



Transformation, auf die Sie *vertrauen* können

Wie Pega Blueprint Daten, Datenschutz
und KI sicher handhabt

— Pega Blueprint™ – Sicherheit und Datenschutz

Dashboard Pega GenAI • Blueprint™

RETAIL BANKING - BP-206181

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. [Edit Lifecycle](#)

Primary Stages:

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
<ul style="list-style-type: none">Collect Applicant InformationCollect Financial InformationCollect Collateral Information + Add Step	<ul style="list-style-type: none">Eligibility CheckCredit CheckValidate Financial DocumentationCheck Collateral TypeValidate Guarantor's Financial DataRetrieve Guarantor's Credit ScoreCheck Guarantor's EligibilityOffer Risk Reducing Product to Client + Add Step	<ul style="list-style-type: none">Additional Documentation CheckCollect Additional DocumentationCollect CollateralValidate CollateralValuation of CollateralApprove/Reject Loan + Add Step	<ul style="list-style-type: none">Loan Amount CheckLoan Terms CalculationLoan Terms Approval + Add Step	<ul style="list-style-type: none">Prepare Loan AgreementReview and Sign AgreementApprove Loan DisbursementUpdate Loan Account InformationUpdate Collateral SystemsLoan DisbursementNotify Applicant for Loan Disbursement + Add Step

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

Inhalt

01 Was ist Pega Blueprint?

Benutzer
Betriebsmodell
Geschäftswert

02 Blueprint-Architektur

Cloud-Architektur
Bereitstellungsregionen

03 Zugriff und Authentifizierung

Anwenderverwaltung
Single Sign-on (SSO)
Berechtigungen

04 Datenschutz

Datenfluss
Speicher und Verschlüsselung
Sichtbarkeit und Zugriff

05 Cloud-Sicherheit

Abläufe
Bedrohungsmodellierung
Notfallwiederherstellung

06 KI-Governance

LLM-Nutzung
Risiken und Kontrollen
LLM-Governance



Pega Blueprint™ Sicherheit und Datenschutz

Bei der Entwicklung von Pega GenAI 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 Ihren Single-Sign-on (SSO) gebunden werden.

- Blueprint regelt den Datenzugriff mit rollenbasierten Zugriffskontrollen. So sind Blueprints nur für den Ersteller zugänglich – es sei denn, sie werden aktiv freigegeben.
- Wenn ein Benutzer Ihr Unternehmen verlässt, 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 mehrere 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 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, Name des Erstellers).

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

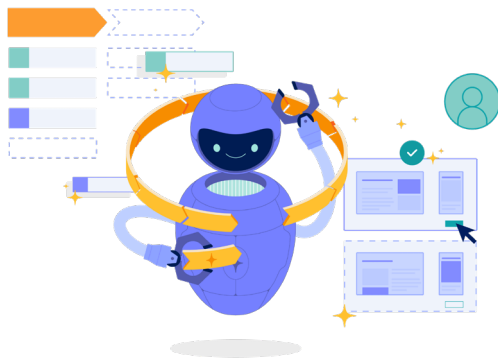
Was ist Pega Blueprint?



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.



Retail Loan Origination

Select the Case Type to define the workflow details: [Secured Retail Loan Application](#) [Edit Case Type](#) [Settings](#)

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. [Edit Lifecycle](#)

Primary Stages

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
<ul style="list-style-type: none">Collect Applicant InformationCollect Financial InformationCollect Collateral Information + Add Step	<ul style="list-style-type: none">Eligibility CheckCredit CheckValidate Financial DocumentationCheck Collateral TypeValidate Guarantor's Financial DataRetrieve Guarantor's Credit ScoreCheck Guarantor's EligibilityOffer Risk Reducing Product to Client + Add Step	<ul style="list-style-type: none">Additional Documentation CheckCollect Additional DocumentationCollect CollateralValidate CollateralValuation of CollateralApprove/Reject Loan + Add Step	<ul style="list-style-type: none">Loan Amount CheckLoan Terms CalculationLoan Terms Approval + Add Step	<ul style="list-style-type: none">Prepare Loan AgreementReview and Sign AgreementApprove Loan DisbursementUpdate Loan Account InformationUpdate Collateral SystemsLoan DisbursementNotify Applicant for Loan Disbursement + Add Step

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



Wie funktioniert das?



