NUTZUNGSBEDINGUNGEN

Wellpoint

Therapeuten-Software inkl. Microsoft-, Google- & Apple-Integrationen

Anbieter: PCM Solution GmbH, Kohlerweg 155, 5531 Eben im Pongau, Österreich
Geltungsbereich: B2B – alle Kunden und Nutzer von Wellpoint
Version: 1.0 – Stand März 2026
Kontakt: office@pcm-group.at · www.pcm-group.at

§ 1 Geltungsbereich und Vertragsverhältnis

(1) Diese Nutzungsbedingungen (nachfolgend „NB“) regeln die Nutzung der SaaS-Software Wellpoint einschließlich aller integrierten Drittdienste (Microsoft, Google, Apple) durch Kunden und deren autorisierte Nutzer. Sie ergänzen die Allgemeinen Geschäftsbedingungen (AGB) der PCM Solution GmbH und gehen diesen in Fragen der Drittdienst-Integration vor.

(2) Durch die Aktivierung einer Drittdienst-Integration in Wellpoint erklärt der Nutzer sein ausdrückliches Einverständnis mit den entsprechenden Abschnitten dieser NB sowie mit den Nutzungsbedingungen des jeweiligen Drittanbieters.

(3) Die Nutzung von Wellpoint-Integrationen ist freiwillig. Kernfunktionen der Software stehen auch ohne Aktivierung von Microsoft-, Google- oder Apple-Integrationen vollständig zur Verfügung.

§ 2 Account-Erstellung und Zugangsdaten

(1) Für die Nutzung von Wellpoint ist die Erstellung eines Nutzer-Accounts erforderlich. Dies kann entweder durch direkte Registrierung mit E-Mail und Passwort oder – sofern aktiviert – durch Anmeldung über einen der unterstützten OAuth-Anbieter (Microsoft oder Google) erfolgen.

(2) Der Nutzer ist verpflichtet, bei der Registrierung wahrheitsgemäße Angaben zu machen und sein Konto aktuell zu halten. Insbesondere muss die hinterlegte E-Mail-Adresse jederzeit erreichbar sein, da über sie sicherheitsrelevante Benachrichtigungen zugestellt werden.

(3) Zugangsdaten sind vertraulich zu behandeln und dürfen nicht an Dritte weitergegeben werden. Der Nutzer haftet für alle Aktivitäten, die unter seinem Account durchgeführt werden, es sei denn, er hat den Missbrauch unverzüglich gemeldet.

(4) Zwei-Faktor-Authentifizierung (2FA) wird für alle Nutzer-Accounts, die auf Patientendaten zugreifen können, dringend empfohlen und für administrative Accounts verpflichtend vorgeschrieben.

§ 3 Microsoft-Integration (OAuth 2.0 / Azure AD)

3.1 Art der Integration und OAuth-Fluss

Wellpoint unterstützt die Anmeldung und Kalender-Synchronisation über Microsoft-Konten (Microsoft 365, Outlook.com, Azure AD) mittels des OAuth-2.0-Protokolls. Der Authentifizierungsfluss verläuft ausschließlich über die offiziellen Microsoft Identity Platform-Endpunkte (login.microsoftonline.com). Wellpoint erhält dabei zu keinem Zeitpunkt das Passwort des Nutzers.

Wie OAuth 2.0 mit Microsoft funktioniert

1. Der Nutzer klickt auf „Mit Microsoft anmelden“ in Wellpoint.
2. Er wird auf die sichere Microsoft-Anmeldeseite weitergeleitet (login.microsoftonline.com).
3. Nach erfolgreicher Anmeldung bei Microsoft erteilt der Nutzer Wellpoint explizit die gewünschten Berechtigungen.
4. Microsoft stellt Wellpoint ein kurzlebiges Access Token und ein Refresh Token aus.
5. Wellpoint verwendet ausschließlich diese Tokens – niemals das Passwort des Nutzers.
6. Der Nutzer kann die Berechtigungen jederzeit in seinem Microsoft-Konto widerrufen.

