immoGenio

No. 02
April 2026

WHITELABEL

Whitelabel-Portal für Verwalter-Gruppen: Logo, Brand-Farben und Brief-Branding pro Tenant — AES-256-GCM für Provider-Credentials

Portal und Briefe unter eigener Marke ausgeben — Logo, Brand-Farben, Hide-Logo-Flag und AES-256-GCM-verschlüsselte Letter-Provider-Credentials pro Tenant.

AUTOR
ImmoGenio

VERÖFFENTLICHT
14. April 2026

ONLINE
www.immogenio.de/blog

— AUF EINEN BLICK

Inhalt

Vier Töchter, vier Logos, eine Software-Frage

Eine mittelgroße Verwalter-Gruppe aus Nordrhein-Westfalen betreut über vier regionale Tochterfirmen rund 11.000 Einheiten. Jede Tochter trägt einen eigenen Markennamen, ein eigenes Logo, eine eigene Mail-Domain, einen eigenen Briefkopf — und wirbt im Markt mit dieser regionalen Identität, weil Eigentümergemeinschaften lieber den lokalen Ansprechpartner sehen als die zentrale Holding. Bisher arbeiten alle vier Töchter auf vier getrennten Software-Instanzen ihrer alten Verwaltungs-Lösung, jede mit eigenem Datenbank-Server, eigenem Backup-Vertrag, eigenem Update-Termin. Die IT-Leitung der Gruppe verbringt einen erheblichen Teil ihrer Zeit damit, vier Systeme synchron zu halten, vier Migrations-Runden zu koordinieren und vier Audit-Berichte zu pflegen, deren Inhalte sich zu neunzig Prozent decken.

Bei der Software-Auswahl im Jahr 2026 lautet die Anforderung an den neuen Anbieter folgerichtig: Eine Plattform, eine Datenbank, eine Migration, ein Audit — aber vier Marken nach außen. Eigentümer und Mieter der Tochter A dürfen im Portal nichts sehen, was auf Tochter B hindeutet. Briefe gehen unter dem Logo der jeweiligen Tochter raus, von einer Mail-Absenderadresse der jeweiligen Tochter, optional sogar von einem Pingen-Account der jeweiligen Tochter. Genau diese Anforderung ist es, die das Wort „Whitelabel" in der Verwaltungs-Software konkret macht — und die ohne saubere Multi-Tenancy-Architektur nicht zu lösen ist.

Wenn ein Tenant nicht reicht: drei White-Label-Szenarien

Whitelabel-Branding pro Tenant ist kein Marketing-Feature, sondern eine Antwort auf drei Geschäftsmodelle, die in der Verwaltungs-Branche regelmäßig auftreten und die alle dasselbe technische Muster verlangen.

Verwaltungsgruppe mit regionalen Töchtern (B2B2B2C). Das einleitende Beispiel ist der häufigste Fall. Eine Holding hat über die Jahre regionale Verwaltungen aufgekauft, deren Marken in den jeweiligen Märkten etabliert sind. Die Holding möchte die etablierten Marken erhalten, die operative IT aber konsolidieren. Jede Tochter wird ein eigener Tenant in der Plattform mit eigenem Logo, eigenen Brand-Farben, eigener Mail-Domain. Eigentümer der Tochter A bekommen einen Brief mit dem Logo der Tochter A — und sehen nirgendwo, dass im Hintergrund eine zentrale Plattform und eine zentrale Datenbank laufen.

Asset-Manager, der mehrere Eigentümer mit eigenen Brands betreut. Ein institutioneller Asset-Manager verwaltet Bestände für mehrere Fonds oder Family Offices. Jeder Auftraggeber besteht darauf, dass die Mieter im Portal das Logo des Eigentümer-Vehikels sehen, nicht das Logo des Asset-Managers und schon gar nicht das Logo des Software-Anbieters.

Der Asset-Manager selbst sitzt im Hintergrund, betreibt die operative Verwaltung, taucht aber im Mieter-Touchpoint nicht auf. Dieses Modell ist in der Praxis besonders sensibel, weil eine sichtbare Software-Marke im Mieter-Portal die Vertraulichkeits-Vereinbarung mit dem Asset-Eigentümer brechen kann.