1. Schnellere Analyse von Altsystemen

Statt manuell Altsysteme zu analysieren, werden **alle wichtigen Informationen automatisch extrahiert** – indem Sie einfach Ausgangsmaterial hochladen wie:

- **Dokumentationen** (z. B. SOP)
- **Quellcode**-Analysen
- **Videos** und Screenshots

3.

Nahtlose Zusammenarbeit

Blueprint ist ideal für die Zusammenarbeit. Fügen Sie einfach alle **beteiligten IT- und Geschäftsanwender** hinzu und profitieren Sie von:

- **schneller Anpassung** von KI-Vorschlägen
- Erfassung der Anforderungen in **natürlicher Sprache**
- einer ständig verfügbaren **App-Vorschau**

2.

Best Practices als Grundlage

Je nach Ihren Anforderungen wird von den KI-Agenten hinter Blueprint **eine erste Anwendung als Ausgangspunkt zusammengestellt**, die hierauf basiert:

- Best Practices der **Branche**
- **Fachwissen** von Pega und seinen Partnern
- Organisatorisches **Wissen**

4.

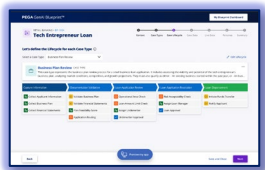
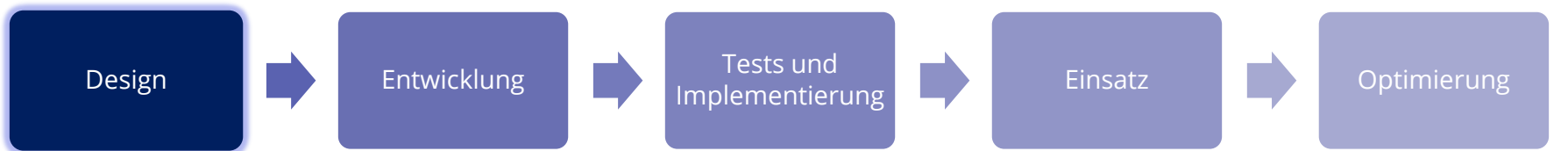
Sofortiger Entwicklungsbeginn

Statt lange alle Anforderungen an Prozesse zusammenzutragen, erhalten Entwickler alles für ein **schnelles Go-Live**:

- Importieren des Blueprint zum **Erstellen der App** in Sekunden
- automatische Erstellung des **User Story Backlogs**
- Nutzung von KI im gesamten Pega App Studio zur **schnellen Finalisierung und Bereitstellung der neuen App**

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

Schnelles Design für schnelle Entwicklung

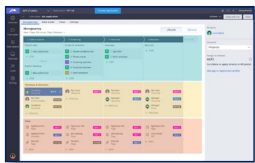


Pega Blueprint™

Zusammenarbeit von Geschäftsanwendern und IT zur Beschleunigung des ersten Workflow-Designs mit GenAI

Keine personenbezogenen Daten*

Sicherer Betrieb über die Pega Cloud®

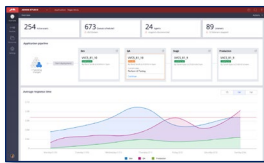


Pega Infinity™
Pega App Studio

Umfassende Konfiguration der Integration, Automatisierung usw. zur Erstellung fertiger Apps basierend auf Ihrem Blueprint

Keine personenbezogenen Daten*

Private-Client-Implementierung



Pega Infinity™
Pega Deployment Manager

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

Keine personenbezogenen Daten*

Private-Client-Implementierung

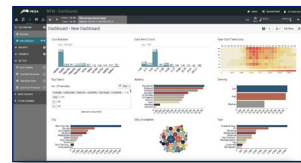


Pega Infinity™

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

Potenziell sensible Daten

Private-Client-Implementierung



Pega Infinity™
Pega Process Mining

Workflow-Analyse auf unentdeckte Lücken und Ineffizienzen in Prozessen

Potenziell sensible Daten

Sicherer Betrieb über die Pega Cloud®

*Anwendungsfälle basierend auf der Designzeit. In all diesen Phasen sollten keine personenbezogenen Daten verwendet werden.

