von All Modules.
AI Website Audit	Nutzungsabhängig über VELUNO Credits oder eigenen API-Schlüssel. Kein Modulabo.

7 Tage kostenlos testen

Die Testphase beginnt erst nach dem bewussten Start im Module Store. Alle Funktionsmodule inklusive Agentur sind verfügbar. Eine Kreditkarte ist nicht erforderlich; es entsteht kein automatisches Abo. AI-Nutzung bleibt separat kostenpflichtig. Details zur Frist und zu Testdaten: Kapitel 75.

Kauf und Kündigung

Lizenzen gelten je Installation. Kaufe einzelne Module oder ein Paket. Bestehende eigene Käufe und Paketfreigaben werden berücksichtigt. Eine normale Kündigung löscht keine Website-Daten; die Behandlung abgelaufener Testdaten ist davon zu unterscheiden. Preise: Kapitel 46.

3. Systemvoraussetzungen

Der Installer und die Diagnose des jeweiligen Moduls zeigen die verfügbaren Serverfunktionen.

- PHP 8.1 oder neuer; JSON, OpenSSL und cURL für die vorgesehenen Funktionen.
- HTTPS und ausgehende HTTPS-Verbindungen zu tatsächlich verwendeten Diensten.
- Schreibrechte für Anwendung und geschützte Datenordner sowie ausreichend freier Webespace.
- ZipArchive für ZIP-Updates, Archive und Wiederherstellung.
- PDO-SQLite für SQLite-basierte Funktionen, insbesondere Stelleninserate und entsprechende lokale Speicher.
- PDO-MySQL für lesbare WordPress-Datenbanken und deren Sicherung.

Betrieb auf unterschiedlichen Hosting-Systemen

PHP-Version, Erweiterungen, Speicherlimit, Laufzeitlimit, Dateirechte und freier Speicher wirken zusammen. Eine funktionierende WordPress-Startseite belegt deshalb noch nicht, dass jedes Site-Control-Modul seine Anforderungen erfüllt. Prüfe das Website-Datenblatt und die konkrete Fehlermeldung.

Fehlende Erweiterung

Nicht jede optionale Erweiterung blockiert den gesamten Core. Ein Datei-Backup kann möglich sein, obwohl die CMS-Datenbank nicht lesbar ist. Ein solches Archiv ist keine vollständige Datenbanksicherung. Siehe auch Kapitel 77.

4. Ordnerstruktur und richtiger Installationsort

Der Ordnername und seine Ebene sind entscheidend.

Richtig:

```
website-root/  
index.php oder index.html  
wp-content/ oder css/  
site-control/  
index.php  
install/  
app/  
assets/  
data/
```

- Nach dem Upload muss /site-control/index.php existieren.
- Falsch ist /site-control/site-control/index.php.
- Den Ordner site-control nicht umbenennen.
- Den Inhalt nicht einzeln zwischen Website-Dateien verteilen.
- Versteckte Dateien wie .htaccess müssen mitkopiert werden.

Nginx

Für Nginx liegt eine Beispielkonfiguration bei. Lesbare URLs funktionieren nur, wenn die Serverregeln den Site-Control-Unterpfad an die Anwendung leiten.

5. Installation über FTP, SFTP oder Dateimanager

Diese Methode funktioniert unabhängig vom verwendeten CMS.

- 1 ZIP lokal entpacken und prüfen, dass genau ein Ordner site-control enthalten ist.
- 2 Per SFTP, FTP oder Hosters-Dateimanager in den öffentlichen Website-Hauptordner wechseln.
- 3 Den kompletten Ordner hochladen und den Abschluss aller Dateien abwarten.
- 4 Die Installationsadresse im Browser öffnen.
- 5 Alle Serverprüfungen lesen. Rote Punkte zuerst beheben, statt die Installation mehrfach zu starten.
- 6 Administrator anlegen und die Installation abschließen.

Sicherheit

Verwende bevorzugt SFTP oder den verschlüsselten Dateimanager des Hosters. Klassisches FTP überträgt Zugangsdaten unverschlüsselt.

6. WordPress-Installation

Das vollständige Site-Control-Paket lässt sich über WordPress oder über den Webpace installieren.

- 1 Offizielle ZIP herunterladen und Website samt Datenbank sichern.
- 2 In WordPress unter Plugins → Installieren → Plugin hochladen das vollständige Paket auswählen.
- 3 Den hochgeladenen Site-Control-Installer aktivieren und den angezeigten Einrichtungsschritten folgen.
- 4 Site Control öffnen und das eigene Administratorkonto einrichten.
- 5 Installation abschließen, Scan prüfen und öffentliche Website testen.

Die produktive Anwendung liegt im Website-Hauptordner unter /site-control/. Der Upload-Installer überträgt sie dorthin; Site Control bleibt eine eigenständige Anwendung. Der WordPress-Menüpunkt öffnet diese Installation. Für die Runtime wird eine MU-Bridge verwendet.

Alternativer Installationsweg

Falls Uploadgrenze, Schreibrechte oder Hostingregeln den WordPress-Weg verhindern, den vollständigen Ordner per SFTP/FTPS oder Dateimanager hochladen. Kapitel 4 und 5 beschreiben die Ordnerstruktur.

Die Installation auf einer WordPress-Website und die kostenlosen Website-Werkzeuge benötigen kein gekauftes WordPress-Modul. Die Verwaltung von WordPress, Plugins und Themes ist die kostenpflichtige Erweiterung aus Kapitel 67.

7. Installer-Felder und Erstkonto

Die im Installer eingegebenen Werte bilden die erste Vertrauensbasis.

Feld	Verwendung
Website-Name	Bezeichnung im Dashboard; später in Einstellungen änderbar
Administrator-E-Mail	Anmeldung und Kontokennung
Passwort	Mindestens zwölf Zeichen; nur für Site Control
Übertragungscode	Nur verwenden, wenn eine berechtigte Installation übertragen wird

- Passwortmanager verwenden.
- Keine E-Mail-Postfach- oder WordPress-Passwörter wiederverwenden.
- Installationsseite nach erfolgreicher Installation nicht erneut ausführen.
- Erstes Konto ist Administrator und besitzt alle aktuellen und künftigen Rechte.

8. Anmeldung, Sitzung und Kontosicherheit

Site Control verwendet eigene Konten, getrennt von WordPress.

- Anmeldung über /site-control/login/.
- Abmelden über das Kontomenü.
- Name, E-Mail, Passwort und Avatar im eigenen Konto ändern.
- Deaktiviert ein Administrator einen Benutzer, endet dessen Zugriff spätestens beim nächsten Request.
- Browser und Passwortmanager dürfen das Passwort speichern; gemeinsam genutzte Geräte vermeiden.

Verdächtiger Zugriff

Passwort sofort ändern, weitere Benutzer prüfen, Server- und Proxy-Konfiguration kontrollieren und ein sauberes Backup sichern.

9. Navigation, Sprachen und lesbare URLs

Die Seitenleiste zeigt nur Bereiche, die für Rolle und Installation verfügbar sind.

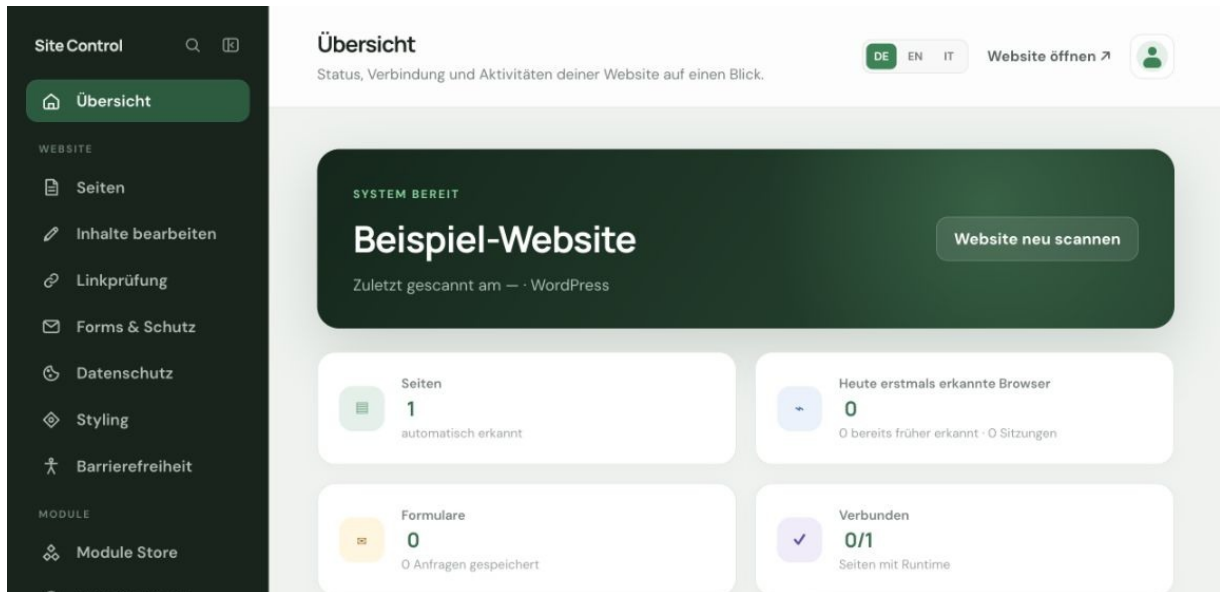
- Menü per Symbol einklappen und wieder ausklappen.
- Über die Suche einen Menüpunkt finden.
- DE, EN und IT wechseln ausschließlich die Dashboard-Sprache.
- Lesbare URLs wie `/site-control/consent/` bleiben bevorzugt.
- Alte sichere Adressen mit `index.php?view=consent` dienen als Rückfallebene.
- Nicht freigegebene Mitarbeiterbereiche erscheinen nicht und sind auch bei direktem Aufruf serverseitig gesperrt.

404 bei lesbarer URL

Zuerst `/site-control/index.php?view=dashboard` testen. Funktioniert die Rückfalladresse, fehlen meist Rewrite-Regeln oder WordPress fängt den Unterpfad ab.

10. Übersicht und Statuskarten

Die Übersicht ist die Startseite für Scanstand, Verbindung und aktuelle Aktivitäten.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

- Website-Name und Zeitpunkt des letzten Scans
- Anzahl erkannter Seiten und Formulare
- Runtime-Abdeckung
- Neue und wiederkehrende Browser, soweit Tracking aktiv und erlaubt ist
- Letzte vollständig in Site Control gespeicherte Anfragen
- Aktive Module und offene Einrichtungen
- Eingeklapptes technisches Website-Datenblatt

Website neu scannen

Nach Theme-, Plugin-, Builder-, Seitenstruktur- oder Formularänderungen erneut scannen. Ein Scan erkennt den Stand; er ersetzt keinen Browser-Funktionstest.

11. Kostenloses Website-Datenblatt

Technische Bestandsdaten findest du in der Übersicht; der Bereich gehört zum Free Core.

Gruppe	Beispiele
Website	Website-Typ, Adresse und robots.txt
Server & PHP	PHP-Version, Schnittstelle, Webserver, Architektur, Betriebssystem, cURL
PHP-Grenzwerte	Arbeitsspeicher, Ausführungszeit, Upload, POST und Eingabevariablen
WordPress	Core-, Theme-, Parent-Theme-, Builder- und Plugin-Versionen
Datenbank	System und Version; sensible Verbindungsangaben nur für Administratoren
SSL & Verbindung	HTTPS, TLS-Verbindung und Zertifikatsdaten

- Die Karten werden auf breiten Ansichten in zwei Spalten angezeigt; kleinere Ansichten passen sich an.
- Das Datenblatt wird bei Website neu scannen aktualisiert. Nicht verfügbare Werte werden entsprechend behandelt.
- Es zeigt Konfiguration und Bestand, keine vollständige Leistungsdiagnose.
- Passwörter gehören weder ins Datenblatt noch in Screenshots für Dritte.

12. Website-Scan und Runtime-Verbindung

Der Scan erfasst Website-Inhalte und überprüft die öffentliche Einbindung.

- 1 Übersicht öffnen und Website neu scannen ausführen.
- 2 Erkannte Seiten und Formulare auf Plausibilität prüfen.
- 3 Runtime-Abdeckung auf verschiedenen Seitentypen kontrollieren.
- 4 Cookie-Einstellungen, Formulare und Besucherwerkzeuge in einem privaten Fenster testen.

Hosting-Dateien sind keine Website-Seiten

Erkannte Hosting-Statistikberichte von AWStats oder Webalizer sowie bestimmte Backup- und Verwaltungsverzeichnisse werden vom Inhaltsscan ausgeschlossen. Eine normale Seite namens stats wird nicht allein wegen ihres Namens entfernt. Die Erkennung berücksichtigt Hinweise auf tatsächlich erzeugte Statistikberichte.

Nach einer Aktualisierung erneut scannen, wenn alte Berichte noch im Bestand stehen. Der Ausschluss ändert den Scanbestand und löscht keine Hosting-Dateien. Tausende unerwartete Seiten sind ein Anlass, die Herkunft zu prüfen.