WEG-Verwalter, der Eigentümern eine „weiße" Sicht zeigt. Der Klassiker im Mittelstand. Eine Hausverwaltung möchte gegenüber Eigentümern als eigenständiger Dienstleister auftreten, ohne dass der Software-Anbieter im Portal sichtbar wird. Hier geht es weniger um große Mehrmarken-Strategie als um eine schlichte Markenhygiene: Der Eigentümer soll seinen Verwalter wahrnehmen, nicht das Tool, das der Verwalter benutzt. § 27 Abs. 1 WEG benennt den Verwalter als Vertragspartner der Gemeinschaft — und ein Vertragspartner, der unter der Marke eines Drittanbieters kommuniziert, wirkt nach außen austauschbar. Whitelabel ist hier auch ein Vertrauens-Signal.

Alle drei Szenarien verlangen technisch dasselbe: pro Tenant ein eigenes Logo, eigene Brand-Farben, eine optional komplett ausgeblendete ImmoGenio-Marke und eine eigene Versand-Identität für Briefe und Mails.

Was Whitelabel technisch heißt

Whitelabel klingt nach einem Logo-Tausch — ist aber im Kern eine Konfigurations-Architektur, die an mindestens fünf Stellen sauber durchgereicht werden muss.

Logo und Brand-Farben pro Tenant. Die ImmoGenio-Plattform persistiert pro Tenant einen Whitelabel-Block in der Spalte `tenants.settings` (JSONB). Das Logo wird als URL hinterlegt (S3- oder MinIO-Bucket mit signierter Zugriffs-URL), die Brand-Farben werden als zwei CSS-Variablen geführt — Primary und Accent. Beim Laden des Portals werden diese Variablen in die Root-CSS-Custom-Properties geschrieben, sodass alle Buttons, Links, Headlines und Card-Borders automatisch in der Mandanten-Farbe erscheinen. Eine separate Theme-Datei pro Tenant gibt es nicht; die Style-Logik liest aus dem Tenant-Setting und applied die Werte zur Laufzeit.

Conditional Logo-Rendering in Brief-Templates. Die Brief-Vorlagen-Bibliothek rendert pro Brief eine Header-Zeile mit Logo. Der Brief-Renderer prüft bei der HTML-Generation, ob der aktive Tenant ein eigenes Logo hinterlegt hat. Falls ja, wird die Logo-URL aus dem Setting eingesetzt; falls nein, fällt der Renderer auf eine generische Variante zurück. Diese Logik sitzt im `VorlageParamPanel` der Brief-Engine und ist für alle 33 Vorlagen identisch.

Hide-immogenio-Logo-Flag. Ein zusätzliches Boolean-Flag im Whitelabel-Block steuert, ob in Vorlagen-Briefen ein dezenter „Versendet über ImmoGenio"-Hinweis erscheint oder nicht. Für Whitelabel-Partner ist dieser Hinweis standardmäßig deaktiviert; für Mandanten ohne Whitelabel-Vereinbarung ist er aktiv und dokumentiert, mit welcher Plattform

der Brief erstellt wurde. Auch die ETV-Protokolle (Eigentümerversammlungs-Protokolle nach § 24 Abs. 6 WEG, siehe Beschlussanfechtungsklage) tragen das Flag, weil ein WEG-Protokoll mit Software-Branding bei Anfechtung zur Stilfrage werden kann.

Eigene Mail-Absender pro Mandant. Briefe sind die eine Achse, Mails die andere. Jeder Tenant kann einen eigenen SMTP-Absender konfigurieren — `verwaltung@tochter-a.de` statt `noreply@immogenio.de`. Damit eine solche Konfiguration sauber zustellt, muss der Mandant SPF, DKIM und DMARC im eigenen DNS einrichten (RFC 7208 für SPF, RFC 6376 für DKIM, RFC 7489 für DMARC). Der DKIM-Selector wird mandanten-spezifisch generiert, der öffentliche Teil als TXT-Record am Mandanten-DNS hinterlegt. Ohne diese DNS-Konfiguration landen Mails von der Mandanten-Domain bei Gmail oder Outlook im Spam-Ordner oder werden gleich abgewiesen.