02

Blueprint-Architektur



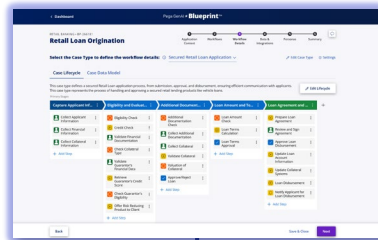
Pega Blueprint™ Architektur

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 (US-East, UK oder EU).
- 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/de Frontend-Web-App



Pega.com/de Auth.-Service

Ihr SSO

Ihre Mitarbeitenden
{Benutzer}@{Ihr-Unternehmen}.de



Vollständig isoliert in der jeweiligen Region:
US – UK – EU

PEGA Cloud® AWS



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 S3-Bucket für Ihr Unternehmen gespeichert. Dieser S3-Bucket wird im Namen des Unternehmens von Blueprint verwaltet.

Kunden, die die Pega Cloud verwenden, können auf Anfrage auch Dateien für Blueprint im privaten S3-Repository ihrer Pega Cloud-Instanz speichern.

Pega Blueprint™ – Regionale Datenresidenz

Unternehmen mit Sitz in der Europäischen Union

- Speicher und Verarbeitung: **AWS EU-Central (Frankfurt)**
- [KI-Modellausführung](#): in der Region

Anbieter	Modell/ Anbieter	LLM- Regionen
 AWS Bedrock <small>Primärer Anbieter</small>	Anthropic	AWS Bedrock: EU
 Google Gemini	Flash	Google Vertex: EU
 Microsoft Azure	GPT	Microsoft Azure: EU



Unternehmen mit Sitz in Großbritannien

- Speicher und Verarbeitung: **AWS EU-WEST-2 (London)**
- [KI-Modellausführung](#): in der Region

Anbieter	Modell/ Anbieter	LLM- Regionen
 AWS Bedrock <small>Primärer Anbieter</small>	Anthropic	AWS Bedrock: UK
 Google Gemini	Flash	Google Vertex: UK
 Microsoft Azure	GPT	Microsoft Azure: UK




Unternehmen mit Sitz in Australien

- Speicher und Verarbeitung: **AWS AP-SOUTHEAST-2 (Sidney)**
- [KI-Modellausführung](#): in der Region

Anbieter	Modell/ Anbieter	LLM- Regionen
 AWS Bedrock <small>Primärer Anbieter</small>	Anthropic	AWS Bedrock: Sidney
 Google Gemini	Flash	Google Vertex: Schweden
 Microsoft Azure	GPT	Microsoft Azure: Schweden

Unternehmen mit globalen Standorten

- Speicher und Verarbeitung: **AWS US-East**
- [KI-Modellausführung](#): in der Region

Anbieter	Modell/ Anbieter	LLM- Regionen
 AWS Bedrock <small>Primärer Anbieter</small>	Anthropic	AWS Bedrock: USA
 Google Gemini	Flash	Google Vertex: USA
 Microsoft Azure	GPT	Microsoft Azure: USA

Für Pega-Partner

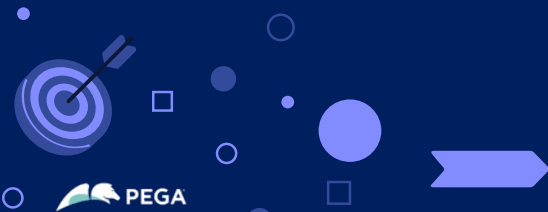
Geben Sie auf der Blueprint-Seite für die funktionale Beschreibung im Feld für den Unternehmensnamen an, für wen Sie einen Blueprint erstellen. Diese Blueprints werden dann für dieses Unternehmen automatisch in der Region gespeichert und verwaltet.

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) oder in Großbritannien (UK) gespeichert und verwaltet wird.

03

Zugriff und Authentifizierung



Pega Blueprint™ Zugriff und Authentifizierung

Blueprint-Zugriff mit 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.