Einbindungswege

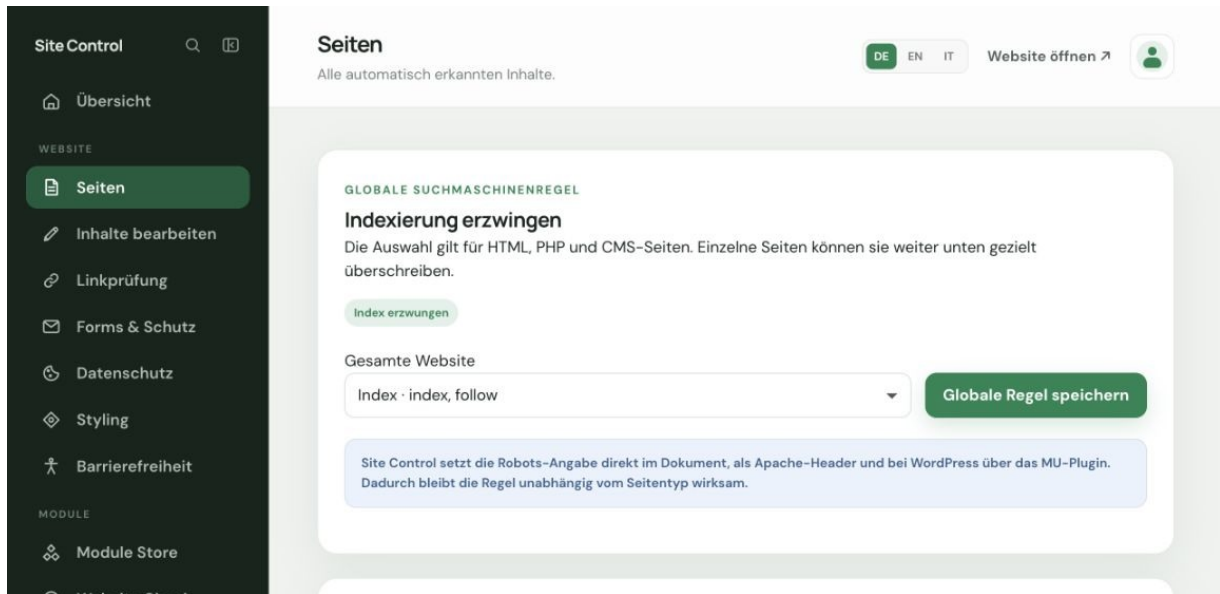
- WordPress: MU-Bridge im Frontend.
- LP-Satellite: gemeinsamer PHP-Renderer.
- Klassische HTML-/PHP-Websites: unterstützte direkte Runtime-Einbindung bzw. gerenderte Head-Bereiche.

Grenze eines Scans

Ein erfolgreicher Scan bestätigt nicht automatisch den Versand eines Formulars oder die korrekte Darstellung jeder Seite. Öffentliche Funktionsprüfungen bleiben nötig.

13. Seitenübersicht

Unter Seiten verwaltest du Status, Verbindung, Indexierung und SEO pro URL.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

- Nach Status, Seitentyp oder URL filtern und sortieren.
- Seiten über Titel oder Route suchen.
- Startseite, WordPress-Seite und andere Typen werden gekennzeichnet.
- Status und Runtime-Verbindung erscheinen getrennt.
- Indexierung global übernehmen, erlauben oder sperren.
- Seite öffnen oder vorübergehend deaktivieren.

Deaktivieren

Eine deaktivierte Seite liefert eine temporäre Nichtverfügbarkeit. Vorher Navigation, Kampagnen, Formulare und Suchmaschinenwirkung bedenken.

14. SEO pro Seite

SEO-Daten lassen sich im Zusammenhang mit der jeweiligen öffentlichen URL prüfen und pflegen.

Feld	Verwendung
SEO-Titel / Beschreibung	Dokumenttitel und Beschreibung für Suchergebnisse; keine Ranking-Garantie
Canonical / Indexierung	Bevorzugte URL und erlaubte oder gesperrte Indexierung
Social-Media-Bild	Vorschaubild, gegebenenfalls globaler Standard
Schema-Typ	Passende strukturierte Einordnung der Seite

WordPress und bestehende SEO-Daten

Beim Import berücksichtigt Site Control die WordPress-Quelle und unterstützte SEO-Daten. Leere, übernommene und bewusst selbst gesetzte Angaben dürfen nicht pauschal gleichbehandelt werden. Vor Änderungen die importierte Vorschau und die tatsächlich ausgelieferte Seite vergleichen.

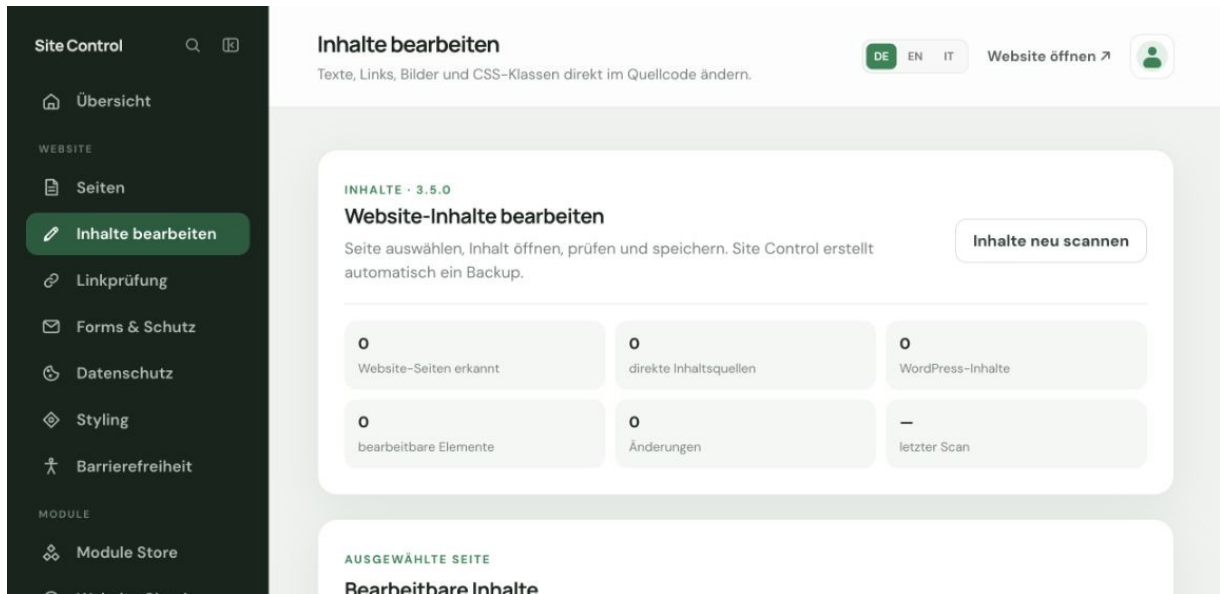
- 1 Seite auswählen und aktuelle Angaben prüfen.
- 2 Gewünschte Werte gezielt bearbeiten und speichern.
- 3 Öffentliche URL, HTML-Quelltext, Canonical und Meta-Tags kontrollieren.
- 4 Bei Abweichungen Cache, SEO-Plugin, Theme und Scanstand vergleichen.

Import ist keine Inhaltsbereinigung

Ein auffälliger SEO-Titel kann bereits aus WordPress stammen oder beim Import entstanden sein. Zuerst beide Quellen prüfen, bevor Originalinhalte oder Plugin-Daten gelöscht werden.

15. Inhalte bearbeiten

Der Inhaltseditor ändert freigegebene statische Inhalte kontrolliert.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

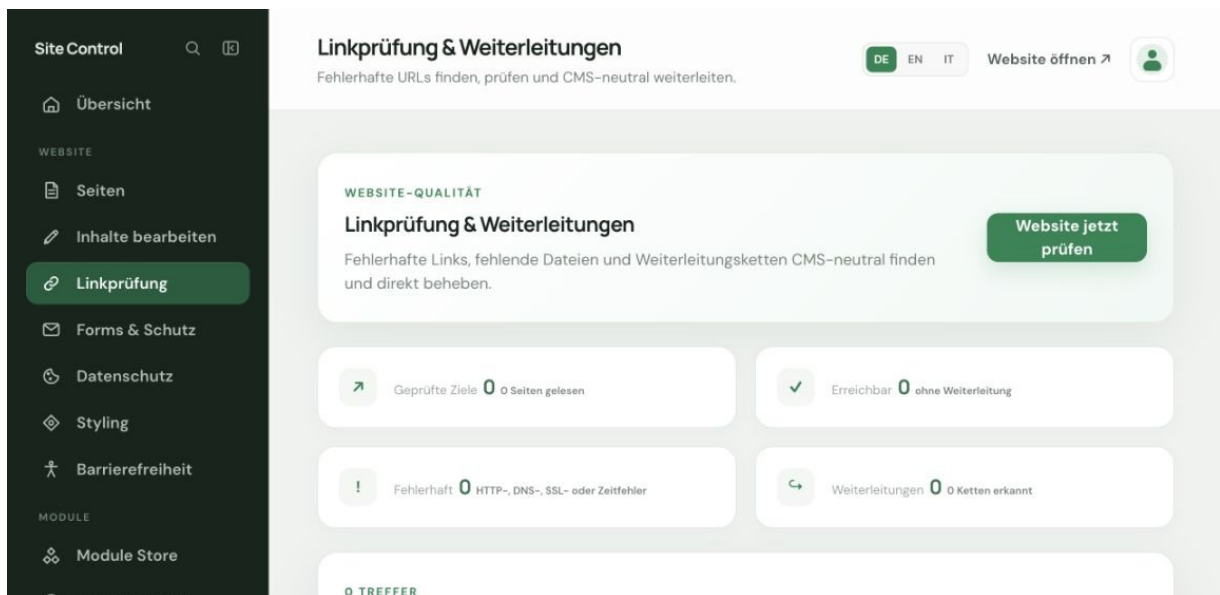
- Website-Inhalte zuerst scannen.
- Seite und danach ein erkanntes Element auswählen.
- Text oder unterstützte Inhalte bearbeiten und Vorschau prüfen.
- Vor dem Schreiben wird die Originaldatei gesichert.
- Ändert sich die Quelldatei zwischen Erkennung und Speichern, stoppt der Konfliktschutz.
- Dynamische PHP- und WordPress-Inhalte werden aus Sicherheitsgründen nicht blind verändert.

Keine statischen Inhalte gefunden

Das bedeutet nicht, dass die Seite leer ist. Der sichtbare Inhalt kann dynamisch aus WordPress, PHP, einem Builder oder einer Datenbank kommen und ist daher nicht direkt dateibasiert änderbar.

16. Linkprüfung

Die Linkprüfung unterscheidet echte Fehler von Blockaden und Weiterleitungen.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

Status	Bedeutung
Erreichbar	Antwort ohne Weiterleitung
Weiterleitung	Ziel erreicht; Ketten werden separat markiert
Fehlerhaft	HTTP-, DNS-, SSL- oder Zeitfehler
Blockiert	Zum Beispiel 401, 403 oder 429; nicht automatisch defekt

- Prüflauf kann fortgesetzt werden.
- Ergebnisse nach Status filtern.
- Einzelne URL im Browser gegenprüfen.
- Bei externen Seiten mögliche Bot-Sperren berücksichtigen.

17. Weiterleitungen

Exakte URL-Regeln werden getrennt von der Linkprüfung verwaltet.

- 1 Alte exakte Route eintragen.
- 2 Neues Ziel vollständig prüfen.
- 3 Passenden dauerhaften oder temporären Status wählen.
- 4 Regel speichern und alte URL in privatem Fenster testen.
- 5 Weiterleitungsketten vermeiden; alte Route direkt auf das endgültige Ziel führen.

Schleifen

Quelle und Ziel dürfen sich nicht gegenseitig aufrufen. Bei einer Schleife Regel sofort deaktivieren und Server- sowie CMS-Regeln mitprüfen.

18. Formulare erkennen

Site Control findet klassische und verbreitete CMS-Formulare beim Scan und zur Laufzeit.