Letter-Provider-Credentials pro Tenant. Der vermutlich sensibelste Bereich. Wer Briefe über Pingen oder LetterXpress versendet — beide Anbieter beschrieben im Hybrid-Briefversand-Beitrag —, entscheidet pro Mandant, ob die Plattform den Provider-Account des Software-Anbieters oder den Account des Mandanten selbst nutzt. Im Whitelabel-Modell ist die zweite Variante Pflicht: Die Versand-Rechnung kommt direkt vom Druckdienstleister an den Mandanten, mit dem Mandanten als Vertragspartner. Dafür muss die Plattform die API-Credentials des Mandanten kennen — und genau diese Credentials sind im Klartext eine Goldgrube für Angreifer.

Wie ImmoGenio das umsetzt

Die technische Umsetzung folgt einem konsistenten Muster, das die Anforderungen aus der Row-Level-Security-Architektur sauber weiterführt.

Tenant-Settings-API mit Whitelabel-Sub-Block. Die `tenants.settings`-Spalte ist als JSONB ausgeführt und unter Row-Level Security stehend. Ein Lese-Zugriff auf das Setting eines fremden Tenants ist über die regulären API-Endpunkte technisch nicht möglich — die `tenant_id`-Policy filtert die Zeile heraus, bevor der Anwendungs-Code überhaupt darauf zugreift. Innerhalb des Settings ist der Whitelabel-Block ein eigenes Sub-Objekt mit den Feldern `logo_url`, `brand_primary`, `brand_accent`, `hide_immogenio_logo`, `mail_from`, `mail_reply_to`. Änderungen erfolgen über einen Admin-Endpunkt, der nur für Tenant-Administratoren freigeschaltet ist und jede Änderung im Audit-Trail protokolliert — wer hat wann welchen Wert geändert.

Brief-Renderer mit Whitelabel-Setting. Der HTML-Renderer der Brief-Engine — produktiv beschrieben im Briefeditor-Beitrag — pulled das Whitelabel-Setting bei jedem Render-Vorgang aus der Datenbank. Die Logo-URL wird als signierte URL eingesetzt, die nur einige Minuten gültig ist; die Brand-Farben werden in das CSS des Brief-PDF eingespielt. Da der

Renderer in einer Puppeteer-basierten PDF-Pipeline läuft, müssen die Logos zum Render-Zeitpunkt erreichbar sein — eine ausgelaufene Logo-URL bricht den Render und löst eine Fehlermeldung aus, anstatt einen Brief ohne Logo zu produzieren.

Tenant-spezifische Letter-Provider-Konfiguration. Die Tabelle `tenant_letter_settings` hält pro Tenant die Konfiguration für Pingen und LetterXpress. Das Schema umfasst den Provider-Typ, einen Status-Flag (aktiv, inaktiv, in Konfiguration), Versand-Defaults (Versand-Klasse, Farbe vs. Schwarzweiß, Simplex vs. Duplex) und die verschlüsselten Credentials in der Spalte `credentials_enc`. Bei jedem Brief-Versand prüft die Versand-Engine zuerst, ob für den Mandanten eine eigene Provider-Konfiguration hinterlegt ist, und nutzt diese; andernfalls läuft der Versand über den geteilten Plattform-Account.

AES-256-GCM-Verschlüsselung der Provider-Credentials. Die Pingen-API-Keys und LetterXpress-Login-Credentials werden mit AES-256-GCM verschlüsselt, bevor sie in die Datenbank geschrieben werden. AES-256-GCM ist ein authentifizierter Verschlüsselungs-Modus (Authenticated Encryption with Associated Data, AEAD), der gleichzeitig Vertraulichkeit und Integrität garantiert — ein Angreifer kann den Chiffretext weder lesen noch unbemerkt modifizieren. Die BSI Technische Richtlinie BSI TR-02102-1 listet AES-256-GCM ausdrücklich als empfohlenes Verfahren für Vertraulichkeit mit Integrität. Der Initialisierungs-Vektor (IV, 96 Bit) ist pro Verschlüsselungs-Operation zufällig und wird mit dem Chiffretext zusammen persistiert; der Authentication-Tag (128 Bit) wird bei der Entschlüsselung verifiziert.