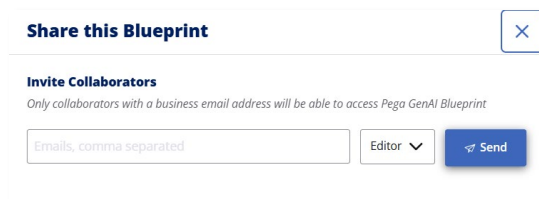
Das brauchen wir von Ihnen: **Konfigurationsdetails** für **SAML 2.0** oder **OAuth**.

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 erstellen Blueprints nicht mehr angezeigt werden.

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

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, für die erste Blueprint-Vorlage	Nein	Pega Cloud-Datenspeicher Vollständig verschlüsselt*	Pega
3	Anwendungsbeschreibung (Text)	Verschlüsselter Text	Ja, für die erste Blueprint-Vorlage	Nein	Pega Cloud-Datenspeicher Vollständig verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
4	Vorhandene Dokumentation	.PDF, .DOC, .DOCX	Ja, für die erste Blueprint-Vorlage	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
5	Vorhandene Videos und Bilder	.MOV, .MP4, .JPG, .PNG	Ja, für die erste Blueprint-Vorlage	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
6	Prozessdiagramme	.BPMN	Ja, für die erste Blueprint-Vorlage	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
7	Integration und Datendokumentation	.YAML, .SQL, .DDL, .CRD	Ja, für die erste Blueprint-Vorlage	Nein	Pega Cloud-Datenspeicher Ruhende Daten verschlüsselt*	Nur Blueprint-Ersteller und Eingeladene**
8	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.

Pega Blueprint™ Datensichtbarkeit

Daten bleiben vertraulich

Die Details Ihrer Blueprints werden in einer verschlüsselten Datenbank gespeichert. Diese Details sind nur für autorisiertes administratives Personal von Pega sichtbar. Und mit den Daten, die Sie in Blueprint eingeben, wird keines der von uns verwendeten KI-Modelle trainiert. Keine Daten (Prompts oder Antworten) werden mit LLM-Anbietern geteilt oder sind für Cloud-Anbieter zugänglich. Informationen bleiben ausschließlich bei Ihnen.



Was sehen die Nutzer bei Pega?

Nur das Mindeste, um das System am Laufen zu halten und uns zu helfen, mit Ihnen in Kontakt zu treten, wenn Sie Hilfe benötigen:

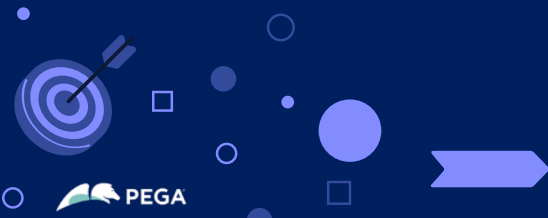
- Die vom **System generierte Blueprint-ID**. Ihr Blueprint erstellt einen Pega-Vorgang, und das ist die Vorgangs-ID.
- Die **E-Mail-Adresse** der Person, die Ihren Blueprint erstellt hat
- Den **Kurznamen**, den Sie für Ihren Blueprint angegeben haben

Und alles andere?

Alles bleibt vollkommen privat: Ihre Prozessbeschreibungen, Workflows, Datenmodelle und alle von Ihnen hochgeladenen Dokumente – einschließlich Anwendungsdokumente, BPMN-Dateien, API-Definitionen oder Integrationskonfigurationen – bleiben wie beschrieben geheim.

05

Cloud-Sicherheit





Mehr Infos im Pega Cloud Trust Center

Pega Blueprint™ 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-Niveau, Ausfallsicherheit, Notfallwiederherstellung und Bedrohungsmodellierung

Abläufe

Zugriff

Compliance

Notfallwiederherstellung

Bedrohungsmodellierung

Verfügbarkeit

Überwachung, Unterstützung der Umgebung und proaktive Reaktion 24/7

[Details](#)

Umgebungs-Governance mit automatisierten operativen Kontrollen und strengen Zugriffsprotokollen

[Details](#)

Strikte Einhaltung von über 20 Industriestandards

[Details](#)

Umfassende Backups, Failover und Wiederherstellung für Daten und Services

[Details](#)

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

[Details](#)