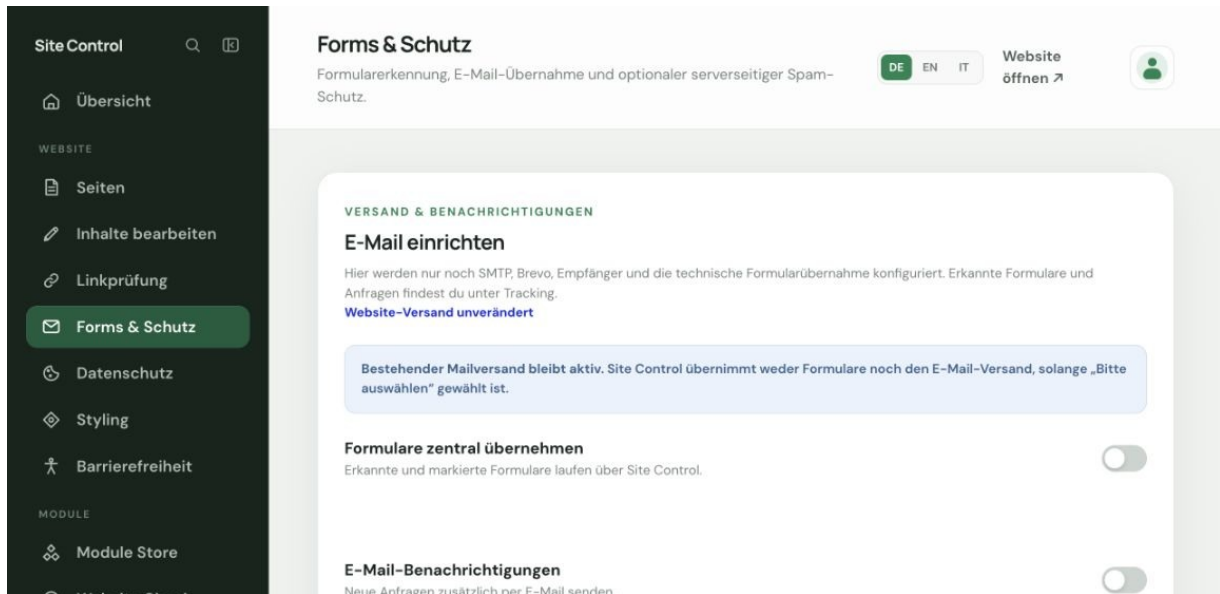
- Funnelforms, Contact Form 7, Fluent Forms, WPForms, Gravity Forms, Elementor und weitere bekannte Quellen
- Divi-Kontaktformulare direkt aus Builder-Shortcodes
- Klassische HTML-, PHP- und AJAX-Formulare
- Eigene markierte Formulare und unterstützte Runtime-Ereignisse
- Login, Suche, Warenkorb, Checkout und Administratorformulare werden standardmäßig ausgeschlossen

Erkannt ist nicht gespeichert

Ein bestätigter Formularabschluss kann gezählt werden, obwohl der vollständige Inhalt weiterhin ausschließlich beim Formularplugin liegt. Site Control speichert Felder nur, wenn das Formular ausdrücklich übernommen wurde.

19. Forms & Schutz

Die Formularseite trennt Versand, Speicherung, Erkennung und Schutz.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

- E-Mail-Versand und Absenderdaten einrichten.
- Erkannte Formulare aktivieren, ignorieren oder konfigurieren.
- Erfolgs-URL, Erfolgsselektor, Erfolgstext und Fehlerselektor ergänzen.
- Tracking und Spam-Schutz pro Formular ein- oder ausschalten.
- Site-Control-Formularanfragen mit Feldern und Zeitpunkt verwalten.
- Aufbewahrung und Upload-Löschung beachten.

- 1 Ein echtes Testformular mit realistischer E-Mail-Adresse absenden.
- 2 Erfolgsanzeige im Browser prüfen.
- 3 E-Mail-Eingang und gegebenenfalls Spamordner prüfen.
- 4 Tracking-Funnel und gespeicherte Inhalte getrennt kontrollieren.

20. Formularfunnel und Quellen

Ein Absendeversuch ist noch keine Conversion.

Ereignis	Definition
Submit	Absendeversuch wurde ausgelöst
Success	Erfolg technisch bestätigt
Failure	Fehler technisch bestätigt
Unknown	Kein belastbares Erfolgs- oder Fehlersignal

Die Herkunftsübersicht ordnet bestätigte Abschlüsse nach Plugin oder technischer Formularart. Wenn ein Plugin seine Erfolgsanzeige ändert, müssen URL, Selektor oder Textmarker möglicherweise angepasst werden.

21. Spam Protection

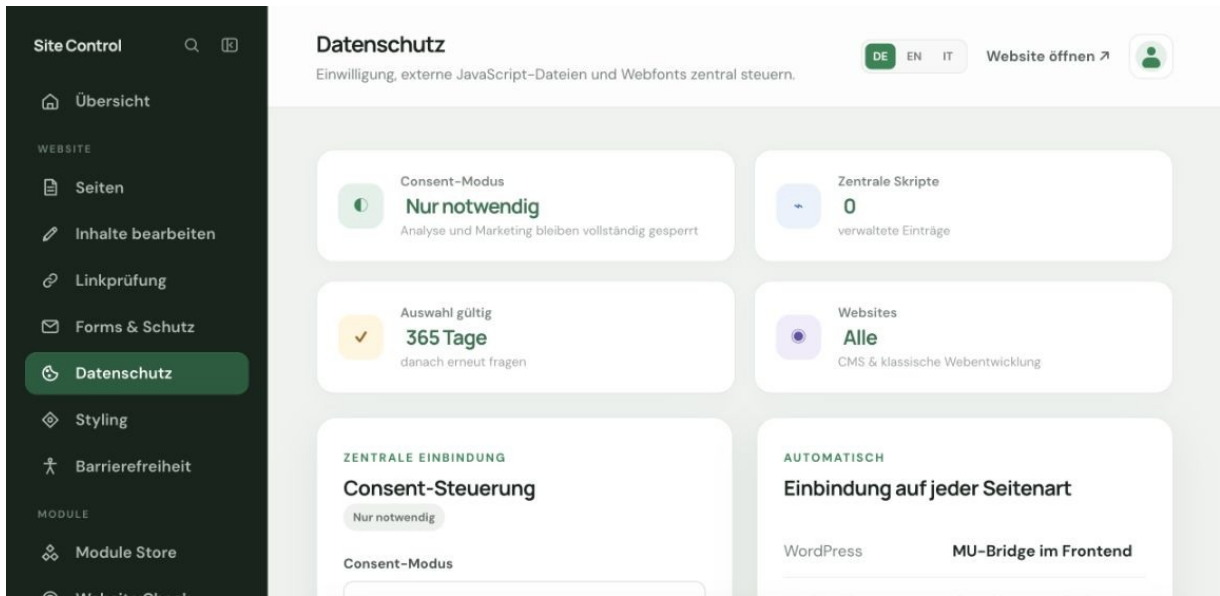
Der Schutz bewertet generische Signale, ohne Formwerte in Spam-Logs zu speichern.

Modus	Verhalten
Observe	Bewerten und protokollieren, aber nicht eingreifen
Mark	Verdächtige Anfragen markieren
Block	Anfragen ab Blockschwelle mit neutraler Meldung ablehnen

- Honeypot, Ausfüllzeit, URLs, Spam-Phrasen, Domains, Muster, Duplikate und Burst-Verhalten fließen in den Score ein.
- Standard: Mark ab 35, Block ab 70, Mindestzeit 1200 ms, URL-Limit 3.
- Allowlist hat Vorrang vor Blocklist.
- Erst Observe prüfen, dann Mark und erst nach False-Positive-Test Block einsetzen.
- Logs enthalten keine Namen, E-Mails, Nachrichten oder Feldwerte.

22. Consent-Modi

Consent steuert, wann optionale Ressourcen geladen werden.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

Modus	Verhalten
Site-Control-Cookie-Banner	Banner und Einwilligungssteuerung aktiv
Externes CMP	Site Control wartet auf das Einwilligungssignal des externen Managers
Nur notwendig	Analyse und Marketing bleiben vollständig gesperrt

- Datenschutzerklärungs-URL setzen.
- Zeitraum bis zur erneuten Abfrage wählen.
- Externe Inhalte bis zur Marketing-Einwilligung blockieren.
- Banner auf der Website mit Vorschauparameter testen.

Rechtlicher Hinweis
Die technische Konfiguration ist keine Rechtsberatung. Kategorien, Texte, Dienste und Aufbewahrung müssen zur tatsächlichen Website und zur anwendbaren Rechtslage passen.

23. Cookie-Banner und zentrale Skripte

Skripte werden ihrem Zweck nach den vorhandenen Consent-Kategorien zugeordnet.

Kategorie	Zweck
Notwendig	Technisch erforderliche Funktionen
Funktional	Optionale Funktionsdienste
Analyse	Interne Messung, GA4 und ähnliche Analysedienste
Marketing	Werbe- und entsprechende externe Dienste

- Datenschutz-URL und angezeigte Texte zur tatsächlichen Website passend eintragen.
- Datei-URLs und Inline-Skripte nur aus bekannter Quelle übernehmen.
- Den JavaScript-Scanner zur Bestandsaufnahme nutzen und Zuordnung bewusst prüfen.
- Externe Inhalte und Iframes zusätzlich auf ihr Ladeverhalten testen.

Nach dem Speichern

Website- und CDN-Caches leeren und in einem privaten Fenster prüfen: ohne Einwilligung, nach Auswahl einzelner Kategorien und nach Widerruf. Die technische Funktion ersetzt keine Prüfung der eigenen Texte und Dienste.

24. JavaScript-Scanner und CSV

Der Scanner hilft beim Zuordnen, entscheidet aber nicht blind für den Administrator.

- Scan findet bekannte und dynamisch nachgeladene Skripte.
- Ohne Auswahl bleibt ein Eintrag unverändert.
- Automatische Zuordnung kann vorsichtig blockiert werden, wenn ein PHP- oder Sonderfall nicht sicher schreibbar ist.
- CSV exportiert ID, Kategorie, Bezeichnung, Zweck und Cookie-Name.
- Eine ausdrückliche manuelle CSV-Zuordnung anhand der ID hat Vorrang vor zuordenbar = false.
- Ungültige oder nicht mehr vorhandene IDs werden übersprungen, ohne gültige Zeilen zu verlieren.

Manuell bedeutet verantwortlich

Der Import übernimmt eine bewusste Administratorenentscheidung. Deshalb Kategorie und Dienstbeschreibung vor dem Import prüfen.

25. Externe Inhalte und Iframes

Optionale Einbettungen sollen vor der Freigabe keine unnötige Verbindung aufbauen.

- Externe Iframes werden bis zur Marketing-Einwilligung blockiert, wenn die Funktion aktiv ist.
- Zahlungs- und Captcha-Dienste können als notwendige Ausnahmen bestehen bleiben.
- Ausnahmen werden über exakten Host und zulässigen Pfad geprüft.
- YouTube, Maps, Social- und andere Einbettungen nach jeder Theme- oder Pluginänderung erneut testen.
- Eine sichtbare leere Fläche kann auf einen blockierten Embed ohne Ersatzdarstellung hindeuten.

26. Datenschutz-Modul und Privacy-Profile

Profile setzen einen technischen Rahmen, einzelne Werte bleiben sichtbar.

Profil	Ausrichtung
Standard	Ausgewogener Schutz für typische Unternehmensseiten
Streng	Weniger gespeicherte Daten, kürzere Fristen und stärkerer URL-Schutz
Maximal	Kein Referrer, maskierte sensible Werte und besonders kurze Fristen

- Referrer-Schutz steuert, welche Quelladresse der Browser mitsendet.
- Eigene sensible Parameternamen können zusätzlich maskiert werden.
- Consent-Nachweise speichern ID, Zeitpunkt, Version und Kategorien.
- Ändert sich die relevante Konfiguration, kann gezielt eine neue Einwilligung verlangt werden.

27. Aufbewahrungsfristen

Consent, Formulare, Tracking und Systemdaten haben getrennte Fristen.

Datentyp	Beispiel Standard	Einstellbereich
Consent-Nachweise	1095 Tage	30 bis 3650 Tage
Formularinhalte	180 Tage	1 bis 3650 Tage
Tracking	90 Tage	1 bis 3650 Tage
Systemdaten	30 Tage	abhängig von Datentyp und Core-Einstellung

Zuerst erreichtes Limit

Bei lokalen Betriebsdaten kann zusätzlich zu Alter auch ein Mengen- oder Größenlimit gelten. Site Control bereinigt nach dem zuerst erreichten Limit.

28. Fonts scannen

Der Font-Scan sucht externe Anbieter und lokale Schriftpfade - auch in versteckten Quellen.

- Google Fonts, Bunny Fonts, Adobe Fonts/Typekit und Font Awesome
- Google reCAPTCHA, Themes, Elementor, Divi und andere Builderquellen
- CSS, PHP, JavaScript, Shortcodes, generierte Caches und lokale Fontdateien
- Anbieterfundstellen, lokal übernehmbare Quellen und lokale Font-Gesundheit werden getrennt dargestellt

Viele Fundstellen

Eine hohe Zahl bedeutet Verweise im Quellcode, nicht dieselbe Zahl sichtbarer Schriften oder Netzwerkaufufe.
Identische Pfade werden in der Oberfläche gruppiert.

29. Fonts lokal übernehmen

Unterstützte Anbieter-Stylesheets werden geprüft, heruntergeladen und auf lokale Auslieferung umgestellt.