Schlüssel-Management mit zweistufiger Hierarchie. Der Schlüssel, mit dem die Credentials verschlüsselt werden, ist nicht ein globaler Plattform-Schlüssel, sondern ein pro Tenant generierter Data Encryption Key (DEK). Dieser DEK ist seinerseits mit einem Key Encryption Key (KEK) verschlüsselt, der im KMS bzw. HSM des Hosting-Anbieters liegt. Die Plattform sieht den KEK nie im Klartext; sie ruft den KMS auf, um den DEK zu entpacken, verwendet ihn im Speicher und verwirft ihn wieder. Diese Envelope-Encryption ist Industriestandard und entspricht der Empfehlung aus NIST SP 800-57 Part 1 Rev. 5 zur Schlüssel-Hierarchie in Multi-Tenant-Systemen. Bei einer hypothetischen Datenbank-Kompromittierung sind die Credentials ohne Zugriff auf das KMS nicht verwertbar.

Praxis-Workflow: Onboarding einer Verwalter-Gruppe

Wie sieht das in der Praxis aus, wenn die eingangs beschriebene Gruppe mit vier Töchtern auf die Plattform migriert?

Schritt 1 — Tenants anlegen. Für jede Tochter wird ein Tenant erstellt. Die Tenant-Administratoren werden eingeladen, das Logo (PNG oder SVG, maximal 1 MB) hochzuladen und die Brand-Farben als Hex-Werte zu hinterlegen. Die Logo-Datei landet im S3-Bucket der Plattform; die signierte Zugriffs-URL wird im Whitelabel-Block gespeichert.

Schritt 2 — Pingen-Account verbinden. Jede Tochter besitzt einen eigenen Pingen-Account mit eigenen Zahlungsdaten. Der Admin trägt den API-Key in der Tenant-Konfiguration ein. Der API-Key durchläuft im Backend einen Test-Call (ein Pingen-`GET /me`), wird bei Erfolg AES-256-GCM-verschlüsselt und in `tenant_letter_settings.credentials_enc` abgelegt. Der Klartext-Key bleibt nicht im Speicher und wird nicht geloggt.

Schritt 3 — Mail-Absender konfigurieren. Die Tochter wählt eine Absender-Adresse (`info@tochter-a.de`). Die Plattform stellt einen DKIM-Selector bereit (zum Beispiel `immo-genio2026._domainkey`) inklusive des öffentlichen Schlüssels als TXT-Record-Wert. Die IT der Tochter trägt SPF, DKIM und DMARC in den DNS der Mandanten-Domain ein. Die Plattform führt einen Verifikations-Call durch, der die DNS-Records prüft; erst nach erfolgreicher Verifikation wird der Absender freigeschaltet. Diese Mechanik entspricht den Anforderungen aus § 5 TMG und § 6 TMG zur Identifizierbarkeit von Diensteanbietern in elektronischer Kommunikation.

Schritt 4 — Erster Brief im Whitelabel-Versand. Ein Sachbearbeiter der Tochter A erzeugt eine Versammlungs-Einladung. Der Brief-Renderer pulled das Logo der Tochter A, die Brand-Farben werden in das PDF eingespielt, der „Versendet über ImmoGenio”-Hinweis bleibt verborgen, weil das Hide-Flag aktiv ist. Die Versand-Engine entschlüsselt den Pingen-API-Key der Tochter A im Speicher, übergibt den Brief an den Pingen-Account der Tochter A und persistiert den Versand-Vorgang. Pingen druckt, kuvertiert, liefert ein. Der Eigentümer erhält einen Brief unter dem Logo seiner Verwaltung, mit einer Rechnung, die Pingen direkt an die Tochter A stellt. Im gesamten Vorgang taucht die Plattform nach außen nicht auf.

Compliance-Anker

Whitelabel-Branding ist nicht nur eine Marketing-Funktion, sondern berührt mehrere konkrete Normen, die in der Verwaltungs-Branche regelmäßig auditiert werden.

DSGVO Art. 32 — technisch-organisatorische Maßnahmen. Die AES-256-GCM-Verschlüsselung der Provider-Credentials erfüllt die Anforderung an „dem Risiko angemessene” technische Maßnahmen zur Sicherstellung von Vertraulichkeit und Integrität. Pingen-Credentials erlauben den Versand physischer Briefe im Namen der Verwaltung; ihre Kompromittierung könnte zur Versendung gefälschter Schreiben an Eigentümer und Mieter führen. Die Risikoklasse ist entsprechend hoch, der eingesetzte Schutz mit AES-256-GCM plus Envelope-Encryption im KMS ist branchenüblich angemessen.

