



# Transformation you can *trust*.

How Pega Blueprint securely manages  
data, privacy, and AI.

— Pega Blueprint™ Security & Privacy

The image shows a woman in a white blazer smiling and holding a tablet. Behind her is a large screen displaying the Pega Blueprint interface for Retail Loan Origination. The interface includes a navigation bar with 'Dashboard' and 'Pega GenAI • Blueprint™'. The main content area is titled 'Retail Loan Origination' and shows a workflow diagram with steps: 'Application Context', 'Workflows', and 'Workflow Details'. Below the diagram, there's a section 'Select the Case Type to define the workflow details:' with a dropdown menu set to 'Secured Retail Loan Application'. The interface also displays a 'Case Lifecycle' and 'Case Data Model' section. A detailed list of steps is shown, including 'Capture Applicant Information', 'Eligibility and Evaluation', 'Additional Documentation', 'Loan Amount and Terms', and 'