



Transformation, auf die Sie *vertrauen* können.

Wie Pega Blueprint Daten, Datenschutz und KI
sicher handhabt

— Pega Blueprint™ – Sicherheit und Datenschutz

Retail Loan Origination

Select the Case Type to define the workflow details: **Secured Retail Loan Application**

Case Lifecycle Case Data Model

This case type defines a secured Retail Loan application process, from submission, approval, and disbursement, ensuring efficient communication with applicants. This case type represents the process of handling and approving a secured retail lending products like vehicle loans.

Primary Steps:

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
- Collect Applicant Information - Collect Financial Information - Collect Collateral Information + Add Step	- Eligibility Check - Credit Check - Validate Financial Documentation - Check Collateral Type - Validate Guarantor's Financial Data - Retrieve Guarantor's Credit Score - Check Guarantor's Eligibility - Offer Risk Reducing Product to Client + Add Step	- Additional Documentation Check - Collect Additional Documentation - Collect Collateral - Validate Collateral - Valuation of Collateral - Approve/Reject Loan + Add Step	- Loan Amount Check - Loan Terms Calculation - Loan Terms Approval + Add Step	- Prepare Loan Agreement - Review and Sign Agreement - Approve Loan Disbursement - Update Loan Account Information - Update Collateral Systems - Loan Disbursement - Notify Applicant for Loan Disbursement + Add Step

[Save & Close](#) [Next](#)

Pega Blueprint™ Sicherheit und Datenschutz

Bei der Entwicklung von Pega Blueprint™ standen Ihre Privatsphäre und Sicherheit an erster Stelle. Wir wissen, dass Ihre Prozesse nicht nur Diagramme und Workflows sind – sie beschreiben Ihren Wettbewerbsvorteil.



Ihr Unternehmen kontrolliert den Zugriff

Der Zugriff auf Blueprint kann an den Single-Sign-on (SSO) Ihres Unternehmens gebunden werden.

- Blueprint regelt den Datenzugriff mit rollenbasierten Zugriffskontrollen. So wird sichergestellt, dass Blueprints nur für den Ersteller zugänglich sind – es sei denn, sie werden aktiv freigegeben.
- Wenn ein Benutzer aus Ihrem Unternehmen ausscheidet, verliert er den Zugriff auf Ihre Blueprints, sobald Sie seinen Status oder seine Rolle bei Ihrem SSO-Anbieter aktualisieren.

Mit Ihren Blueprints wird keine KI trainiert

Prompts, Daten und Designs werden niemals für das Training von KI-Modellen verwendet.

- Blueprint nutzt modernste LLMs, einschließlich Anthropic-Modelle auf AWS und Google Gemini sowie OpenAI auf MS Azure.
- Alle LLMs unterliegen einer ständigen Governance, werden Performance-Tests unterzogen und verwenden bewährte Methoden für die Inhaltsfilterung.

Daten bleiben vertraulich

Die Details Ihrer Blueprints werden in einer verschlüsselten Cloud-Datenbank gespeichert.

- Die Bereitstellung in der Cloud erfolgt in der Region, die für Ihr Unternehmen am meisten Sinn ergibt: USA, UK, Asien-Pazifik oder EU.
- Ihre Daten werden nicht mit anderen Pega-Kunden oder Pega-Partnern geteilt.
- Nur der Ersteller kann auf seine Blueprints zugreifen. Blueprints sind grundsätzlich privat und müssen aktiv zur gemeinsame Nutzung freigegeben werden.
- Nur Berichtsdaten zur Aktivität werden intern von autorisierten Pega-Experten genutzt (wie E-Mail-Adresse, Erstellungszeit, Namen von Erstellern).

Cloud-Sicherheit der Enterprise-Klasse

Ihre Blueprint-Daten erhalten den gleichen erstklassigen Schutz wie unsere Pega Cloud-Umgebungen, einschließlich:

- 256-Bit-AES-Verschlüsselung für ruhende Daten und HTTPS/TLS-Schutz für Daten während der Übertragung.
- Kontinuierliche Überwachung mit hostbasierten Virenschutz- und Intrusion-Prevention-Systemen.
- Hochmoderne Betriebszentren, die physische und ökologische Sicherheit ernst nehmen.
- Integrierte Schutzmaßnahmen gegen DDoS-Angriffe und automatisches Blockieren bekannter bösartiger IP-Adressen.



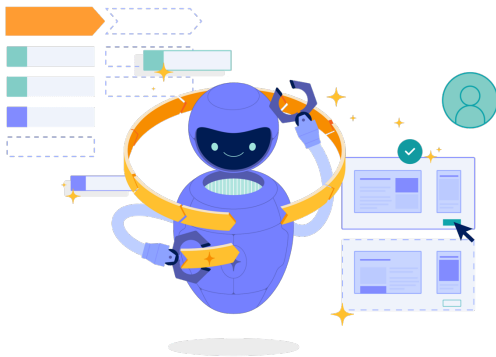
01

Was ist Pega Blueprint?



Die perfekte Unterstützung für Ihre Transformation

Pega Blueprint bietet eine KI-gestützte Workflow-Entwicklung für Unternehmen, mit der Menschen und KI gemeinsam schneller automatisieren und transformative Innovationen realisieren können.



Pega + Blueprint™

Dashboard

RETAIL BANKING • BP-2224548 • ☆

Complaints Management

Define workflow details for: **Complaint Management**

Application Context | Workflows | **Workflow Details** | Data & Integrations | Personas | Summary

Edit Case Type | Settings

Case Lifecycle | Case Data Model | Business Rules | Reports

Orchestrates the end-to-end lifecycle of complaints from intake to resolution and closure, governing assignment, investigation, escalation, regulatory submission, systemic issue detection, and learning capture for continuous improvement.

Step types

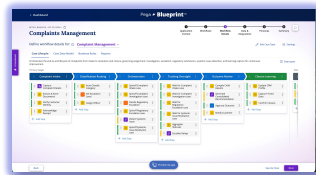
Primary Stages

Complaint Intake	Classification Routing	Orchestration	Tracking Oversight	Outcome Review	Closure Learning
- Capture Complaint Details - Extract & Store Documents - Verify Customer Identity - Acknowledge Receipt	- Auto-Classify Category - Set Escalation Level - Assign Officer	- Spinoff Complaint Intake case - Spinoff Complaint Investigation case - Decide Regulatory Escalation - Spinoff Regulatory Escalation case - Detect Systemic Issue - Spinoff Systemic Issue Resolution case	- Wait for Complaint Intake case - Wait for Complaint Investigation case - Wait for Regulatory Escalation case - Wait for Systemic Issue Resolution case - Aggregate Statuses - Escalate Delays	- Compile Child Results - Generate Consolidated Recommendation - Approve Outcome - Notify Customer	- Update CRM Profile - Capture Trend Data - Confirm Closure

Back | Preview my app | Save & Close | Next

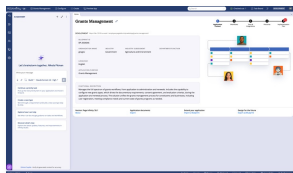
Wie fügt sich Blueprint im Software-Entwicklungszyklus (SDLC) ein?

Beschleunigen Sie Ihre KI-Transformation



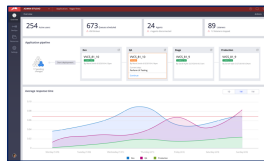
Pega Blueprint™

Zusammenarbeit zwischen Business und IT zur Gestaltung agentenbasierter Workflows und zur Neugestaltung von Arbeitsweisen im Zeitalter von Agenten.



Pega Infinity™
Pega Infinity Studio™

Umfassende Konfiguration von Integration, Automatisierung usw., um Blueprints mit KI-gestützter Entwicklung in vollständige Apps zu verwandeln.



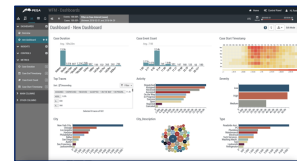
Pega Infinity™
Pega Deployment Manager

Automatisierte DevOps-Pipelines zur Orchestrierung des gesamten Ablaufs, einschließlich Tests, Genehmigungen und Sicherheitsprüfungen.



Pega Infinity™
OOTB-Portal oder DX API

Sicheres Endanwendererlebnis beim Zugriff auf Workflows (mit rollen- und zugriffsbasierten Kontrollen).



Pega Infinity™
Pega Process Mining

Workflow-Analyse auf unentdeckte Lücken und Ineffizienzen in Prozessen.

Neugestaltung

Entwicklung

Tests &
Implementierung

Einsatz

Optimierung

Keine personenbezogenen Daten*

Keine personenbezogenen Daten*

Keine personenbezogenen Daten*

Potenziell sensible Daten

Potenziell sensible Daten

Sicherer Betrieb über die Pega Cloud®

Private-Client-Implementierung

Private-Client-Implementierung

Private-Client-Implementierung

Sicherer Betrieb über die Pega Cloud®

02

Blueprint-Architektur



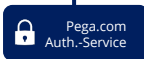
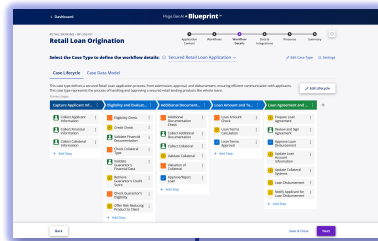
Pega Blueprint™ Architektur

Blueprint wird sicher in der Pega Cloud® auf AWS ausgeführt – mit Management und Betrieb nach führenden Cloud-Standards.

High-Level-Architektur:

- Die Blueprint-Authentifizierung funktioniert über den Single-Sign On (SSO) Ihres Unternehmens.
- Pega bietet geografisch segmentierte Datenresidenz-Services speziell für die Pega Cloud. Bei Blueprint hängt die geografische Region von Ihrem Unternehmensstandort ab (innerhalb der USA, Großbritanniens, der Europäischen Union, Australiens, Singapurs oder Japans).
- Die Blueprint-Verarbeitung erfolgt auf einer sicheren, zuverlässigen Pega Infinity-Anwendung mit der operativen Stärke der Pega Cloud Services. Sie erhalten damit eine Zuverlässigkeit, Compliance, Sicherheit und Notfallwiederherstellung der Enterprise-Klasse.
- Blueprint nutzt LLMs basierend auf dem Anwendungsfall und der Leistung, hauptsächlich Claude-Modelle, die auf AWS Bedrock laufen.
- Mit Ihren Blueprint-Daten wird keine KI trainiert.
- Die Blueprint-Daten werden bei der Übertragung mit TLS verschlüsselt.
- Ihre Blueprint-Daten werden sicher gespeichert, ruhende Daten werden ebenfalls verschlüsselt.

Pega.com Frontend-Web-App



Ihr SSO

Ihre Mitarbeitenden
{Benutzer}@Ihr-Unternehmen.de



US – EU – AUS – UK – JP – SG



Blueprint-Anwendung

Hauptverarbeitung von Benutzeranfragen und Blueprint-Funktionalität

Basiert auf Pega Infinity™



Angewandtes Branchenwissen

Basierend auf der Benutzeranfrage versorgt der Retrieval Augmented Generation Service (RAG) Blueprint mit Informationen zu Best Practices für den Workflow und das Datenmodell.

Basiert auf dem Pega Knowledge Buddy™ und enthält geistiges Eigentum von Pega-Branchenwissen. Kunden- oder Benutzerdaten werden nicht gespeichert.



KI-Orchestrierungs-Service über die Pega Cloud

Orchestriert LLM-Aufrufe

Basiert auf AWS. Speichert keine Prompts, Kunden- oder Benutzerdaten.



AWS Bedrock
Primärer LLM-Anbieter
Claude, Haiku und Sonnet



Google Gemini
Flash



Azure OpenAI
GPT

Blueprint nutzt LLMs basierend auf Anwendungsfall/Leistung. Gesamte Verarbeitung in der Region. Kein KI-Training mit Benutzer- oder Unternehmensdaten.



Sicherer lokaler Datenspeicher

Verschlüsselung von privaten, ruhenden Unternehmensdaten (Data-at-Rest Encryption, DARE)

256-Bit-Verschlüsselung aller auf Datenträgern und in Datenbanken gespeicherten Kundendaten. Standardmäßig werden die Verschlüsselungsschlüssel regelmäßig rotiert und sicher in einem FIPS 140-2-konformen KMS gespeichert.

Private Verschlüsselungsschlüssel für Unternehmen auf Anfrage.



Privater Dateispeicher

Verbindung mit Ihrem Pega Cloud Repository

Alle Dateien bei der Nutzung von Blueprint (wie hochgeladene Dokumentationen oder Videos) werden standardmäßig in einem privaten Pega Cloud File Storage Ordner für Ihr Unternehmen gespeichert. Dieser Ordner wird im Namen des Unternehmens von

Blueprint verwaltet. Die Blueprint-bezogenen Dateien der Pega Cloud-Kunden werden standardmäßig in Ihrem bestehenden privaten Pega Cloud File Storage-Repository gespeichert, das mit Ihrer Pega Cloud-Instanz verknüpft ist.

Pega Blueprint™ – Regionale Datenresidenz (EU, UK, US)

Unternehmen mit Sitz in der Europäischen Union

- Speicherung und Verarbeitung: **AWS EU-Central (Frankfurt)**
- [KI-Modellausführung](#)

Unternehmen mit Sitz in Großbritannien

- Speicherung und Verarbeitung: **AWS EU-West (London)**
- [KI-Modellausführung](#)

Unternehmen mit weltweiten Standorten

- Speicherung und Verarbeitung: **AWS US-East**
- [KI-Modellausführung](#)

Anbieter	Modell/ Anbieter	LLM-Regionen
 AWS Bedrock Primärer Anbieter	Anthropic	AWS Bedrock: EU
 Google Cloud	Gemini	Google Vertex: EU
 Microsoft Azure	OpenAI GPT	Microsoft Azure: EU

Anbieter	Modell/ Anbieter	LLM-Regionen
 AWS Bedrock Primärer Anbieter	Anthropic	AWS Bedrock: Europäische Union
 Google Cloud	Gemini	Google Vertex: EU
 Microsoft Azure	OpenAI GPT	Microsoft: Europäische Union

Anbieter	Modell/ Anbieter	LLM-Regionen
 AWS Bedrock Primärer Anbieter	Anthropic	AWS Bedrock: USA
 Google Cloud	Gemini	Google Vertex: USA
 Microsoft Azure	OpenAI GPT	Microsoft Azure: USA

Für Pega-Partner

Geben Sie auf der Blueprint-Seite für die funktionale Beschreibung im Feld für den Unternehmensnamen an, für wen Sie einen Blueprint erstellen. Diese Blueprints werden dann für dieses Unternehmen automatisch in der Region gespeichert und verwaltet.

So finden Sie die Speicher-Region von Blueprints heraus

Die Blueprint-ID enthält einen Bezeichner für die Region, wenn der Blueprint in der EU, in Australien (AU), in Großbritannien (UK), in Japan (JA) oder in Singapur (SG) gespeichert und verwaltet wird.

Pega Blueprint™ – Regionale Datenresidenz (Asien-Pazifik – APAC)

Unternehmen mit Sitz in

Australien

- Speicherung und Verarbeitung: **AWS: Australien – Sydney**
- [KI-Modellausführung](#)

Anbieter	Modell/ Anbieter	LLM-Regionen
 AWS Bedrock Primärer Anbieter	Anthropic	AWS Bedrock: Australien
 Google Cloud	Gemini	Google Vertex: Australien
 Microsoft Azure	OpenAI GPT	Microsoft Azure: Australien

Unternehmen mit Sitz in

Japan

- Speicherung und Verarbeitung: **AWS: Japan – Osaka**
- [KI-Modellausführung](#)

Anbieter	Modell/ Anbieter	LLM-Regionen
 AWS Bedrock Primärer Anbieter	Anthropic	AWS Bedrock: Japan/Asien- Pazifik
 Google Cloud	Gemini	Google Vertex: Japan
 Microsoft Azure	OpenAI GPT	Microsoft Azure: Japan/Europäi- sche Union

Unternehmen mit Sitz in

Singapur

- Speicherung und Verarbeitung: **AWS: Singapur**
- [KI-Modellausführung](#)

Anbieter	Modell/ Anbieter	LLM-Regionen
 AWS Bedrock Primärer Anbieter	Anthropic	AWS Bedrock: Asien-Pazifik
 Google Cloud	Gemini	Google Vertex: Singapur
 Microsoft Azure	OpenAI GPT	Microsoft Azure: EU

Für Pega-Partner

Geben Sie auf der Blueprint-Seite für die funktionale Beschreibung im Feld für den Unternehmensnamen an, für wen Sie einen Blueprint erstellen. Diese Blueprints werden dann für dieses Unternehmen automatisch in der Region gespeichert und verwaltet.

So finden Sie die Speicher-Region von Blueprints heraus

Die Blueprint-ID enthält einen Bezeichner für die Region, wenn der Blueprint in der EU, in Australien (AU), in Großbritannien (UK), in Japan (JA) oder in Singapur (SG) gespeichert und verwaltet wird.

03

Zugriff und Authentifizierung



Pega Blueprint™

Zugriff und Authentifizierung

Blueprint-Zugriff mit Ihrem Single Sign-on (SSO)

Benutzer können zur Authentifizierung den Identitätsanbieter (IDP) Ihres Unternehmens verwenden. Dann können nur berechtigte Benutzer auf ALLE Pega-Websites und -Anwendungen zugreifen (z. B. Blueprint, Support-Portal).

Ist für die Anmeldung die föderierte Authentifizierung aktiviert, müssen Benutzer kein Passwort eingeben und werden zur Authentifizierung direkt zum Identitätsanbieter weitergeleitet.

Zur Aktivierung der föderierten Authentifizierung können sich IT-Leiter gern an unser Account-Team wenden.

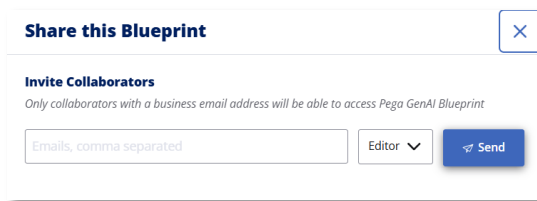
Das brauchen wir von Ihnen: **Konfigurationsdetails** für **SAML 2.0** oder **OAuth**.

Zur Anmeldung bei den folgenden Anwendungen wird die föderierte Authentifizierung verwendet: Blueprint, Pega.com, community.pegacom, academy.pegacom, support.pegacom, docs.pegacom, partners.pegacom, saleshub.pegacom, partner-logo-generator.pegacom, My Support Portal, My Pega Cloud, My Pega, PDC, Deployment Manager, Pega Trials

Nur der Ersteller sieht die Blueprints – Freigaben müssen aktiv erfolgen

Standardmäßig kann nur der Ersteller (der *Blueprint-Besitzer*) seinen Blueprint sehen.**

Blueprint-Besitzer können den Blueprint mit anderen teilen (z. B. Kollegen, Partnern) und auch andere Benutzer per E-Mail als *Bearbeiter* oder *Betrachter* einladen.



Verlässt ein Benutzer Ihr Unternehmen, bleiben die Blueprints bei Ihnen

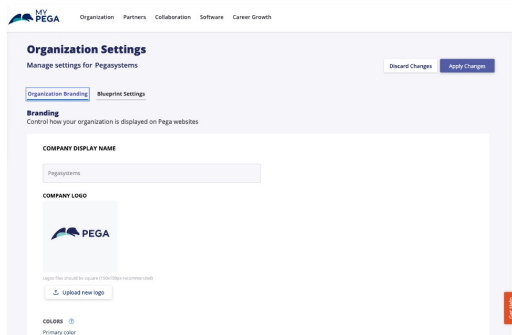
Wenn ein Unternehmen die föderierte Authentifizierung über seinen SSO mit digitalen Pega-Lösungen (wie Blueprint) verwendet, können sich nur Benutzer mit aktivem SSO-Zugriff bei Blueprint anmelden.

Ändert ein Benutzer die eingetragene Domain in seinem Profil auf Pega.com – z. B. beim Wechsel der Organisation –, können die für die alte Domain erstellten Blueprints nicht mehr angezeigt werden.

Der Zugriff auf diese Blueprints kann für andere Benutzer in der Organisation auf Anfrage wiederhergestellt werden.

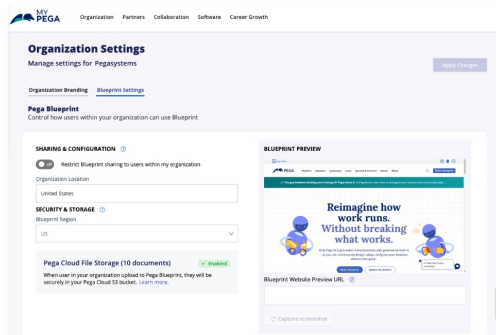
Pega Blueprint™

Kontrollbereich für Organisationen



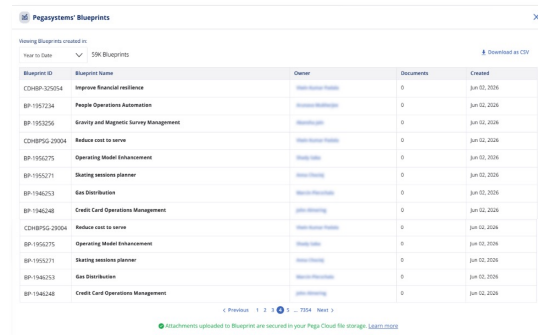
Organisations-Branding anpassen

Behalten Sie die volle Kontrolle über den Anzeigenamen, die Farben und das Logo Ihres Unternehmens. Der Blueprint-Administrator hat die volle Kontrolle, um das Branding zu aktualisieren und die Produktion-Implementierung von Anwendungen zu beschleunigen, wobei das gesamte Branding berücksichtigt wird.



Speicherung und Freigabe verwalten

Sie können voll auf die Sicherheitskontrollen für Blueprints vertrauen, da Sie die Freigabe von Blueprints außerhalb Ihres Unternehmens einschränken können. Prüfen Sie den Organisationsstandort und wählen Sie die Region für Datenresidenz und Datenspeicherung aus.



Transparenz bei Organisations-Blueprints

Volle Transparenz über Blueprint-IDs, Ersteller, Namen, Dokumente und Erstellungsdaten in Ihrem gesamten Unternehmen.

Um die administrativen Blueprint-Funktionen über „My Pega“ für Ihre Organisation **zu aktivieren**, wenden Sie sich an Ihren Client Success Manager (CSM) oder kontaktieren Sie Support@accounts.pegacom mit den relevanten Organisations-Administratoren.

04

Datenschutz



Pega Blueprint™ Datenverarbeitung

Was wird erfasst und wie erfolgt die Verarbeitung?

Nr.	Datenpunkt	Format	Verarbeitet vom LLM?	Verwendet für KI-Training?	Speicherort	Sichtbar für ...
1	Ersteller-Informationen	Metadaten (Name, E-Mail, Unternehmen)	Nein	Nein	Pega Cloud-Datenspeicher Vollständig verschlüsselt*	Pega
2	App-Beschreibung	Metadaten (Branche, App-Name)	Ja	Nein	Pega Cloud-Datenspeicher Vollständig verschlüsselt*	Pega
3	Anwendungsbeschreibung (Text)	Verschlüsselter Text	Ja	Nein	Pega Cloud-Datenspeicher Vollständig verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
4	Vorhandene Dokumentation	.PDF, .DOC, .DOCX, .md	Ja	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
5	Vorhandene Videos und Bilder	.MOV, .MP4, .JPG, .PNG, .jpeg, .avi	Ja	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
6	Prozessdiagramme	.BPMN, .jpm, .jpeg	Ja	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
7	Integration und Datendokumentation	.YAML, .SQL, .DDL, .CRD	Ja	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
8	Codeanalyse-Dokumente	AWS Transform, Google MAT, NotestoBlueprint, .Blueprint	Ja	Np	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
9	Blueprint-Bearbeitungen und -Endversionen	Verschlüsselte Metadaten (exportiert als verschlüsselte Blueprint-Datei)	Nein	Nein	Pega Cloud-Datenspeicher Vollständig verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**

*Blueprint-Daten können auf Anfrage dauerhaft vom Pega-Support gelöscht werden.

**Nur für autorisiertes administratives Personal von Pega Cloud Operations sichtbar.

05

Cloud-Sicherheit





Pega Blueprint läuft auf den bewährten Pega Cloud® Services. Das gewährleistet eine Sicherheit der Enterprise-Klasse.

Transformation, auf die Sie vertrauen können

- Betriebsüberwachung, Management und Support rund um die Uhr an allen Tagen der Woche
- Secure-by-Design-Architekturabläufe mit strengen Zugriffskontrollen, operativen Schutzmaßnahmen und Automatisierung für minimale manuelle Eingriffe
- Compliance auf Enterprise-Ebene, Ausfallsicherheit, Notfallwiederherstellung und Bedrohungsmodellierung

Überwachung, Unterstützung der Umgebung und proaktive Reaktion rund um die Uhr

Zugriff

Umgebungs-Governance mit automatisierten operativen Kontrollen und strengen Zugriffsprotokollen

Details

Compliance

Strikte Einhaltung von über 20 Industriestandards

Details

Notfallwiederherstellung

Umfassende Backups, Failover und Wiederherstellung für Daten und Services

Details

Bedrohungsmodellierung

Befolgung der Red-Team-Methode basierend auf den OWASP Top 10

Details

Verfügbarkeit

Architektur mit integrierter Hochverfügbarkeit und Notfallwiederherstellung für nahezu ununterbrochene Verfügbarkeit

Details

06

KI-Governance





Pega Blueprint™ nutzt Spitzenmodelle für eine schnellere KI-Transformation

Alle Modelle werden auf sichere Weise gemanagt und in das Produkt integriert, damit das Verhältnis von Effektivität und Performance stimmt.

Stand: 3. Quartal 2025

Pega bewertet unablässig LLMs, damit wir sicher das richtige Modell für die richtige Aufgabe einsetzen. Derzeit basieren unsere Produkte und Lösungen auf folgenden Modellen:

Hyperscaler	LLM-Anbieter	Blueprint-Region	LLM-Region
 AWS Primärer Anbieter	Anthropic Claude Sonnet 4.5	AMS (USA)	AWS Bedrock: USA
		EU	AWS Bedrock: EU
		UK	AWS Bedrock: UK
 Google Cloud	Google Gemini	AMS (USA)	Google Vertex: USA
		EU	Google Vertex: EU
		UK	Google Vertex: UK
 Microsoft Azure	OpenAI – GPT	AMS (USA)	Microsoft Azure: USA
		EU	Microsoft Azure: EU
		UK	Microsoft Azure: UK

Alle Vereinbarungen mit Hyperscalern umfassen Verpflichtungen, dass weder der Hyperscaler noch der LLM-Provider Prompts oder Daten von Pega oder Kunden erhalten oder darauf zugreifen.

*Stand Juni 2025

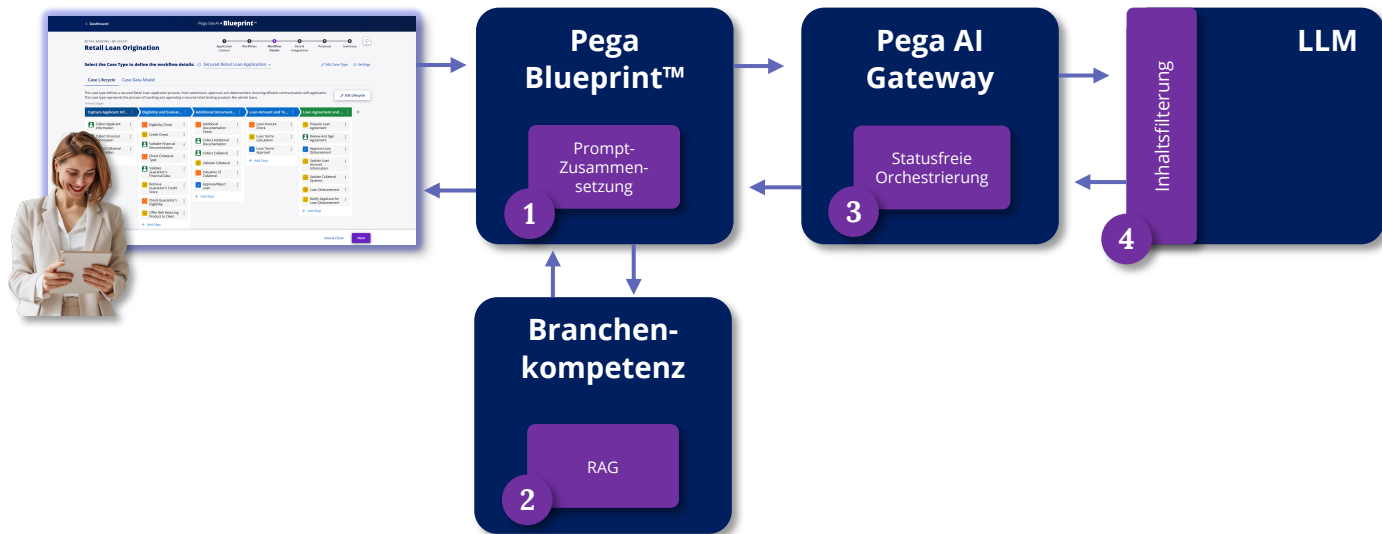
**Aktuellste Version auf pega.com/de

Datenfluss

Pega Blueprint™

Sicherer, geschützter KI-Einsatz:

1. Pega Blueprint **erstellt Prompts**, die die Anwendung basierend auf den Benutzereingaben beschreiben.
2. Pega Blueprint ruft mit aus der Pega-Wissensdatenbank spezielle **Informationen zur Branche** ab. Das Ganze läuft auf dem Pega Knowledge Buddy, der bewährte Branchenmethoden für den Blueprint-Anwendungsfall zusammenstellt, LLM-Prompts ergänzt und den Blueprint erstellt.
3. Alle LLM-Aufrufe laufen über den **Pega AI Gateway Service** der Pega Cloud, der eine vertrauenswürdige Sicherheits-, Segmentierungs- und Skalierbarkeitsebene für die Kommunikation mit LLM-Anbietern bereitstellt.
4. Wird ein verschlüsselter Prompt an ein sicheres LLM gesendet, wird der **Inhalt gefiltert**. So lassen sich schädliche Inhalte in Prompts und Vervollständigungen erkennen und vermeiden.



So funktioniert die Inhaltsfilterung

Pega nutzt die bewährtesten Anbieter von großen Sprachmodellen (LLM) für Pega-Funktionen, die auf generativer KI basieren. In jedem dieser LLMs sind robuste Inhaltsfilter integriert, die schädliche, unethische oder toxische Antworten auf ein Minimum reduzieren. Dennoch kann es in seltenen Fällen zu Ausrutschern kommen, weil eine Filterung keine garantierte Entfernung solcher Inhalte darstellt. Da jeder LLM-Anbieter einen anderen Ansatz für eine verantwortungsvolle, ethische KI verfolgt,

können sich die Klassifizierungsmodelle, Schwellenwerte und Erkennungskategorien unterscheiden. Für jedes Modell wird eine andere Inhaltsklassifizierung und -filterung angewendet. Wenn Kunden z. B. Pega GenAI Connect nutzen, sollten sie sich dieser möglichen Unterschiede bewusst sein und entsprechende Tests durchführen.

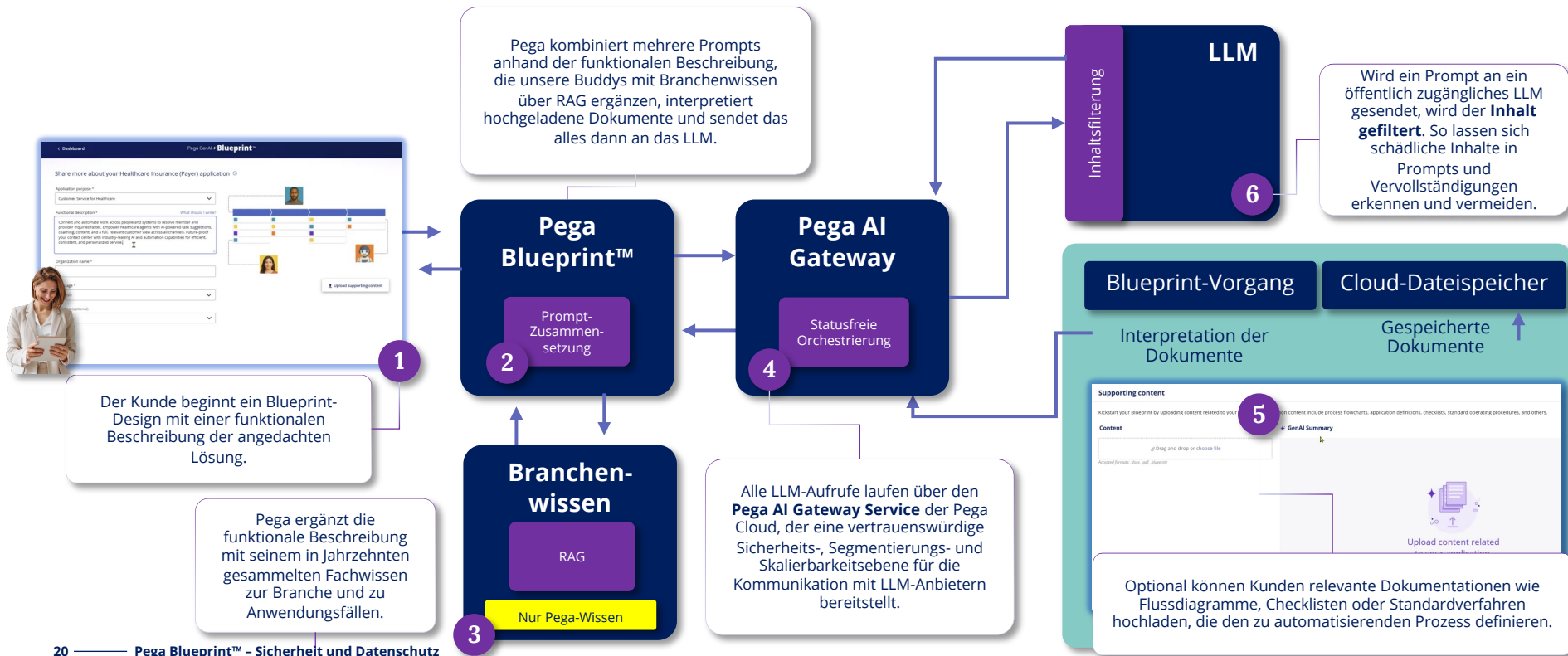
Datenfluss

Pega Blueprint™

So funktioniert die Inhaltsfilterung

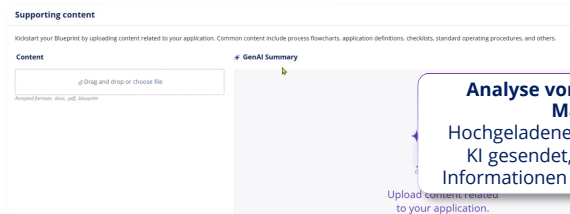
Pega nutzt die Spitzenanbieter von großen Sprachmodellen (LLM) für Pega-Funktionen, die auf generativer KI basieren. In jedem dieser LLMs sind robuste Inhaltsfilter integriert, die schädliche, unethische oder toxische Antworten auf ein Minimum reduzieren. Dennoch kann es in seltenen Fällen zu Ausrutschern kommen, weil eine Filterung keine garantierte Entfernung solcher Inhalte darstellt. Da jeder LLM-Anbieter einen anderen Ansatz für eine verantwortungsvolle, ethische KI verfolgt,

können sich die Klassifizierungsmodelle, Schwellenwerte und Erkennungskategorien unterscheiden. Für jedes Modell wird eine andere Inhaltsklassifizierung und -filterung angewendet. Wenn Kunden z. B. Pega GenAI Connect nutzen, sollten sie sich dieser möglichen Unterschiede bewusst sein und entsprechende Tests durchführen.

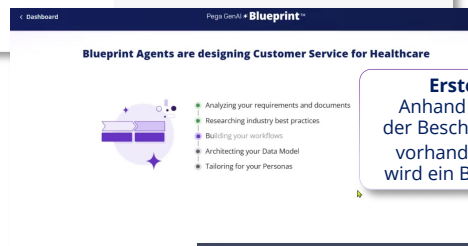


Datenfluss

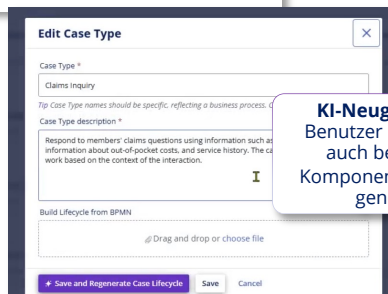
Pega Blueprint™



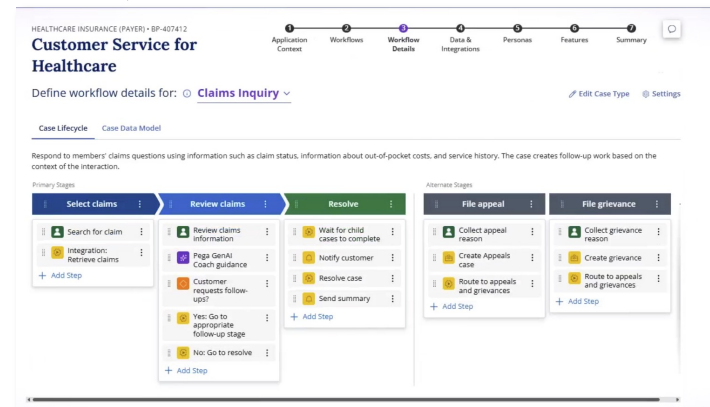
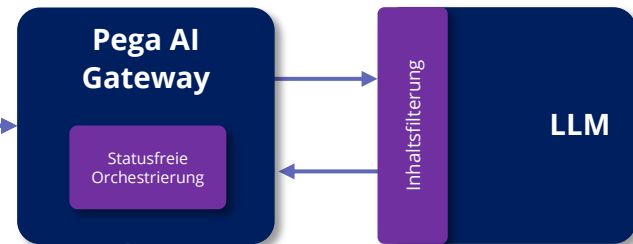
Analyse von vorhandenem Material
Hochgeladenes Material wird zur KI gesendet, die Insights und Informationen an Blueprint liefert.



Erster Entwurf
Anhand der KI-Analyse der Beschreibung und des vorhandenen Materials wird ein Blueprint erstellt.



KI-Neugenerierung
Benutzer können die KI auch beauftragen, Komponenten erneut zu generieren.



KI-Governance bei Pega

Lückenlose Aufsicht

Das KI-Governance-Gremium des Cloud-Sicherheitsteams beaufsichtigt die gesamte Nutzung von KI in Pega-Produkten.

Dem Gremium gehören Experten und Verantwortliche aus den Bereichen Produkt, Cloud-Sicherheit, Cloud Operations, IT, Rechtswesen und Go-To-Market an, die dafür sorgen, dass KI bei Pega sicher und verantwortungsvoll eingesetzt wird.

Strategische Partnerschaften

Für die einzigartigen Anforderungen von Unternehmen hat Pega strategische Partnerschaften und übergreifende Vereinbarungen zu gemeinsamen KI-Initiativen mit AWS, Google Cloud, und Microsoft getroffen.

Pega und seine Cloud-LLM-Anbieter treffen sich regelmäßig zum Austausch über Modelloptionen, Probleme sowie Performance- und Sicherheitsfragen.

Sicherheit an erster Stelle

Das KI-Governance-Gremium bei Pega organisiert und erarbeitet ständige Sicherheitsbewertungen aller KI-Funktionen – auch von Pega Blueprint.

Die Sicherheitsbewertungen umfassen u. a.:

1. ISO 42001
2. die KI-Red-Team-Methode von Microsoft
3. bewährte Sicherheitsmethoden von OpenAI
4. von Microsoft verlangte Abhilfemaßnahmen
5. OWASP Top 10 für LLM-Anwendungen
6. OWASP Top 10 für cloudnative Anwendungssicherheit





Pega ist führend bei der Umsetzung digitaler Transformationen und unterstützt Unternehmen mit KI-Entscheidungsfindung und -Workflow-Automatisierung – ganz nach unserem Motto: Build for Change®. Viele der weltweit einflussreichsten Unternehmen verlassen sich auf unsere Plattform, um ihre dringlichsten Herausforderungen zu lösen – von personalisierten Kundenbeziehungen über Service-Interaktionen bis hin zur Optimierung von Betriebsabläufen. Unsere skalierbare und flexible Architektur unterstützt Unternehmen seit 1983, die strategischen Anforderungen ihrer Kunden effizient zu erfüllen und gleichzeitig mit neuen Technologien Schritt zu halten. Weitere Informationen zu Pega (NASDAQ: PEGA) finden Sie unter <http://www.pegacom/de>