- 1 Fonts neu scannen.
- 2 Unter Externe Fonts lokal ausliefern eine konkrete Quelle öffnen.
- 3 Quelle und Anzahl der Dateien prüfen.
- 4 Lokal übernehmen wählen.
- 5 Website in mehreren Browsern und Seitentypen visuell prüfen.
- 6 Netzwerkprüfung wiederholen und externe Anbieteraufrufe kontrollieren.

Nach Kündigung

Bereits gespeicherte lokale Auslieferungen und Fontdateien bleiben aktiv. Das Dashboard bleibt lesbar; neue Scans, Aktualisierungen und Änderungen werden gesperrt.

30. Font-Fehler und manueller Upload

Nicht jede gefundene URL ist ein gültiges, direkt lokalisierbares Stylesheet.

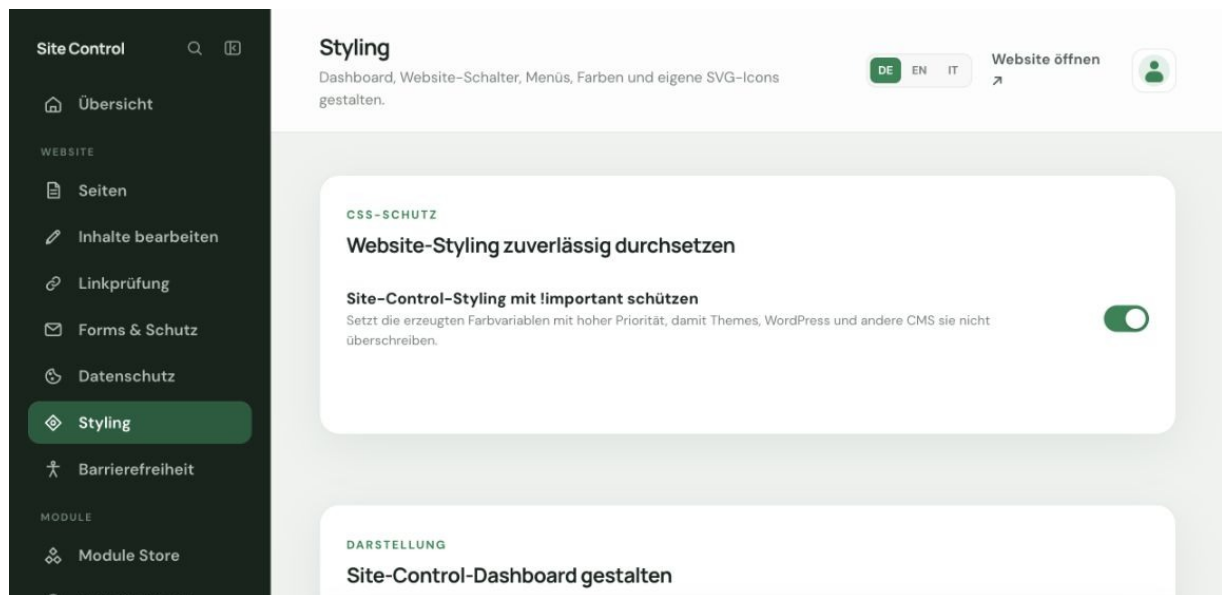
Meldung	Typische Ursache
Stylesheet ungültig	HTML, Script, Platzhalter oder unerwarteter Inhalt statt CSS
Zu viele Schriftdateien	Sicherheitsgrenze bei sehr großem oder generiertem Anbieter-Stylesheet
HTTP 400	Unvollständige URL, dynamischer Parameter oder Anbieter lehnt Anfrage ab
Quellcode-Pfad nicht auflösbar	Dateiverweis existiert im Code, ist aber nicht als reale lokale Datei nachweisbar

Manueller Weg

- 1 Anbieter-Quelle auswählen.
- 2 Schriftfamilie, Gewicht und Stil korrekt eintragen.
- 3 WOFF2, WOFF, TTF oder OTF auswählen.
- 4 Datei prüfen und lokal speichern.
- 5 Weitere Gewichte nacheinander derselben Quelle hinzufügen.

31. Styling

Dashboard und Besucherwerkzeuge lassen sich zentral gestalten.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

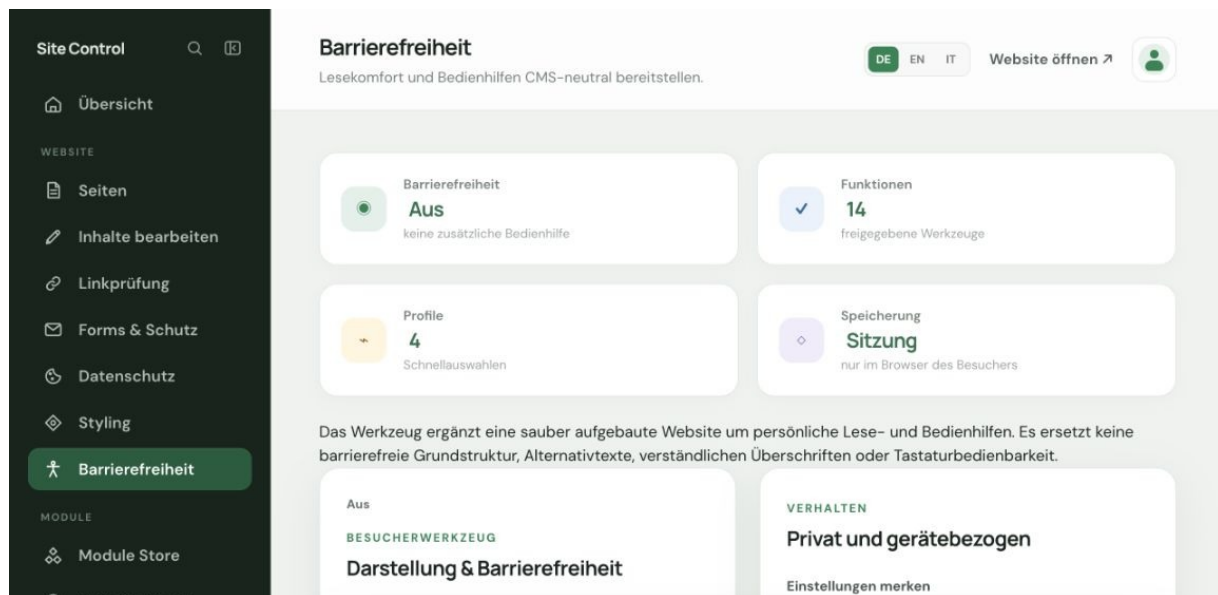
- Dashboard-Grundfarben ohne White Label
- CSS-Schutz für zuverlässig durchgesetzte Website-Regeln
- All-in-one-Schalter und gemeinsames Werkzeugmenü
- Cookie-Button und Banner
- Sprachumschalter und Sprachmenü
- Barrierefreiheits-Button und Bedienfeld
- Eigene SVG-Icons mit sicherer Prüfung

Testen

Kontrast, Fokus, Mobilansicht und Überlagerungen auf realen Seiten prüfen. Ein schönes Dashboard sagt nichts über die Barrierefreiheit der Website aus.

32. Darstellung & Barrierefreiheit

Das Besucherwerkzeug bietet persönliche Lese- und Bedienhilfen.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

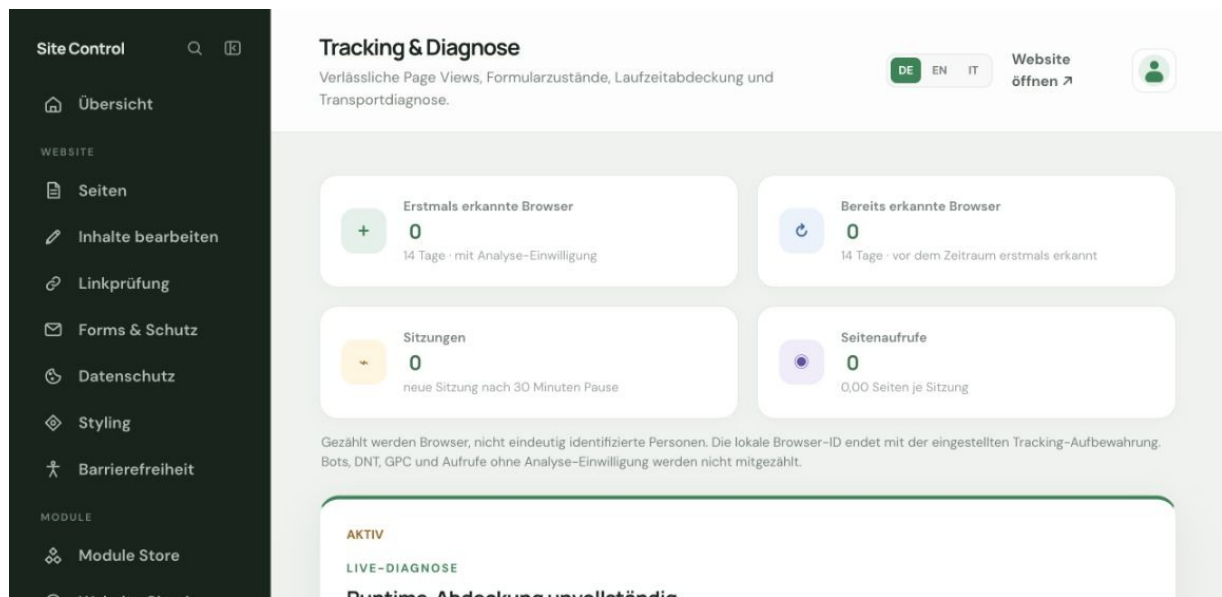
- Werkzeug global aktivieren oder deaktivieren.
- Einstellungen nur in der Browsersitzung oder entsprechend der Auswahl merken.
- Systemeinstellungen des Geräts berücksichtigen.
- Profile als schnelle Ausgangspunkte anbieten.
- Einzelne Werkzeuge deaktivieren; sie verschwinden vollständig aus dem Besucherpanel.

Kein Ersatz für barrierefreien Code

Das Werkzeug ersetzt keine semantische Struktur, Alternativtexte, verständliche Überschriften, Tastaturbedienung, Fokusführung oder ausreichende Kontraste.

33. Tracking aktivieren

Site Control zählt nur nach den konfigurierten Datenschutz- und Browsersignalen.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

- 1 Tracking & Diagnose öffnen.
- 2 Internes Tracking aktivieren.
- 3 Consent-Modus kontrollieren.
- 4 Speichern und Endpunkt & Speicher testen ausführen.
- 5 Private Website-Sitzung mit Analyse-Einwilligung öffnen.
- 6 Mehrere Seiten besuchen und Diagnose erneut prüfen.

- GA4-ID ist optional.
- Bei Site-Control-Consent starten internes Tracking, GA4 sowie Telefon- und E-Mail-Tracking erst nach Analyse-Einwilligung.
- DNT und GPC haben Vorrang.

34. Pageviews, Browser und Sitzungen

Die Kennzahlen sind technisch definiert und dadurch reproduzierbar.

Kennzahl	Definition
Pageview	Ein initialer Dokumentaufruf oder tatsächlicher SPA-Wechsel von Pfad oder Query
Erstmals erkannt	Lokale Browser-ID im Zeitraum zum ersten Mal gesehen
Bereits erkannt	Browser war vor Beginn des Zeitraums bekannt
Sitzung	Ereignisgruppe; nach 30 Minuten Pause beginnt eine neue
Seiten je Sitzung	Pageviews geteilt durch Sitzungen

Browser sind keine Personen

Ein Mensch kann mehrere Geräte oder Browser verwenden; Cookies können gelöscht werden. Umgekehrt können mehrere Personen denselben Browser teilen. Die Oberfläche benennt deshalb bewusst Browser statt eindeutiger Besucher.

35. Tracking-Zuverlässigkeit

Die Zahlen sind nutzbar, aber bewusst nicht identisch mit Serverlogs oder GA4.

- Bots, Crawler, Monitoring, Headless-Browser und navigator.webdriver werden gefiltert.
- DNT, GPC und fehlende Analyse-Einwilligung verhindern die Erfassung.
- Eine zufällige Event-ID verhindert Duplikate für sieben Tage.
- Fetch ist primär, Beacon der Fallback, sessionStorage hält eine begrenzte Retry-Queue.
- Manuelle Tests werden getrennt gespeichert und beeinflussen keine Produktionsstatistik.
- Adblocker, Browserlöschung, Netzabbrüche und Consent-Entscheidungen erzeugen unvermeidbare Abweichungen.

Interpretation

Nutze Trends, Seitenverhältnisse und bestätigte Aktionen. Behaupte nicht, eine Zahl seien exakt so viele Menschen.

36. Tracking-Auswertungen

Die Seite verbindet Aktivität, Quellen und technische Diagnose.

- Zeitraum 14 oder 28 Tage
- Tagesdiagramm für Seitenaufrufe
- Top-5-Seiten im gewählten Zeitraum
- Erstmals und bereits erkannte Browser
- Sitzungen und Seiten je Sitzung
- Formularfunnel Submit, Success, Failure und Unknown
- Formularquellen nach Plugin oder technischer Art
- Telefon- und E-Mail-Klicks sowie Kopiervorgänge
- Runtime-Abdeckung, Endpunkt und letzter Pageview

37. Audience-Speicher und Retention

Kleine Websites bleiben bei JSON; größere Historien migrieren automatisch zu SQLite.

- Bis 10.000 Browser und 5 MB: atomare JSON-Historie.
- Ab einem Grenzwert: automatische vollständige SQLite-Migration.
- Neue Pageviews werden danach transaktional geschrieben.
- Die Browser-ID wird spätestens mit der Tracking-Aufbewahrung erneuert.
- Bei entzogenem Analyse-Consent wird die lokale ID sofort gelöscht.
- Die tägliche Retention läuft auch ohne neue Pageviews.

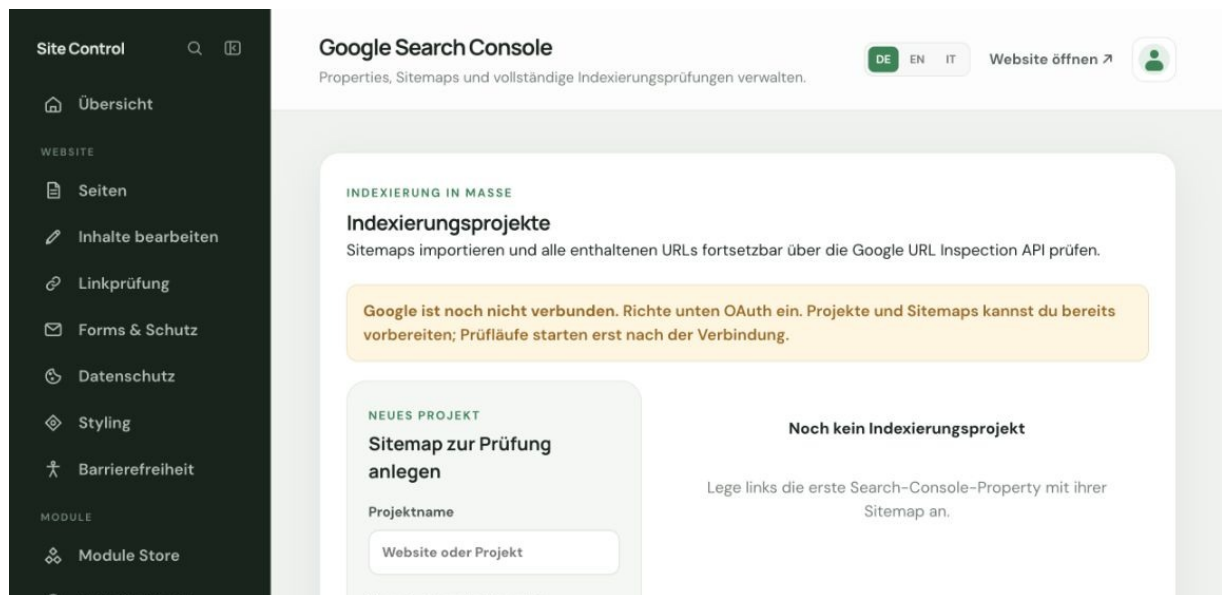
38. Google Analytics 4

GA4 kann optional parallel eingebunden werden.

- Measurement-ID im Format G-XXXXXXXXXX eintragen.
- Consent-Konfiguration bestimmt den Ladezeitpunkt.
- GA4 und Site Control verwenden unterschiedliche Identifikations-, Filter- und Verarbeitungsregeln.
- Abweichungen sind normal und kein automatischer Fehler.
- In GA4 Echtzeit, Tag Assistant und Browsernetzwerk getrennt prüfen.
- Keine Garantie zur Einwilligungsfreiheit ableiten.

39. Google Search Console

Das Modul bringt Properties, Sitemaps und URL-Inspections in Site Control.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

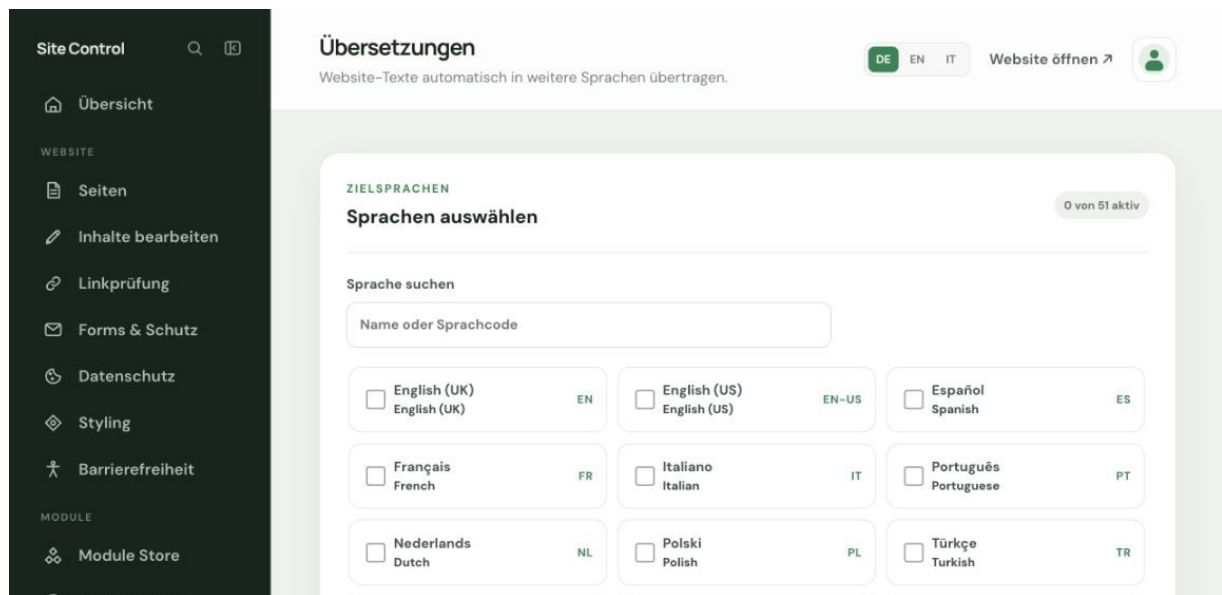
- 1 Google OAuth verbinden.
- 2 Verfügbare Property auswählen.
- 3 Indexierungsprojekt mit Name und Sitemap-URL anlegen.
- 4 URLs importieren und fortsetzbaren Prüflauf starten.
- 5 PASS, nicht indexiert und ungeprüft getrennt auswerten.
- 6 Einzelne URL bei Bedarf direkt prüfen.

Google-Limits

URL Inspection unterliegt Google-Quoten und Berechtigungen. Ein Site-Control-Ergebnis kann nur so aktuell sein wie die von Google gelieferte Antwort.

40. Übersetzungen

Translations führt von der Zielsprache bis zur veröffentlichten Sprachseite.



Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

- 1 Zielsprachen auswählen.
- 2 Sprach-URL und Umschalter einrichten.
- 3 Seiten und Textbausteine erfassen.
- 4 Übersetzungen bearbeiten oder per CSV austauschen.
- 5 SEO-Titel, Meta-Beschreibung und übersetzte URL prüfen.
- 6 Sprachabhängige Bilder hinterlegen.
- 7 Review abschließen und veröffentlichen.
- 8 Sprach-Sitemap kontrollieren.

- Ohne Ersatzbild bleibt das Original aktiv.
- Statusfilter und Fortschritt helfen bei großen Websites.
- Echte Sprach-URLs und hreflang-/Sitemap-Signale nach Veröffentlichung prüfen.

41. Vollbackup erstellen

Die aktuelle Oberfläche erstellt ein normales ZIP ohne Backup-Passwort und ohne Archivverschlüsselung.

- 1 Backups öffnen und prüfen, ob die CMS-Datenbank erkannt und lesbar ist.
- 2 Backup erstellen oder Neues Backup erstellen wählen.
- 3 Den Auftrag bis zum Abschluss verfolgen; die Verarbeitung läuft in fortsetzbaren Serverabschnitten.
- 4 Datum, ZIP-Größe, Dateianzahl, Datenbanktabellen und eventuelle Warnungen prüfen.
- 5 Die ZIP herunterladen, extern aufbewahren und die Sicherung kontrollieren.

Die Anzeige entscheidet über den Sicherungsumfang

Wird die Datenbank als nicht enthalten gemeldet, enthält die ZIP nur den tatsächlich gesicherten Dateistand. Kurzlebige oder nicht lesbare Einträge können übersprungen werden; dazu zeigt die Oberfläche einen Hinweis. Prüfe, ob diese Einträge für eine Wiederherstellung relevant sind.

ZIP geschützt aufbewahren

Die ZIP kann Datenbankinhalte, Konfiguration und personenbezogene Daten enthalten. Lege sie an einem geschützten Ort ab. Das Kontopasswort bei einer späteren Wiederherstellung bestätigt deine Berechtigung; es verschlüsselt das ZIP nicht.

Gespeicherte Generationen und ihre Aufbewahrung beschreibt Kapitel 44.

42. Backup-Inhalt und Konsistenz

Prüfe vor einer Wiederherstellung, was das konkrete Archiv tatsächlich enthält.

- Website-Dateien einschließlich unterstützter versteckter Dateien.
- Erkannte und lesbare CMS-Datenbanktabellen; fehlgeschlagene Datenbankaufnahme wird angezeigt.
- Sicherungsinformationen zur Zuordnung von Zeitpunkt, Umfang und Prüfergebnis.
- Konsistente Behandlung lokaler SQLite-Daten statt unkontrollierter Kopie laufender Datenbanken.
- Hinweise auf übersprungene, veränderte oder nicht lesbare Dateien.

Sicherung beurteilen

Ein großes ZIP ist kein Beweis für Vollständigkeit. Vergleiche die erwarteten Dateien und Datenbanken mit der Zusammenfassung. Eine kleine WordPress-Website kann durch Medien, alte Archive oder Hosting-Dateien ein großes Backup erzeugen.

Vorhandenes Archiv nicht vorschnell löschen

Lade die neue Sicherung vollständig herunter und prüfe sie, bevor du die letzte unabhängige Rückfallebene entfernst. Wiederherstellung möglichst zunächst an einer getrennten Testinstallation erproben.

Kopiere bei einer manuellen Serverdiagnose SQLite-Dateien samt offenen Journals nicht wahllos hin und her. Für eine Rücksicherung den vorgesehenen Backup- und Restore-Weg verwenden.

43. Wiederherstellung und Umzug

Die Wiederherstellung ersetzt vorhandene Website-Dateien und gegebenenfalls die enthaltenen WordPress-Tabellen.

- 1 Zielinstallation und aktuelle Website extern sichern.
- 2 Unter Backups ein gespeichertes Backup wählen oder die Site-Control-ZIP hochladen.
- 3 Bei lokaler Anmeldung mit dem eigenen Site-Control-Kontopasswort bestätigen. Das ZIP selbst braucht kein Passwort.
- 4 Bei Fernverwaltung die Wiederherstellung anfordern; der Kunde bestätigt sie in seiner lokalen Anmeldung.
- 5 Prüfung und Wiederherstellung abwarten, danach Website und Zugang testen.

Was dabei erhalten bleibt

Die laufende Site-Control-Installation bleibt auf ihrer aktuell installierten Version, damit die Steuerung während der Wiederherstellung weiterläuft. Ein Website-Backup ist deshalb kein Downgrade-Paket für die Anwendung.

Bei einem Umzug zusätzlich prüfen

Domain, Pfade, WordPress-URLs, Permalinks, Datenbankzugang, HTTPS und Serverregeln müssen zur Zielumgebung passen. Eine ZIP auf einem anderen Server einzuspielen ersetzt diese Prüfungen nicht.

Abnahme

Login, wichtige Seiten, Medien, Kontaktformulare, Stellen, Bewerbungsweg, Consent und Tracking testen. Bei Warnungen den Auftrag und die Sicherungskennung dokumentieren.

44. Backup-Historie und Aufbewahrung

Mehrere gespeicherte Sicherungen bieten Rückfallmöglichkeiten für unterschiedliche Zeitpunkte.

- 1 Unter Gespeicherte Backups Datum, Größe und Kennzeichnung des aktuellen Backups vergleichen.
 - 2 Über ZIP herunterladen eine bestimmte Generation extern sichern.
 - 3 Backups behalten auf die gewünschte Anzahl setzen und speichern.
 - 4 Vor einer Löschung prüfen, ob eine unabhängige und nutzbare Sicherung vorhanden ist.
- Standardmäßig bleiben die letzten drei Backups erhalten.
 - Die sichtbare Auswahl erlaubt eine bis zehn Generationen.
 - Ältere Generationen werden entsprechend der Aufbewahrung bereinigt; die Bestätigung im Dialog beachten.
 - Einzelne Generationen lassen sich gezielt herunterladen, wiederherstellen oder löschen.