DSGVO Art. 28 — Auftragsverarbeitung. Bei Whitelabel-Versand über den Pingen-Account der Tochter ist die Tochter der Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO; Pingen ist Auftragsverarbeiter. Der Auftragsverarbeitungs-Vertrag wird zwischen Tochter und Pin-

gen geschlossen, nicht zwischen Plattform-Anbieter und Pingen. Diese Klarheit der Verantwortungs-Verteilung ist ein zentrales Argument gegen das Modell „Plattform-Account für alle".

BSI TR-02102-1 — Kryptografie-Standards. Die Technische Richtlinie BSI TR-02102-1 in der aktuellen Fassung (2026-1) führt AES-256-GCM als empfohlenes Verfahren für authentifizierte symmetrische Verschlüsselung. Die Mindest-Schlüssellänge von 128 Bit wird mit der gewählten 256-Bit-Schlüsselstärke deutlich überschritten. Die in der Richtlinie geforderte Frische des Initialisierungs-Vektors (eindeutig pro Schlüssel und Klartext) ist durch die zufällige IV-Generierung pro Operation gegeben.

Markenrecht und Haftung. Jede Tochter ist nach § 14 MarkenG selbst verantwortlich für die Rechtmäßigkeit ihrer Marke. Die Plattform stellt das technische Mittel zur Verfügung; die markenrechtliche Verantwortung für Logo, Farben und Wortmarke trägt der Mandant. Diese saubere Trennung ist auch deshalb wichtig, weil die Plattform keinen Einfluss auf Inhalte der hochgeladenen Logos hat — der Mandant trägt die Verifikations- und Lizenz-Pflicht.

§ 5 TMG — Impressumspflicht im Whitelabel-Portal. Wenn das Portal unter der Marke der Tochter erscheint, muss das Impressum die Tochter ausweisen, nicht den Software-Anbieter. § 5 TMG verlangt unverzügliche und leichte Erkennbarkeit des Diensteanbieters; ein versteckter ImmoGenio-Hinweis im Footer wäre nicht TMG-konform, wenn die Tochter den Dienst gegenüber Eigentümern erbringt. Die Plattform stellt deshalb pro Tenant ein konfigurierbares Impressum-Modul bereit, in dem die Mandanten-Daten gepflegt werden.

Grenzen der aktuellen Lösung

Die produktive Whitelabel-Funktion deckt den Kern ab, hat aber dokumentierte Grenzen, die bewusst gesetzt sind.

Eine Brand pro Tenant. Ein Tenant trägt eine Marke. Eine dynamische Umschaltung („Mieter aus Bestand X sehen Logo A, Mieter aus Bestand Y sehen Logo B im selben Tenant") ist nicht vorgesehen. Wer mehrere Marken betreibt, legt mehrere Tenants an — das hält die Architektur sauber und entlastet das Permissions-System von Brand-Logik.

Keine Custom-Domain. Das Portal läuft unter einem ImmoGenio-Hostname, das Logo und die Farben sind aber die des Mandanten. Custom-Domain-Routing (`portal.tochter-a.de`) ist als nächste Ausbaustufe geplant, erfordert aber zusätzliches TLS-Zertifikats-Management pro Mandanten-Domain und ist deshalb nicht in der ersten Welle enthalten.

Keine White-Label-Mobile-App. Die Funktion betrifft das Web-Portal und Briefe. Eine Mobile-App mit Mandanten-spezifischem Icon im App-Store ist nicht Teil der aktuellen Lösung.

Keine Custom-Templates jenseits des Vorlagen-Sets. Die 33 Brief-Vorlagen werden um Logo, Brand-Farben und Hide-Flag erweitert; eine komplett freie Template-Sprache pro Mandant gibt es nicht. Das hält die Pflege und die Audit-Sicherheit überschaubar.

FAQ

Was kostet Whitelabel pro Mandant?

Die Whitelabel-Funktion ist Teil des Tarif-Modells; der konkrete Aufpreis hängt von der Anzahl der Mandanten in der Gruppe und vom gewünschten Funktionsumfang ab. In der Regel bewegt sich der Aufpreis im niedrigen dreistelligen Bereich pro Tenant und Monat — die Kosten-Ersparnis gegenüber dem Betrieb mehrerer Software-Instanzen amortisiert ihn meist im ersten Quartal.

Wo wird das Logo gespeichert?