3.2 Angeforderte Berechtigungen (Scopes)

Wellpoint fordert ausschließlich die für den jeweiligen Funktionsumfang notwendigen Berechtigungen an. Der Nutzer wird vor der ersten Verbindung über alle angeforderten Scopes informiert und muss diesen aktiv zustimmen:

Berechtigung / Scope	Zweck in Wellpoint	Was wir NICHT tun
openid, profile, email	Single Sign-On (SSO): Anmeldung mit Microsoft-Konto ohne separates Passwort	Wir speichern kein Microsoft-Passwort; kein Zugriff auf sonstige Microsoft-Dienste
Calendars.ReadWrite	Lesen und Schreiben von Terminen im Outlook-Kalender für die Wellpoint-Terminplanung	Kein Zugriff auf E-Mails, Kontakte, Teams, SharePoint oder OneDrive
Calendars.Read.Shared	Lesen von freigegebenen Teamkalendern (optional, nur wenn aktiviert)	Keine automatische Synchronisation ohne explizite Nutzeraktivierung
offline_access	Automatische Token-Erneuerung ohne erneuten Login (Hintergrund-Synchronisation)	Kein Zugriff auf weitere Daten über den definierten Scope hinaus

3.3 Token-Verwaltung und Datenspeicherung

(1) Access Tokens (kurzlebig, typisch 1 Stunde) werden ausschließlich verschlüsselt im Arbeitsspeicher und nicht dauerhaft auf Festplatte gespeichert.

(2) Refresh Tokens (langlebig) werden AES-256-verschlüsselt in der Wellpoint-Datenbank gespeichert, um eine automatische Token-Erneuerung ohne erneuten Login zu ermöglichen. Sie werden nicht an Dritte weitergegeben.

(3) Bei Trennung der Microsoft-Integration werden alle gespeicherten Tokens sofort und unwiderruflich gelöscht.

3.4 Nutzungsbedingungen von Microsoft

Durch die Aktivierung der Microsoft-Integration erklärt der Nutzer sein Einverständnis mit den Microsoft-Dienstbedingungen und der Microsoft-Datenschutzerklärung (microsoft.com/privacy). Der Anbieter übernimmt keine Verantwortung für Änderungen in Microsofts API, Serviceausfälle der Microsoft-Plattform oder Änderungen der Microsoft-Nutzungsbedingungen.

Unternehmenskunden, die Azure Active Directory (Azure AD / Entra ID) einsetzen, benötigen möglicherweise eine zusätzliche Admin-Genehmigung durch ihren IT-Administrator, bevor Nutzer die Integration aktivieren können. Wellpoint unterstützt den Azure AD Admin Consent Flow.

3.5 Einschränkungen und Haftung

Der Anbieter haftet nicht für Datenverluste oder Synchronisationsfehler, die auf Einschränkungen, Änderungen oder Ausfälle der Microsoft-API zurückzuführen sind. Im Falle von API-Einschränkungen durch Microsoft informiert der Anbieter die betroffenen Nutzer zeitnah per E-Mail.

§ 4 Google-Integration (OAuth 2.0 / Google Identity)

4.1 Art der Integration und OAuth-Fluss

Wellpoint unterstützt die Anmeldung und Kalender-Synchronisation über Google-Konten mittels OAuth 2.0 über die Google Identity Platform (accounts.google.com). Wellpoint ist eine verifizierte Google-App und erfüllt die Google API Services User Data Policy, einschließlich der Einschränkungen für sensible Scopes.

Wie OAuth 2.0 mit Google funktioniert

1. Der Nutzer klickt auf „Mit Google anmelden“ in Wellpoint.
2. Er wird auf die sichere Google-Anmeldeseite weitergeleitet (accounts.google.com).
3. Google zeigt dem Nutzer einen Berechtigungsbildschirm mit allen angeforderten Scopes.
4. Nach Zustimmung stellt Google Wellpoint ein Access Token und ein Refresh Token aus.
5. Wellpoint verwendet diese Tokens ausschließlich für die genehmigten Zwecke.
6. Der Nutzer kann die Berechtigungen jederzeit unter myaccount.google.com widerrufen.