Vorhandene Automatisierungen

Bei älteren Installationen können eingerichtete Cron-Aufrufe weiter bestehen. Prüfe deren tatsächliche Konfiguration und Ergebnisse separat. Der aktuelle Standardablauf erfolgt über die sichtbare Backup-Oberfläche; eine tägliche Sicherung ist nicht allein durch die Installation garantiert.

45. Module Store, Kauf und Stripe

Module, Testphase und Lizenzpakete werden pro Installation verwaltet.

- 1 Module öffnen und Store oder Meine Lizenzen wählen.
 - 2 Vorhandene Freigaben prüfen; bei Bedarf Lizenzstatus aktualisieren.
 - 3 Ein Einzelmodul oder All Modules und Agentur mit passender Lizenzanzahl auswählen.
 - 4 Monatliche oder jährliche Abrechnung wählen und den bestätigten Preis im Checkout prüfen.
 - 5 Nach dem Kauf zur Installation zurückkehren und Freischaltung prüfen.
- WordPress: 4,99 USD pro Monat oder 49,99 USD pro Jahr.
 - WordPress ist bereits in All Modules und Agentur enthalten.
 - Agentur ist ausschließlich jährlich buchbar.
 - Aktivierungscode und Vorhandene Käufe wiederherstellen helfen bei der Zuordnung bestehender Lizenzen.
 - Abonnements verwalten öffnet das Kundenportal für Rechnungen, Zahlungsdaten und Kündigung.

Test und Kauf sind getrennt

7 Tage kostenlos testen startet kein automatisches Abo. Gewünschte Module selbst kaufen. Käufe und Abrechnung erfolgen über die lokale Website-Anmeldung; eine Fernverwaltung ersetzt diese Anmeldung nicht.

46. Module und Preise

Preisstand 08.09.2026. Beträge in USD je Installation, ggf. zzgl. anfallender Steuern.

Funktion / Paket	Monat	Jahr
Free Core + Website Essentials	Free	Free
WordPress	4,99	49,99
Tracking & Analytics	7,99	79,99
Spam Protection	4,99	49,99
Google Search Console	4,99	49,99
Translations / Übersetzungen	7,99	79,99
Backup & Migration	7,99	79,99
Datenschutz	7,99	79,99
Stelleninserate / Jobs & Bewerbungen	4,99	49,99
All Modules Bundle	24,99	249,99
Agentur / White Label + Multi-Site	-	69,99
AI Website Audit	nach Verbrauch	Credits / BYOK

Jahrespakete nach Lizenzanzahl

Lizenzen	All Modules / Jahr	Agentur / Jahr
1	249,99	69,99
5	349,99	99,99
25	599,99	199,99
50	749,50	249,50

Ab 50 Lizenzen: 14,99 USD je All-Modules-Lizenz und 4,99 USD je Agentur-Lizenz im Jahr.
Mengenpreise gelten für die beiden Pakete; ihre Kontingente werden getrennt geführt.

Paketumfang

All Modules umfasst alle kostenpflichtigen Funktionsmodule einschließlich WordPress. Agentur und AI-Credits sind separat. Agentur beinhaltet WordPress, White Label und Kundenverwaltung.
AI-Nutzung ist auch während der Testphase separat kostenpflichtig.

47. AI Website Check

Der AI Website Audit verbindet technische Bestandsaufnahme mit einer nachvollziehbaren Auswertung.

- 1 Website bzw. URL-Liste und gewünschten Prüfumfang festlegen.
- 2 Verarbeitungsweg und Kostenschätzung prüfen.
- 3 Audit starten und Crawl-, Analyse- und Berichtsstatus verfolgen.
- 4 Management Summary, Prioritäten und systemische Befunde lesen.
- 5 Belegstellen, Beispiel-URLs und eingeschränkte Teilbereiche kontrollieren.
- 6 PDF exportieren und bei Bedarf den Audit-Chat zum gespeicherten Kontext nutzen.

Was der Bericht enthalten kann

- Management Summary mit Einordnung und nächsten Maßnahmen.
- Audit-Matrix, priorisierte Roadmap und ausdrücklich erhaltenswerte Stärken.
- Systemische Befunde mit Wirkung, Maßnahme, Beispiel-URLs und Evidence-Bezügen.
- Technische Methodik, Abdeckung, verfügbare visuelle Analysen und GSC-Status.

Abdeckung mitlesen

Ein Bericht über eine einzelne Startseite ist keine vollständige Prüfung aller Unterseiten. Ein nicht verfügbarer Bereich wird als Lücke behandelt. Kapitel 76 erklärt, wie du den Bericht bewertest.

48. AI Credits und BYOK

AI-Nutzung wird separat abgerechnet; ein Modulabo oder Test ersetzt kein AI-Guthaben.

Modus	Bedeutung
VELUNO Credits	Verwaltete Verarbeitung nach Verbrauch. Guthaben hat kein Ablaufdatum; kein automatisches Aufladen.
BYOK	Eigener API-Schlüssel und Abrechnung über den jeweiligen Providerzugang.

- Vor einem Lauf die Kostenschätzung und den Prüfumfang ansehen.
- Ein eigener Schlüssel wird geprüft und geschützt gespeichert; niemals in Screenshots oder Supportnachrichten teilen.
- Der AI-Status kann für einzelne Teilbereiche unvollständig sein. Ergebnisse und Verbrauch gemeinsam prüfen.
- Ein Bericht mit 0 VELUNO Credits im BYOK-Modus bedeutet nicht, dass der Provider den Lauf kostenlos ausgeführt hat.

Berichte sind Zustandsaufnahmen

Crawl, Technik, Inhalte und Drittanbieter können sich später ändern. Für den Vergleich erneute Läufe mit bewusst gewähltem Umfang durchführen.

49. Agentur und White Label einrichten

Agentur bündelt White Label, Kundenverwaltung und WordPress für 69,99 USD pro Jahr bei einer Lizenz.

- 1 Agentur im Module Store aktivieren oder eine vorhandene Paketlizenz zuordnen.
 - 2 Lizenzstatus aktualisieren und die Freischaltung prüfen.
 - 3 In den Einstellungen eigenen Namen und Logo für White Label hinterlegen.
 - 4 Login, Dashboard und einen neu erstellten AI-Bericht prüfen.
 - 5 Kundeninstallationen über den vorgesehenen Freigabeweg verbinden; siehe Kapitel 74.
- All Modules und Agentur sind getrennte Pakete mit eigenen Lizenzkontingenten.
 - Die Agentur-Zentrale benötigt Agentur für die Fernverwaltung.
 - Für White Label direkt auf einer Kundenwebsite benötigt auch diese Installation eine Agenturlizenz.
 - Kundenwebsites benötigen die jeweils passenden Modulfreigaben.
 - Bereits erzeugte PDFs werden durch spätere Branding-Änderungen nicht rückwirkend verändert.

Kundenfreigabe

Die Agentur arbeitet nur in freigegebenen Installationen. Eine Lizenzzuteilung und eine Verbindungsfreigabe sind bewusst zu prüfen; bestehende eigene Kundenkäufe bleiben getrennt.

50. Benutzer und Rollen

Es gibt nur Administrator und Mitarbeiter.

Originale Site-Control-Oberfläche mit neutralen Beispieldaten.

Rolle	Rechte
Administrator	Alle aktuellen und künftigen Site-Control-Bereiche und Aktionen
Mitarbeiter	Nur ausdrücklich freigegebene Bereiche; Menü und Serveraktionen sind begrenzt

- 1 Benutzer & Freigaben öffnen.
- 2 Name, E-Mail und Passwort eintragen.
- 3 Rolle wählen.
- 4 Bei Mitarbeiter nur benötigte Bereiche markieren.
- 5 Speichern und Zugang in einem privaten Browser testen.

Prinzip der geringsten Rechte

Mitarbeiter nur für die tatsächliche Aufgabe freischalten. Module Store, Benutzer, Backups, Updates und Einstellungen nur an vertrauenswürdige Administratoren geben.

51. Einstellungen

Systemweite Werte werden an einer zentralen Stelle verwaltet.

- Website-Name und Basiswerte
- White-Label-Name und Logo bei aktivem Modul
- Reverse Proxy und Besucher-IP
- Automatische Datenaufbewahrung
- Nach-oben-scrollen-Button
- Support-Link und Supportangaben
- Dashboard- und Kontoeinstellungen

Reverse Proxy

Cloudflare wird automatisch erkannt. Andere Proxies nur über echte Proxy-IP oder enges CIDR-Netz freigeben. Eine zu breite Freigabe ermöglicht gefälschte Besucher-IPs.

52. Updates direkt installieren

Site Control weist auf neue Versionen hin. Die Installation startest du bewusst.

- 1 Update-Hinweis in der Übersicht oder den Bereich Updates öffnen.
 - 2 Mit Erneut prüfen den aktuellen Stand abrufen.
 - 3 Versionsnummer und Release-Hinweise lesen.
 - 4 Update sicher installieren wählen und Paketprüfung sowie Sicherung abwarten.
 - 5 Ergebnis und Update-Verlauf prüfen.
 - 6 Login, öffentliche Website und betroffene Module testen.
- Die Suche nach Updates installiert noch kein Update.
 - Pakete werden auf Signatur, Version und Inhalt geprüft.
 - Konfiguration und lokale Nutzdaten werden nicht durch eine frische Standardkonfiguration ersetzt.
 - Der manuelle ZIP-Weg bleibt für den Fall verfügbar, dass der direkte Abruf nicht gelingt.

Fehler nicht überspringen

Bei Signaturfehlern oder unvollständigen Paketen die Installation nicht erzwingen. Meldung und Sicherungskennung notieren, offizielle ZIP und Systemvoraussetzungen prüfen.

53. Manuelles ZIP-Update und Rückfall

Der alte Upload-Weg bleibt als eingeklappter Fallback vorhanden.

- Nur vollständige Pakete bis zur angezeigten Maximalgröße verwenden.
- Das ZIP darf den Ordner site-control enthalten oder direkt dessen Inhalt.
- Konfiguration, Anfragen, Tracking und Zugangsdaten im Datenordner werden nicht überschrieben.
- Vor jeder Änderung wird eine vollständige Programmsicherung angelegt.
- Bei Fehlern Meldung und Sicherungskennung dokumentieren.

54. Datenschutz und lokale Datenspeicherung

Die tatsächlich gespeicherten Daten hängen von aktivierten Funktionen und deren Nutzung ab.

Bereich	Typische Daten
Konfiguration	Website, Benutzer, Rechte, Module, Consent, Styling und Aufbewahrung
Formulare	Ausdrücklich übernommene Inhalte und Versandstatus
Tracking	Technische Ereignisse, Browserkennungen, Sitzungen und Tageswerte
Consent / Spam	Nachweise, Kategorien, Versionen, Scores und technische Gründe
Stelleninserate	Unternehmensdaten, Stellen, Bewerbungen, Status, Notizen und geschützte Anhänge
AI	Auditkontext, technische Belege und exportierbare Berichte
Backups	Kopien von Website-Dateien und enthaltenen Datenbanken

Aufbewahrung und Berechtigungen je Bereich kontrollieren. Bewerbungen haben eigene Fristen; die Löschung umfasst ihre Anhänge. Eine exportierte CSV oder ein heruntergeladenes Backup wird nicht dadurch entfernt, dass die Quelldaten in Site Control gelöscht werden.

Lokale und externe Verarbeitung unterscheiden

Die Anwendung läuft auf dem eigenen Hosting. Aktivierte externe Dienste, E-Mail-Versand, AI-Provider, Google und Lizenzdienste können Verbindungen nach außen erfordern. Die Konfiguration und die Website-Datenschutzhinweise müssen den tatsächlichen Einsatz abbilden.

55. Sicherheitsmodell

Mehrere Schutzschichten verhindern unbemerkte oder unsichere Änderungen.

- CSRF-Schutz für zustandsändernde Dashboard-Aktionen
- Serverseitige Rollen- und Aktionsprüfung
- Signierte Updatepakete und Inhaltsmanifest
- Atomare Schreibvorgänge und Dateisperren
- Originaldateien und Konfliktschutz im Inhaltseditor
- Verschlüsselung sensibler Geheimnisse
- Datenordner per Serverregeln geschützt
- Backup-Prüfsummen und transaktionale Wiederherstellung
- Fail-closed bei unsicherer SQLite-Sicherung

56. WordPress-Besonderheiten

Site Control ergänzt WordPress und respektiert dessen Inhalte, Plugins und Theme-Struktur.

- Die MU-Bridge bindet die öffentliche Runtime ein; Site Control selbst bleibt unter /site-control/.
- Unterstützte WordPress-Seiten und SEO-Angaben werden aus der passenden Quelle importiert.
- Dynamische Builder-Inhalte sind nicht automatisch wie statische HTML-Dateien bearbeitbar.
- Formulare können beim Scan oder erst zur Laufzeit erkannt werden.
- Caching, Script-Delay und Minifizierung nach relevanten Änderungen prüfen.
- Die WordPress-Verwaltung für Updates, Plugins und Themes beschreibt Kapitel 67.