Architektur mit integrierter Hochverfügbarkeit und Notfallwiederherstellung für nahezu ununterbrochene Verfügbarkeit

[Details](#)

The screenshot shows the Pega Cloud Trust Center website. At the top, there's a navigation bar with links like Platform, Solutions, Customers, Learn, Services & Partners, Events, and About. Below this is a header section with the text 'Pega Trust Center' and a sub-header 'Secure. Reliable. Compliant. Pega Cloud empowers the world's biggest brands to meet - and exceed - the challenges of today and tomorrow. Learn how.' There's a search bar and a '7/7 Pega' button. The main content area is divided into sections: 'Learn more about Pega's security features.' with links for Security, Privacy, Compliance, WAFs, and Service reliability. The 'Security' section is expanded, showing sub-sections like Authorization & access, Network protection, Secure system integration, Client-based access control, and Data encryption. Each sub-section has a brief description and a 'View security bulletins' link. Below this is a 'Supporting security documents' section with a list of documents including 'Open Security Policies', 'Veracode Statement', 'Penetration Test Summaries', 'Business Continuity Plan Summary', and 'Disaster Recovery Test Results'. The 'Privacy' section is also visible, with a 'Read Pega's privacy notice' link. At the bottom, there's a 'Compliance certifications, attestations, and accessibility' section with a table listing various certifications like APRA, CS, CSA STAR, Cyber Essentials, Cyber Essentials Plus, CyberGIX, Cybervaldis, and ENX.

Resources	Last updated (YYYY-MM-DD)	Assessment scope
Open Security Policies	2024-12-27	Pega Cloud AWS, GCP
Veracode Statement	N/A	Pega Cloud AWS, GCP
Penetration Test Summaries	2024-09-17	Pega Cloud AWS, GCP
Business Continuity Plan Summary	2024-05-03	Pega Cloud AWS, GCP
Disaster Recovery Test Results	2024-12-09	Pega Cloud AWS, GCP

Compliance certifications, attestations, and accessibility	
Pega Cloud certifications	
APRA	▼
CS	▼
CSA STAR	▼
Cyber Essentials	▼
Cyber Essentials Plus	▼
CyberGIX	▼
Cybervaldis	▼
ENX	▼

06

KI-Governance








Pega Blueprint™ nutzt mehrere Frontier-Modelle – ideal für eine schnelle 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	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