4.2 Angeforderte Berechtigungen (Scopes)

Wellpoint hält sich strikt an die Google API Services User Data Policy. Sensible Scopes werden nur nach expliziter Zustimmung des Nutzers und nur für den angegebenen Zweck verwendet:

Berechtigung / Scope	Zweck in Wellpoint	Was wir NICHT tun
openid, profile, email	Single Sign-On (SSO): Anmeldung mit Google-Konto	Wir speichern kein Google-Passwort; kein Zugriff auf Gmail oder Google Drive
calendar.events	Lesen und Erstellen von Terminen im Google Kalender für die Wellpoint-Terminplanung	Kein Zugriff auf Kalender anderer Google-Nutzer ohne deren explizite Freigabe
calendar.readonly (optional)	Nur-Lese-Zugriff für Nutzer, die keine Termine aus Wellpoint in Google Kalender schreiben möchten	Keine Weitergabe von Kalenderinhalten an Dritte

4.3 Google Limited Use Policy

Wellpoints Nutzung von Google-Nutzerdaten beschränkt sich auf die Bereitstellung und Verbesserung der in Wellpoint angebotenen Funktionen. Insbesondere gilt:

- Wir übertragen keine Google-Nutzerdaten an Dritte, ausgenommen nach Maßgabe der Google Limited Use Policy
- Wir verwenden Google-Nutzerdaten nicht für Werbezwecke jeglicher Art
- Wir geben keine Google-Nutzerdaten für Kreditwürdigkeitsprüfungen oder andere außerhalb von Wellpoint liegende Zwecke weiter
- Menschen haben immer die Möglichkeit, Google-Daten nur für den Nur-Lese-Zugriff freizugeben, wenn sie keine Termine aus Wellpoint in Google Kalender schreiben möchten

4.4 Google Workspace (G Suite) Unternehmenskunden

Nutzer, die mit einem Google Workspace-Konto (ehemals G Suite) arbeiten, möglicherweise eine zusätzliche Genehmigung durch den Google Workspace-Administrator ihrer Organisation benötigen. Wellpoint ist als vertrauenswürdige App im Google Workspace Marketplace gelistet. Administratoren können die Integration über die Google Workspace Admin Console für alle Nutzer ihrer Domain freigeben oder einschränken.

4.5 Nutzungsbedingungen von Google und Haftung

Durch die Aktivierung der Google-Integration erklärt der Nutzer sein Einverständnis mit den Google Nutzungsbedingungen (policies.google.com) und der Google Datenschutzerklärung. Der Anbieter übernimmt keine Verantwortung für Änderungen in Googles API-Richtlinien, Serviceausfälle der Google-Plattform oder Änderungen der Google-Nutzungsbedingungen.

§ 5 Apple Kalender-Anbindung (CalDAV / iCloud)

5.1 Art der Integration – CalDAV statt OAuth

Im Unterschied zu Microsoft und Google verwendet Apple für die Kalenderanbindung kein OAuth-2.0-Protokoll, sondern das offene CalDAV-Protokoll (RFC 4791) in Kombination mit einem app-spezifischen Passwort („App-Specific Password“). Apple hat bewusst entschieden, OAuth für CalDAV nicht zu unterstützen; die vorliegende Integrationsmethode entspricht Apples offiziellen Empfehlungen für Drittanbieter-Anwendungen.

Wie die Apple Kalender-Anbindung funktioniert (CalDAV)

1. Der Nutzer erstellt unter appleid.apple.com ein app-spezifisches Passwort für Wellpoint.
   (Pfad: Apple-ID → Anmelden und Sicherheit → App-spezifische Passwörter → Generieren)
2. Das app-spezifische Passwort gewährt nur Zugriff auf Kalender – nicht auf die Apple-ID.
3. Der Nutzer gibt in Wellpoint seine iCloud-E-Mail-Adresse und das app-spezifische Passwort ein.
4. Wellpoint verbindet sich über CalDAV mit dem Apple-Kalenderserver (caldav.icloud.com).
5. Das Passwort wird AES-256-verschlüsselt in Wellpoint gespeichert.
6. Der Nutzer kann das Passwort jederzeit in seiner Apple-ID widerrufen.

5.2 Sicherheitshinweise zum app-spezifischen Passwort

App-spezifische Passwörter sind ein Sicherheitsmerkmal von Apple für Konten mit aktivierter Zwei-Faktor-Authentifizierung (2FA). Sie bieten folgende Sicherheitsvorteile:

- Das tatsächliche Apple-ID-Passwort wird niemals an Wellpoint übermittelt
- Jedes app-spezifische Passwort kann unabhängig widerrufen werden, ohne das Haupt-Apple-ID-Passwort zu ändern
- Apple begrenzt den Zugriff auf den jeweils gewährten Dienst (hier: CalDAV/Kalender)

– Bei Verdacht auf Missbrauch kann das Passwort sofort unter appleid.apple.com deaktiviert werden

Wichtiger Hinweis: Apple 2FA muss für die Apple-ID des Nutzers aktiviert sein, um app-spezifische Passwörter generieren zu können. Ohne aktivierte 2FA ist eine Verbindung mit Apple Kalender über Wellpoint nicht möglich.

5.3 Angeforderte Berechtigungen (CalDAV)

Berechtigung / Scope	Zweck in Wellpoint	Was wir NICHT tun
Kalenderlesezugriff (CalDAV)	Lesen von Terminen aus Apple Kalender (iCloud) zur Anzeige in Wellpoint	Kein Zugriff auf iCloud Drive, Fotos, Kontakte oder andere Apple-Dienste
Kalenderschreibzugriff (CalDAV)	Erstellen und Bearbeiten von Terminen in Apple Kalender aus Wellpoint heraus	Keine Speicherung von Apple-ID-Passwörtern; Verbindung über App-spezifisches Passwort

5.4 Unterstützte Apple-Kalender-Dienste

Wellpoint unterstützt die Anbindung folgender Apple-Kalender-Dienste per CalDAV:

– iCloud Kalender (caldav.icloud.com) – vollständig unterstützt

– Lokale On-Premise CalDAV-Server – auf Anfrage (Enterprise-Paket)

Nicht unterstützt werden: lokale Apple Kalender ohne iCloud-Synchronisation, CalDAV-Server mit selbstsignierten Zertifikaten ohne vorherige Konfiguration.

5.5 Besonderheiten bei iOS-Geräten

Die Wellpoint-Web-App kann auf iOS-Geräten im Safari-Browser genutzt werden. Die native CalDAV-Verbindung läuft dabei über den Wellpoint-Server, nicht über die native Apple-Kalender-App. Eine native iOS-App mit direkter Kalenderintegration über EventKit ist in Entwicklung und wird in einer zukünftigen Version von Wellpoint verfügbar sein.

5.6 Nutzungsbedingungen von Apple und Haftung

Durch die Aktivierung der Apple-Kalender-Integration erklärt der Nutzer sein Einverständnis mit den Apple-Mediendienstleistungsbedingungen und der Apple-Datenschutzrichtlinie (apple.com/de/privacy). Der Anbieter übernimmt keine Verantwortung für Änderungen an Apples CalDAV-Implementierung, iCloud-Verfügbarkeit oder Apple-seitige Einschränkungen.

§ 6 Kalender-Synchronisation – allgemeine Regelungen

(1) Die Kalender-Synchronisation zwischen Wellpoint und den unterstützten Drittdiensten (Microsoft Outlook, Google Kalender, Apple Kalender) erfolgt in Echtzeit oder in konfigurierbaren Synchronisationsintervallen (Standard: alle 15 Minuten).

(2) Synchronisationskonflikte (z. B. gleichzeitige Änderung desselben Termins in Wellpoint und im externen Kalender) werden nach dem Prinzip „letzte Änderung gewinnt“ aufgelöst. Der Nutzer wird über Konflikte in der Wellpoint-Oberfläche informiert.