Nach Änderungen kontrollieren

Seitenzahl und Scanbestand prüfen, betroffene Seiten ohne Cache aufrufen und SEO-Daten mit dem ausgelieferten Quelltext vergleichen. Ein funktionierender WordPress-Frontend-Aufruf beweist weder einen funktionierenden Site-Control-Login noch verfügbare SQLite-Erweiterungen.

Bei HTTP 500

Den Zeitpunkt und die konkrete Aktion dokumentieren. PHP-/Webserver-Log, Dateirechte, freien Speicher und installierte Version prüfen. Keine lokalen Site-Control-Datenbanken löschen, um einen Fehler zu verdecken. Kapitel 77 hilft bei der Einordnung.

57. Klassische HTML-/PHP-Websites

Site Control funktioniert auch ohne WordPress, wenn der Renderer erreichbar ist.

- Runtime wird direkt oder über den gemeinsamen PHP-Renderer eingebunden.
- Statische HTML-Elemente können sicher erfasst und bearbeitet werden.
- Eigene PHP-Formularhandler können die Spam-Bridge serverseitig aufrufen.
- Formulare können über data-Attribute oder Runtime-Struktur erkannt werden.
- Bei eigenen Routern müssen /site-control/ und Endpunkte ausgenommen sein.
- SPA-Routenwechsel werden nur bei tatsächlicher URL-Änderung als Pageview gezählt.

58. Fehlerbehebung: Banner oder Werkzeuge fehlen

Wenn Cookie-Banner, Styling oder Barrierefreiheit auf allen Seiten fehlen, zuerst die Runtime prüfen.

- 1 Öffentliche Seite ohne eingeloggten Cache in privatem Fenster öffnen.
- 2 Browserkonsole und Netzwerk auf runtime.js.php bzw. Site-Control-Endpunkte prüfen.
- 3 Tracking & Diagnose oder Website-Scan auf Runtime-Abdeckung prüfen.
- 4 WordPress-, Server-, CDN- und Optimierungscaches leeren.
- 5 Lesbare Dashboard-URL und index.php?view=... getrennt testen.
- 6 Consent-Modus, Werkzeugschalter und Mitarbeiterrechte prüfen.

Nicht sofort neu installieren

Eine Neuinstallation kann die Ursache verdecken. Erst Endpunkt, Serverrouting, Bridge und Caches dokumentieren.

59. Fehlerbehebung: Formular nicht erkannt

Ein sichtbares Formular kann dynamisch erzeugt oder vom Scan ausgeschlossen sein.

- | | |
|---|---|
| 1 | Website neu scannen. |
| 2 | Betroffene Seite ohne Cache öffnen und Formular vollständig laden. |
| 3 | Formular-Registry unter Forms & Schutz prüfen. |
| 4 | Bei Divi sicherstellen, dass der Kontaktformular-Shortcode im gespeicherten Builder-Inhalt existiert. |
| 5 | Bei AJAX/Plugin-Formularen einen echten Submit ausführen und Laufzeiterkennung prüfen. |
| 6 | Login-, Suche-, Warenkorb- und Checkout-Ausschlüsse berücksichtigen. |
| 7 | Erfolgs- und Fehlerselektoren ergänzen, wenn der Funnel Unknown zeigt. |

60. Fehlerbehebung: Tracking zeigt null oder andere Werte

Null kann korrekt sein, obwohl die Website Aufrufe hatte.

- Analyse-Einwilligung wurde nicht erteilt.
- DNT oder GPC ist aktiv.
- Besuch stammt von Bot, Monitoring oder Headless-Browser.
- Runtime fehlt auf der Seite.
- Endpunkt wird durch Firewall, Cache, CSP oder Adblocker blockiert.
- Zeitraum 14/28 Tage enthält keine erlaubten Events.
- GA4 verwendet andere Consent-, Filter- oder Identifikationsregeln.

- | | |
|---|--|
| 1 | Endpunkt & Speicher testen. |
| 2 | Private Sitzung ohne DNT/GPC und mit Analyse-Einwilligung verwenden. |
| 3 | Einmal Startseite und zwei weitere Routen besuchen. |
| 4 | Letzten Pageview, Runtime und Endpunktstatus prüfen. |

61. Fehlerbehebung: Fonts

Font-Fundstellen, lokale Dateien und Browseraufrufe sind drei verschiedene Ebenen.

- Erneut scannen und gruppierte Anbieter öffnen.
- Unvollständige URLs oder Platzhalter nicht automatisch übernehmen.
- HTTP-Status und tatsächlichen Content-Type der Quelle prüfen.
- Bei geschütztem Adobe-/Theme-Asset Lizenz und Abrufweg beachten.
- Manuellen Upload mit korrekter Familie, Gewicht und Stil nutzen.
- Nach lokaler Übernahme Website und Browsernetzwerk prüfen.
- Quellcode-Pfad nicht auflösbar ist kein sicherer Beleg für eine fehlende sichtbare Schrift.

62. Fehlerbehebung: Updates und Backups

Bei sicherheitsrelevanten Vorgängen ist Abbruch besser als ein halbfertiger Zustand.

- Direktes Update erneut prüfen; kurzlebiger Link kann abgelaufen sein.
- Serverzeit, HTTPS, cURL und ausgehende Verbindung kontrollieren.
- Signaturfehler niemals umgehen.
- Bei ZIP-Problemen ZipArchive und Uploadgrenzen prüfen.
- Bei Backupfehlern freien Speicher, Schreibrechte und Datenbanktreiber prüfen.
- Audience-SQLite ohne PDO-SQLite wird bewusst nicht unsicher kopiert.
- Sicherungskennung und genaue Meldung für Support notieren.

63. Betriebskalender

Kurze, feste Routinen verhindern stille Fehler.

Rhythmus	Kontrolle
Nach Änderungen	Website-Scan, Cache, Consent, Formulare und betroffene Seiten testen
Wöchentlich	Formularfunnel, Spam-Logs, Trackingdiagnose und Fehlerlinks prüfen
Monatlich	Benutzer, Module, Updates, Retention, GSC und Backupstatus prüfen
Vor Update	Externes Backup, Release-Hinweise, Speicherplatz und Wartungsfenster
Nach Update	Login, Runtime, Banner, Formulare, Tracking, Frontend und Cron testen
Vierteljährlich	Restore-Test, Rollenprüfung, Datenschutztexte und Datenfristen

64. Checkliste für einen sauberen Produktivstart

Prüfe die aktivierten Funktionen mit echten Abläufen.

- Dashboard und Website-Datenblatt zeigen einen plausiblen Bestand.
- Wichtige Seitentypen sind mit der Runtime verbunden.
- Lesbare Dashboard-URLs und öffentliche Website funktionieren.
- Cookie-Kategorien, Dienste und Datenschutz-URL passen zusammen.
- Mindestens ein Formular inklusive Erfolgs- und Fehlerfall wurde getestet.
- Tracking wurde mit passender Einwilligung und aktivem Modul geprüft.
- Mitarbeiterrechte wurden in einer getrennten Sitzung kontrolliert.
- Backupumfang, externe Kopie und Wiederherstellungsweg sind bekannt.
- Bei WordPress: ein abgesicherter Update- und Rückfallweg ist festgelegt.
- Bei Jobs: Unternehmen, Bewerbungsweg, Versand, Einwilligung und Anhänge sind geprüft.
- Bei Agentur: Kundenfreigaben und Lizenzzuteilungen stimmen.
- Testfrist und gewünschte Käufe sind vor Fristende geklärt.

Verantwortlichkeiten

Zugänge, Ansprechpartner und Betriebsabläufe geschützt dokumentieren. Die Verantwortung für heruntergeladene Backups, CSV-Dateien und Bewerbungsunterlagen bleibt auch außerhalb von Site Control bestehen.

65. Glossar

Die wichtigsten Begriffe für den Alltag.

Begriff	Erklärung
Free Core	Kostenlose Basis der Anwendung; Website Essentials ergänzt die kostenlosen Website-Werkzeuge.
Modulfreischaltung	Bestätigte Berechtigung zur Nutzung eines kostenpflichtigen Moduls (Entitlement).
Agentur	Paket mit White Label, Kundenverwaltung und WordPress.
All Modules	Paket der kostenpflichtigen Funktionsmodule; Agentur und AI separat.
White Label	Eigene Marke bei aktiver Agenturfreischaltung.
BYOK	Bring Your Own Key: Nutzung eines eigenen API-Schlüssels.
Evidence / Coverage	Technischer Beleg / tatsächlich geprüfter Umfang eines Audits.
Consent	Gespeicherte Einwilligungsentscheidung.
DNT / GPC	Vom Browser übermittelte Datenschutzsignale.
Pageview / SPA	Seitenaufruf / Website mit Navigation ohne vollständiges Neuladen.
Retention	Aufbewahrungs- und Löschrufen.
Runtime	Site-Control-Code auf öffentlichen Website-Seiten.
SQLite / WAL	Lokaler Datenbankspeicher / begleitendes Schreibjournal.

66. Support richtig vorbereiten

Gute Informationen verkürzen die Diagnose erheblich.

- Site-Control-Version und Installations-ID
- Website-Typ und betroffene öffentliche URL
- Exakter Zeitpunkt und Zeitzone
- Genaue Meldung als Text, nicht nur als Ausschnitt
- Browser, Gerät und privates Fenster ja/nein
- Letzte Änderung an Theme, Plugin, Server, CDN oder Consent
- Runtime-, Endpunkt- und Scanstatus
- Update- oder Backup-Sicherungskennung
- Reproduktionsschritte und erwartetes Ergebnis

Keine Geheimnisse senden

Keine Passwörter, API-Keys, vollständigen Backup-Passwörter, Datenbankzugänge oder privaten Lizenz-/Installations-Token in eine normale Supportnachricht kopieren.

Technischer Support ist direkt in Site Control unter Hilfe & Support erreichbar.

67. WordPress, Plugins und Themes

WordPress-Modul: 4,99 USD pro Monat oder 49,99 USD pro Jahr; in All Modules und Agentur enthalten.

- 1 WordPress öffnen und Updates prüfen wählen.
 - 2 Versionen, verfügbare Updates und Aktivierungsstatus ansehen.
 - 3 Einzelne oder sichtbare Einträge auswählen.
 - 4 Aktualisieren, Aktivieren oder Deaktivieren wählen, soweit für den Eintrag verfügbar.
 - 5 Auswahl prüfen und die Aktion bewusst starten.
 - 6 Ergebnis sowie WordPress-Frontend und Admin-Zugang kontrollieren.
- Themes werden aktiviert; das aktive Theme benötigt einen funktionsfähigen Ersatz, wenn gewechselt wird.
 - Plugin-Aktivierung und -Deaktivierung können sichtbare Funktionen und Formulare verändern.
 - Sammelaktionen zeigen die gewählten Einträge vor dem Start.
 - Aufträge lassen sich nach der laufenden Aktion pausieren und später fortsetzen; wartende Aktionen können abgebrochen werden.

Sicherungsgrenze

Vor Änderungen sichert Site Control betroffene Dateien und Aktivierungen. Plugin-eigene Datenbankänderungen werden damit nicht zurückgesetzt. Für ein vollständiges Rückfallkonzept Website und Datenbank separat sichern.

68. WordPress-ZIP-Updates und Rückfall

Mit einer passenden Plugin- oder Theme-ZIP lässt sich eine installierte Komponente aktualisieren.

- 1 WordPress → Update aus einer ZIP öffnen und ZIP auswählen.
- 2 Erkannten Pakettyp, Komponente und Version prüfen.
- 3 Bei Agentur die passenden freigegebenen Websites und übersprungenen Ziele prüfen.
- 4 Auswahl bestätigen und Jetzt ausführen wählen.
- 5 Status jeder Aktion ansehen und Website testen.

Die ZIP dient zum Aktualisieren einer passenden installierten Komponente. Sie ist nicht mit der vollständigen Site-Control-Update-ZIP oder einer Website-Backup-ZIP gleichzusetzen.

Nach einem fehlgeschlagenen Auftrag

Ergebnis und verfügbare Wiederherstellung prüfen. Site Control kontrolliert nach einer Änderung, ob WordPress startet. Nutze den vorgesehenen Rückfallweg und dokumentiere verbleibende Fehler. Datei-Rückfall allein entfernt keine bereits erfolgten Datenbankänderungen eines Plugins.

Beim Verlassen der Ansicht

Die laufende Aktion wird beendet. Weitere Websites warten gegebenenfalls auf Fortsetzen. Verlasse dich nicht auf eine Hintergrundausführung aller noch wartenden WordPress-Aktionen.

69. Unternehmen für Stelleninserate

Die Unternehmensdaten werden von Stellenanzeigen und Bewerbungsabläufen verwendet.