Die Logo-Datei liegt im S3- oder MinIO-Bucket der Plattform, getrennt nach Tenant in einem eigenen Pfad. Der Zugriff erfolgt über signierte URLs mit Kurzgültigkeit. Backups laufen verschlüsselt, die Aufbewahrungs-Dauer entspricht der allgemeinen Archiv-Politik der Plattform.

Können wir eine eigene Domain für unser Portal nutzen?

Aktuell noch nicht. Das Portal läuft unter einem ImmoGenio-Hostname; das Logo und die Farben sind aber die des Mandanten, sodass der Eigentümer das Mandanten-Branding wahrnimmt. Custom-Domain-Routing ist die nächste geplante Ausbaustufe.

Werden unsere Pingen-Kosten direkt von uns abgerechnet?

Ja, sobald die Tochter einen eigenen Pingen-Account verbindet, rechnet Pingen direkt mit der Tochter ab. Der Auftragsverarbeitungs-Vertrag nach DSGVO Art. 28 wird zwischen Tochter und Pingen geschlossen. Die Plattform ist in dieser Konstellation kein Vertragspartner des Briefversands, sondern nur das technische Mittel.

Was passiert mit dem Branding, wenn wir den Anbieter wechseln?

Logo-Dateien und Konfigurations-Werte werden bei einer Migration als strukturierter Export bereitgestellt (JSON-Export der Whitelabel-Settings plus Logo-Dateien). Die Brand-Farben sind als Hex-Werte dokumentiert und sofort in einer Nachfolge-Plattform verwendbar. Die AES-256-GCM-verschlüsselten Pingen-Credentials werden im Klartext nicht exportiert — die Tochter muss den API-Key beim Wechsel neu vergeben und beim neuen Anbieter eintragen. Das ist eine bewusste Sicherheits-Eigenschaft, kein Bug.

Wie sicher ist die AES-256-GCM-Verschlüsselung der Credentials?

AES-256-GCM gilt nach aktuellem Stand der Kryptografie als sicher gegen klassische Angriffe. Die effektive Schlüsselstärke von 256 Bit ist gegen Brute-Force selbst mit hypothetischen Quanten-Computern in absehbarer Zeit nicht angreifbar (Grover's Algorithm reduziert die Stärke auf effektiv 128 Bit, was immer noch als sicher gilt). Die Authentifizierungs-Komponente (GCM-Tag) erkennt Modifikationen am Chiffretext mit einer Fehlerwahrscheinlichkeit unter 2^{-128}. Die BSI TR-02102-1 listet das Verfahren ausdrücklich als geeignet. Die operative Sicherheit hängt am Schutz der Master-Schlüssel im KMS — und der wiederum ist als zentrale Komponente besonders gehärtet und protokolliert.

Verwandte Beiträge

- Row-Level Security in der Hausverwaltungs-Software
- Hybrid-Briefversand mit Pingen und LetterXpress
- Mustervorlagen-Bibliothek mit 33 revisionssicheren Vorlagen
- Briefeditor mit Markdown, WYSIWYG, DIN 5008 und PDF-Vorschau

Wo wir stehen

Das Whitelabel-Branding ist produktiv für Logo, Brand-Farben, Mail-Absender und Hide-Logo-Flag. Die AES-256-GCM-Verschlüsselung der Letter-Provider-Credentials läuft mit Envelope-Encryption gegen einen KMS-verwalteten Master-Schlüssel. Pingen-Accounts pro Mandant sind im Betrieb, LetterXpress-Accounts pro Mandant sind in der zweiten Welle vorgesehen. Custom-Domain-Routing — also `portal.tochter-a.de` statt der ImmoGenio-Hostname mit Mandanten-Logo — ist die nächste Ausbaustufe und benötigt zusätzliches TLS-Zertifikats-Management pro Mandanten-Domain. Eine White-Label-Mobile-App ist nicht in Planung; die responsive Web-Variante deckt die typischen Mieter- und Eigentümer-Touchpoints ab.

Kontakt

Verwaltungs-Gruppen, Asset-Manager oder einzelne Verwalter, die ihr Portal und ihre Briefe unter eigener Marke ausgeben möchten, erreichen uns für ein konkretes Onboarding-Gespräch unter kontakt@immogenio.de. Wir zeigen, wie der Tenant-Setup für eine bestehende Verwalter-Gruppe aussieht und welche DNS- und KMS-Voraussetzungen für einen reibungslosen Whitelabel-Start zu erfüllen sind.