(3) Folgende Termin-Metadaten werden bei der Synchronisation übertragen: Titel, Datum, Uhrzeit, Ort, Teilnehmer (sofern vorhanden), Beschreibung und Wiederholungsregeln. Klinische Notizen, Diagnosen und Patientendaten aus Wellpoint werden übermittelt nur wenn der Nutzer dies explizit für einen Termin aktiviert und sind standardmäßig deaktiviert.

(4) Der Nutzer ist selbst dafür verantwortlich sicherzustellen, dass bei der Kalender-Synchronisation keine schützenswerten Patientendaten unbeabsichtigt in externe Kalender übertragen werden. Wellpoint zeigt vor der ersten Aktivierung der Synchronisation eine Datenschutz-Warnung an.

(5) Der Anbieter empfiehlt, für Wellpoint-Termine in externen Kalendern einen separaten, dedizierten Kalender zu verwenden, um eine klare Trennung von privaten und beruflichen Terminen sicherzustellen.

§ 7 Datenschutz bei Drittdienst-Integrationen

(1) Bei der Aktivierung einer Drittdienst-Integration werden die in §§ 3–5 beschriebenen Daten an den jeweiligen Drittanbieter übermittelt bzw. von diesem abgerufen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung) bzw. Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) für optionale Integrationen.

(2) Die bei Microsoft, Google und Apple gespeicherten Daten unterliegen den Datenschutzbestimmungen des jeweiligen Anbieters. PCM Solution GmbH hat auf diese Daten keinen Einfluss und übernimmt für deren Verarbeitung durch die Drittanbieter keine Verantwortung.

(3) Wellpoint überträgt an keinen der drei Anbieter (Microsoft, Google, Apple) Patientendaten, Diagnosen oder sonstige Gesundheitsdaten, außer der Nutzer aktiviert dies ausdrücklich für einzelne Termine.

(4) Bei Deaktivierung einer Integration werden alle in Wellpoint gespeicherten Tokens, app-spezifischen Passwörter und Synchronisations-Metadaten der jeweiligen Integration unwiderruflich gelöscht. In externen Kalendern bereits angelegte Termine werden nicht automatisch gelöscht.

§ 8 Widerruf und Trennung von Integrationen

Der Nutzer kann jede Integration jederzeit in Wellpoint oder direkt beim Drittanbieter trennen. Die folgende Tabelle zeigt die jeweiligen Wege:

Integration	Zugriff widerrufen	Verbindung in Wellpoint trennen
Microsoft / Azure AD	myaccount.microsoft.com → Apps & Dienste → Wellpoint entfernen	Wellpoint → Einstellungen → Integrationen → Microsoft trennen
Google	myaccount.google.com → Sicherheit → Drittanbieter-Apps → Wellpoint entfernen	Wellpoint → Einstellungen → Integrationen → Google trennen
Apple (iCloud/CalDAV)	appleid.apple.com → Anmelden und Sicherheit → App-spezifische Passwörter → Wellpoint widerrufen	Wellpoint → Einstellungen → Integrationen → Apple Kalender trennen

Nach dem Widerruf auf Seiten des Drittanbieters beendet Wellpoint die Synchronisation automatisch, sobald das nächste Token-Erneuerungsintervall abgelaufen ist (in der Regel spätestens nach 1 Stunde).

Der Widerruf einer Integration hat keinen Einfluss auf in Wellpoint gespeicherte Patientendaten oder sonstige Wellpoint-Inhalte. Lediglich die Verbindung zum externen Dienst wird beendet.

§ 9 Verfügbarkeit und Einschränkungen der Integrationen

(1) Die Verfügbarkeit der Drittdienst-Integrationen ist von der Betriebsstabilität der jeweiligen externen Plattformen abhängig. Der Anbieter übernimmt keine Gewähr für die jederzeitige Verfügbarkeit von Microsoft-, Google- oder Apple-Diensten.

(2) API-Änderungen, Quotenbeschränkungen oder Richtlinienänderungen der Drittanbieter können ohne Vorankündigung Einfluss auf den Funktionsumfang der Integrationen haben. Der Anbieter informiert Nutzer über bekannte Einschränkungen zeitnah per E-Mail und über das Wellpoint-Status-Dashboard (status.pcm-group.at).