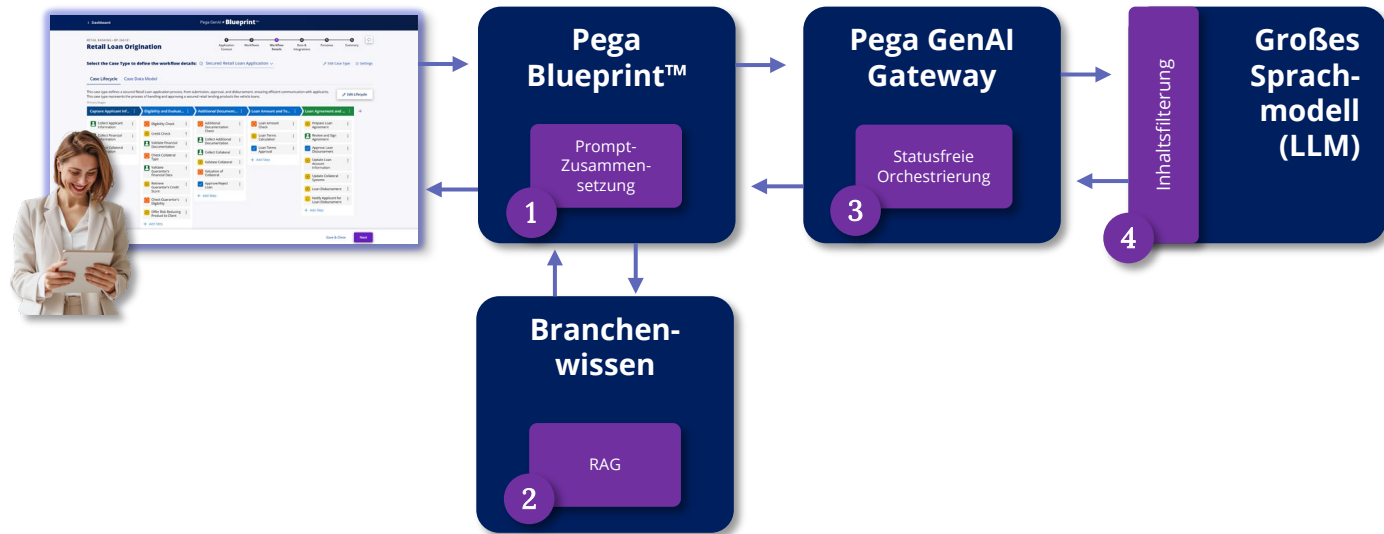
**Aktuellste Version auf pega.com/de

KI-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 GenAI 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.