- 1 Stelleninserate → Unternehmen öffnen.
 - 2 Unternehmen anlegen oder einen bestehenden Eintrag bearbeiten.
 - 3 Name eintragen und bei Bedarf Logo, Website, Kontakt und Adresse ergänzen.
 - 4 Datenschutz-URL und Impressum-URL prüfen.
 - 5 Absendername und gegebenenfalls eigenen Text der Eingangsbestätigung ergänzen.
 - 6 Unternehmen speichern und in einer Stellenanzeige auswählen.
- Pflichtfelder tragen ein *. Felder ohne Stern sind freiwillig.
 - Logo: PNG, JPG, GIF oder WebP, maximal 3 MB und 5000 × 5000 Pixel.
 - Website und Karriere-E-Mail erscheinen ohne die Zusätze empfohlen oder optional.
 - Eine Datenschutz-URL ermöglicht den verlinkten Platzhalter im Einwilligungstext.
 - Ein Logo lässt sich über Vorhandenes Logo entfernen gezielt entfernen.

Vor Veröffentlichung

Unternehmensname, Kontaktweg und Datenschutzlink im öffentlichen Formular kontrollieren. Eine leere freiwillige Eingabe ist keine zusätzliche Veröffentlichungsanforderung.

70. Stellen anlegen und veröffentlichen

Das Modul Stelleninserate / Jobs & Bewerbungen kostet 4,99 USD monatlich oder 49,99 USD jährlich.

- 1 Stelleninserate → Stellen → Neue Stelle öffnen.
 - 2 Titel, Slug und Unternehmen sowie die als Pflicht markierten Angaben ausfüllen.
 - 3 Beschreibung, Standort, Arbeitszeit und Arbeitsort ergänzen.
 - 4 Status, Veröffentlichungszeitraum und gegebenenfalls sichtbare Gehaltsangaben setzen.
 - 5 Bewerbungsweg auswählen: lokales Formular, externer Link, E-Mail-Kontakt oder keine Bewerbung.
 - 6 Speichern und öffentliche Detailseite sowie die Einbettung testen.
- Stellen lassen sich suchen, filtern, duplizieren und archivieren.
 - Der öffentliche Basis-Slug ist unter Einbindung & Einstellungen konfigurierbar; Standard ist jobs.
 - Besteht am Basispfad bereits eine CMS-Seite, kann sie als Übersicht erhalten bleiben; Site Control ergänzt die Detailseiten.
 - JobPosting-Daten, Sitemap und Feed unterstützen die technische Veröffentlichung, garantieren aber keine Aufnahme durch Google.

Empfänger prüfen

Kontakt-E-Mail, internen Empfänger und Standard-Empfänger unterscheiden. Für das lokale Formular müssen E-Mail-Versand und Einwilligung richtig eingerichtet sein.

71. Bewerbungen und Anhänge bearbeiten

Bewerbungsdaten werden geschützt in der Installation verarbeitet und über berechnigte Konten verwaltet.

- 1 Stelleninserate → Bewerbungen öffnen.
 - 2 Nach Stelle, Unternehmen, Zeitraum oder Status filtern.
 - 3 Bewerbung öffnen und Angaben sowie Anhänge prüfen.
 - 4 Status und interne Notizen pflegen.
 - 5 Bei Bedarf die gefilterte Übersicht als CSV exportieren.
 - 6 Aufbewahrungsfrist kontrollieren und Fristen jetzt prüfen bei Bedarf ausführen.
- Unter Einbindung & Einstellungen kann die Annahme lokaler Bewerbungen ein- oder ausgeschaltet werden.
 - Die Aufbewahrung ist von 1 bis 3650 Tagen einstellbar; Standard sind 180 Tage.
 - Die fristbedingte Bereinigung schließt zugehörige Anhänge ein.
 - Das öffentliche Formular erlaubt PDF, DOC, DOCX oder ODT: maximal fünf Dateien, je 8 MB und zusammen 20 MB.

Funktionsprüfung

Eine eigene Testbewerbung absenden und Formularmeldung, E-Mail, Eintrag und Dateizugriff prüfen. Eine erfolgreiche E-Mail allein belegt nicht den gesamten Ablauf. Exportierte Dateien unabhängig von der Anwendung geschützt verwalten.

72. Jobs einbetten und gestalten

Stelleninserterate → Einbindung & Einstellungen steuert öffentliche Stellenlisten und Detailseiten.

- 1 Den angezeigten CMS-neutralen Einbettungscode kopieren.
- 2 In einen passenden HTML-/Code-Bereich der Karriereseite einfügen, etwa in WordPress oder Divi.
- 3 Rückweg zur Karriereseite, öffentlichen Basispfad und Such-/Filterverhalten prüfen.
- 4 Unter Farben & Darstellung die gewünschten Farben wählen und speichern.
- 5 Karriereseite und Stellen-Detailseite neu laden und auf Desktop sowie Mobil prüfen.

Einstellung	Wirkung
Unternehmensname	Eigene Farbe für die Unternehmensbezeichnung
Button-Hintergrund / Button-Text	Getrennte Farben für die Handlungsbuttons
Text / Sekundärtext	Haupttext und ergänzende Angaben
Hintergrund / Karten / Rahmen	Flächen und Begrenzungen
Radius	Rundung innerhalb des erlaubten Bereichs

Die Farben gelten für öffentliche Stellenanzeigen und die eingebettete Liste. Suche und Filter können automatisch ab vier Stellen, immer oder nie erscheinen.

Datenschutztext

Der Platzhalter {datenschutz} wird mit der beim Unternehmen hinterlegten URL verlinkt. Der Satz bleibt zusammenhängender Text neben der Checkbox. Pflichtfelder tragen einen Stern.

73. Stellen und Bewerbungen als CSV

Stellenimport und Bewerbungsexport haben unterschiedliche Aufgaben.

Stellen übertragen oder gesammelt ändern

- 1 Unter Stellen zunächst CSV exportieren.
- 2 Die exportierten Spalten und das Semikolon als Trennzeichen beibehalten.
- 3 Vorhandene IDs zum Aktualisieren unverändert lassen; eine leere ID legt eine neue Stelle an.
- 4 Felder wie Unternehmen, Status, Bewerbungsweg und Datumsangaben prüfen.
- 5 CSV importieren und die Rückmeldung sowie betroffene Stellen kontrollieren.

Bewerbungen exportieren

Unter Bewerbungen passende Filter setzen und CSV exportieren wählen. Der Export dient der Weiterverarbeitung der Übersicht. Er ersetzt weder die geschützten Originalanhänge noch ein vollständiges Backup.

Vor einem großen Import

Zuerst mit wenigen gezielten Änderungen arbeiten und Rückmeldung kontrollieren. Keine bestehenden IDs willkürlich verändern. CSV-Dateien können personenbezogene Daten enthalten und benötigen einen geschützten Ablageort.

74. Agentur-Zentrale und Lizenzpakete

Die Zentrale verbindet Websites, Freigaben und Lizenzen in einem gemeinsamen Arbeitsbereich.

- 1 Agentur auf der eigenen Installation aktivieren.
- 2 Kundeninstallation über den vorgesehenen Verbindungs- und Freigabeweg hinzufügen.
- 3 Bei Paketkäufen einen passenden Aktivierungscode für die Kundeninstallation bereitstellen.
- 4 Der Kunde löst den Code ein und bestätigt die angezeigte Freigabe.
- 5 In der Zentrale Website auswählen und die freigegebenen Bereiche nutzen.

Frage	Regel
Fernverwaltung	Agentur wird auf der Zentrale benötigt. Die Kundeninstallation muss die Verbindung freigeben.
White Label beim Kunden	Dafür braucht die Kundeninstallation selbst eine Agenturlizenz.
Module beim Kunden	Passende eigene Käufe oder zugeordnete Modul-/All-Modules-Freigaben sind erforderlich.
Lizenzkontingente	All Modules und Agentur zählen getrennt.
Freigabe widerrufen	Zugeordnete Agenturfreigabe endet und der betreffende Platz wird frei; eigene Kundenkäufe bleiben erhalten.

Wiederherstellung aus der Ferne

Die Agentur kann eine Wiederherstellung anfordern. Der Kunde bestätigt sie in seiner lokalen Anmeldung. Sein Kontopasswort bleibt bei ihm.

75. Sieben Tage kostenlos testen

Alle Funktionsmodule inklusive Agentur lassen sich bewusst und ohne Kreditkarte ausprobieren.

- 1 Module Store öffnen und 7 Tage kostenlos testen wählen.
 - 2 Start und angezeigtes Ende der Testphase prüfen.
 - 3 Gewünschte Funktionen mit realistischen eigenen Testdaten ausprobieren.
 - 4 Benötigte Module oder Pakete vor Fristende selbst kaufen.
 - 5 Lizenzstatus prüfen, bevor mit wichtigen Moduldaten dauerhaft weitergearbeitet wird.
- Kein automatisches Abo und keine automatische Abbuchung aus dem bloßen Teststart.
 - AI-Credits bzw. BYOK-Verbrauch sind nicht kostenlos enthalten.
 - Die Testphase gilt einmal pro Lizenz, bei Free Core einmal pro registrierter Website.
 - Eine Neuinstallation setzt die Frist nicht zurück.

Nach Ablauf

Ungekaufte Testmodule werden gesperrt und ihre Moduldaten nach bestätigtem Lizenzabgleich gelöscht. Bei unklaren Zahlungen wird bis zur Klärung gewartet. Website, Free Core, Formulareingänge, veröffentlichte Schriftdateien und gekaufte Moduldaten bleiben erhalten.

Die Testdatenregel ist keine allgemeine Regel für regulär gekündigte Abonnements. Bewahre benötigte Exporte vor Ablauf geschützt auf und entscheide rechtzeitig über den Kauf.

76. AI-Auswertungen richtig lesen

Ein Audit zeigt belegte Beobachtungen und daraus abgeleitete Empfehlungen mit ihrem jeweiligen Prüfumfang.

- 1 Management Summary lesen: Zustand, Hauptprobleme, nächste Schritte und Grenzen.
- 2 Audit-Matrix und Roadmap nutzen, um Prioritäten zu ordnen.
- 3 Bei einem systemischen Befund Wirkung, Maßnahme und Beispiel-URLs prüfen.
- 4 Evidence-Bezüge und technische Methodik für die Nachvollziehbarkeit heranziehen.
- 5 Erhaltenswerte Stärken sowie Nicht-ändern-Hinweise berücksichtigen.
- 6 Offene Bereiche durch gezielte Folgeprüfungen ergänzen.

Umfang und Ergebnis nicht verwechseln

Ein Crawl über eine URL belegt Aussagen über diese Stichprobe. Er ist keine Prüfung aller Unterseiten. Fehlende GSC-Daten erlauben keine belegte Aussage über reale Rankings oder Nachfrage. Ein fehlgeschlagener visueller Teil ist keine erfolgreiche Designprüfung.

Beobachtung, Interpretation und Handlung

Eine technische Beobachtung, etwa mehrfach vorkommende Hauptüberschriften, ist vom abgeleiteten Verbesserungsvorschlag zu unterscheiden. Vor der Umsetzung die Fundstelle ansehen. Ein Product-Fit-Abschnitt ordnet passende Leistungen nach der Diagnose ein; er ersetzt keine Belege.

Maßnahmen kontrolliert umsetzen

Nicht jede Empfehlung verlangt einen Relaunch. Gute Bestandteile erhalten, konkrete Fehler prüfen und anschließend erneut messen. Ein exportierter Bericht beschreibt den Zustand zum Auditzeitpunkt.

77. Hosting-, Scan- und SQLite-Fehler

Eine funktionierende WordPress-Seite schließt einen Fehler in einer eigenständigen Site-Control-Funktion nicht aus.

Symptom	Gezielt prüfen
HTTP 500	Zeitpunkt, Aktion, PHP-/Webserver-Fehlerlog und installierte Site-Control-Version.
Unerwartet viele Seiten	Herkunft der Scan-Einträge; erkannte Hosting-Statistikberichte nach Update neu scannen.
Module nicht authentifiziert	Installation, Lizenzstatus und Verbindung zum Lizenzdienst; Token nicht öffentlich teilen.
SQLite / Transaktion	PDO-SQLite, Schreibrechte, freier Speicher und zusammengehörige Programmdateien.
Backup lädt langsam	Archivgröße und tatsächlichen Fortschritt prüfen; ein mehrgigabytegroßes ZIP kann lange übertragen werden.

Bei Datenbankfehlern

Aktuelle vollständige Version installieren und die konkrete Aktion erneut prüfen. Die SQLite-Korrekturen berücksichtigen unterschiedliche Treiberstände. Lokale Datenbanken, Journaldateien und Konfiguration nicht als pauschale Reparatur löschen. Für eine Wiederherstellung den vorgesehenen Sicherungsweg verwenden.

Speicherangaben richtig lesen

Eine Anzeige zu zugewiesenem Webspace kann Kontingente und nicht die tatsächliche Dateibelegung meinen. Belegung, Quota und freien Speicher für die betroffene Website getrennt prüfen. Weitergabe an den Hoster mit Zeitpunkt und Logmeldung ist aussagekräftiger als die Versionsnummer allein.