(3) Wartungsarbeiten oder Änderungen an den Drittdienst-Integrationen können vorrübergehend zu Unterbrechungen der Synchronisation führen. Der Anbieter ist bemüht, solche Unterbrechungen auf ein Minimum zu begrenzen und kündigt planbare Wartungsfenster rechtzeitig an.

(4) Die SLA-Garantien gemäß den AGB beziehen sich ausschließlich auf die Kernfunktionen von Wellpoint. Ausfälle der Microsoft-, Google- oder Apple-Plattformen gelten nicht als Verfügbarkeitsverletzung im Sinne des Service Level Agreements.

§ 10 Verhalten bei Sicherheitsvorfällen

(1) Wird ein unbefugter Zugriff auf einen integrierten Drittdienst-Account bekannt oder vermutet, ist der Nutzer verpflichtet:

- Das app-spezifische Passwort (Apple) bzw. den OAuth-Zugriff (Microsoft/Google) sofort beim jeweiligen Anbieter zu widerrufen
- Wellpoint über den Vorfall unter sicherheit@pcm-group.at zu informieren
- Das Wellpoint-Passwort zu ändern und alle aktiven Sessions zu beenden

(2) Wellpoint bietet eine Übersicht aller aktiven Integrationen und Sessions unter Einstellungen → Sicherheit → Aktive Verbindungen. Von dort aus können alle Verbindungen mit einem Klick getrennt werden.

(3) Im Falle eines sicherheitsrelevanten Vorfalls, der Wellpoint-seitige Tokens kompromittiert, widerruft der Anbieter unverzüglich alle betroffenen Tokens und informiert die betroffenen Nutzer gemäß Datenschutzerklärung.

§ 11 Zukünftige Integrationen

(1) Der Anbieter behält sich vor, weitere Drittdienst-Integrationen (z. B. weitere Kalender-Anbieter, Videoplattformen für Telemedizin, Abrechnungssysteme) in Wellpoint aufzunehmen. Über neue Integrationen informiert der Anbieter die Kunden vorab.

(2) Neue Integrationen werden stets nach den Prinzipien Privacy by Design und Minimal Permission (nur notwendige Berechtigungen) implementiert und in diese Nutzungsbedingungen aufgenommen.

(3) Der Nutzer kann die Aktivierung neuer Integrationen verweigern, ohne dass dies Auswirkungen auf die übrigen Wellpoint-Funktionen hat.

§ 12 Änderungen dieser Nutzungsbedingungen

Der Anbieter ist berechtigt, diese Nutzungsbedingungen mit einer Ankündigungsfrist von mindestens 4 Wochen zu ändern, insbesondere bei Änderungen der OAuth-Implementierungen, neuen Sicherheitsanforderungen der Drittanbieter oder geänderten rechtlichen Vorgaben. Kunden werden per E-Mail informiert. Die jeweils aktuelle Version ist unter www.pcm-group.at/nutzungsbedingungen abrufbar.

§ 13 Anwendbares Recht und Gerichtsstand

Es gilt österreichisches Recht. Gerichtsstand ist, soweit gesetzlich zulässig, Salzburg, Österreich.

Kurzübersicht: Drittdienst-Integrationen auf einen Blick

	Microsoft	Google	Apple (CalDAV)	Wellpoint-intern
Protokoll	OAuth 2.0 / Azure AD	OAuth 2.0 / Google Identity	CalDAV + App-Passwort	E-Mail + Passwort + 2FA
Passwort an Wellpoint	Nein (Token)	Nein (Token)	App-spez. Passwort (kein Haupt-PW)	Ja (verschlüsselt)
SSO möglich	Ja	Ja	Nein	Nein
Kalender-Sync	Outlook (Lesen + Schreiben)	Google Kalender (Lesen + Schreiben)	iCloud Kalender (Lesen + Schreiben)	Wellpoint-intern
Widerruf	myaccount.microsoft.com	myaccount.google.com	appleid.apple.com	Einstellungen → Sicherheit

PCM Solution GmbH · Kohlerweg 155 · 5531 Eben im Pongau · office@pcm-group.at · www.pcm-group.at