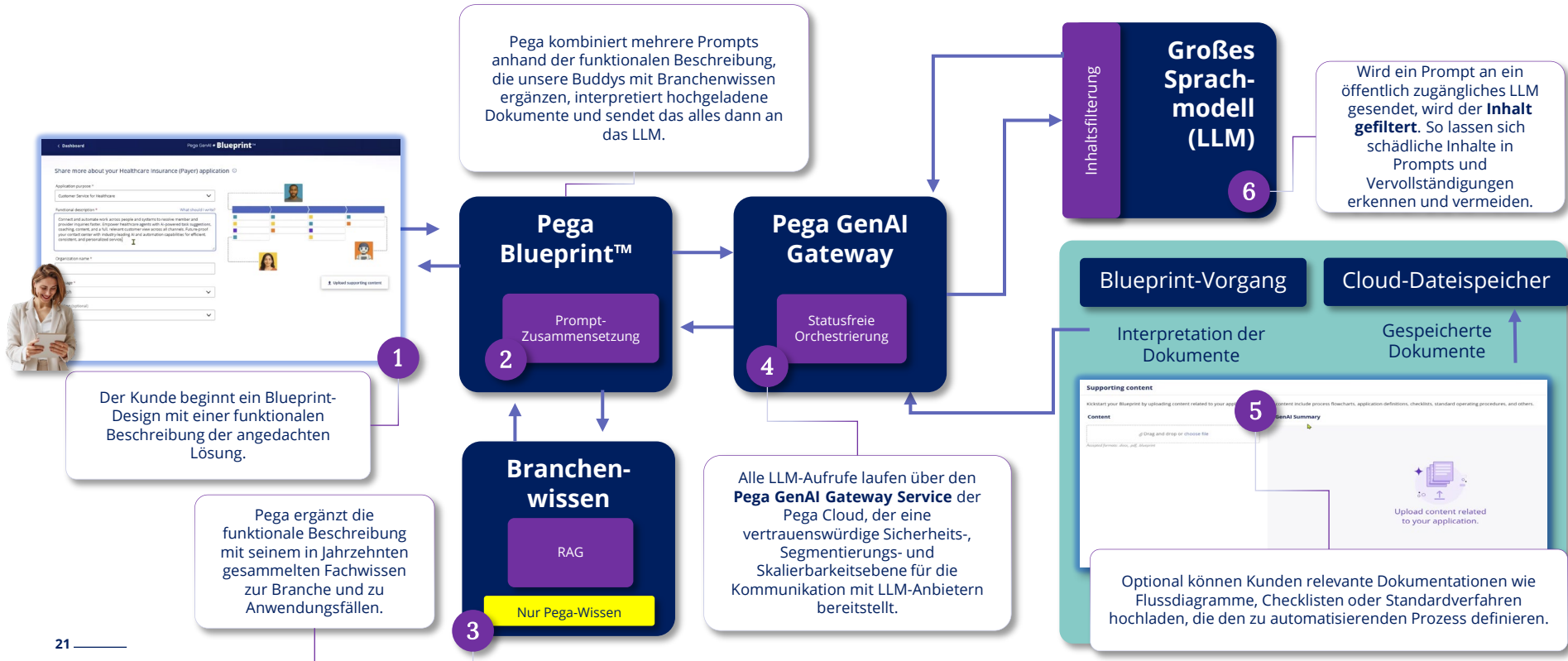
KI-Datenfluss

Pega Blueprint™

So funktioniert die Inhaltsfilterung

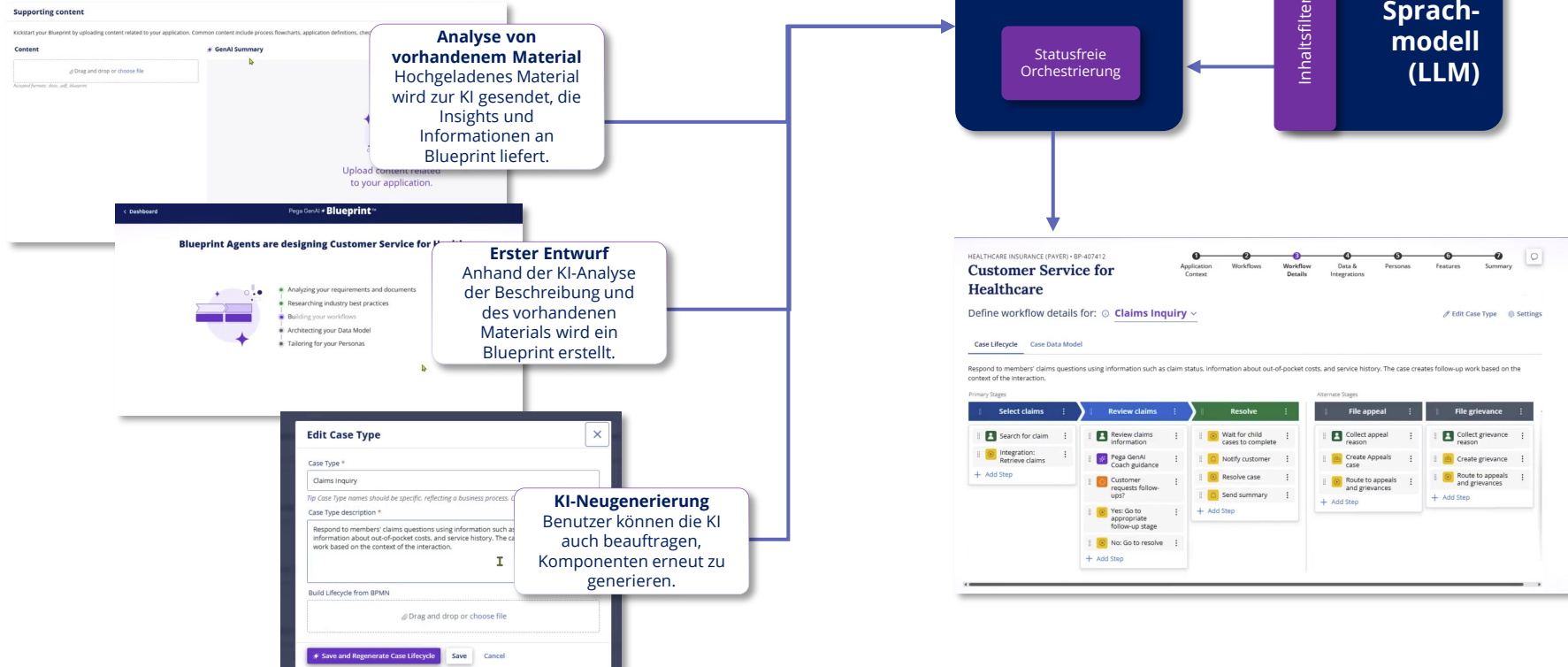
Pega nutzt die bewährtesten Anbieter von großen Sprachmodellen (LLM) für Pega-Funktionen, die auf generativer KI basieren. In jedem dieser LLMs sind robuste Inhaltsfilter integriert, die schädliche, unethische oder toxische Antworten auf ein Minimum reduzieren. Dennoch kann es in seltenen Fällen zu Ausrutschern 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.



KI-Datenfluss

Pega Blueprint™



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. die KI-Red-Team-Methode von Microsoft
2. bewährte Sicherheitsmethoden von OpenAI
3. von Microsoft verlangte Abhilfemaßnahmen
4. OWASP Top 10 für LLM-Anwendungen
5. 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.pegas.com/de>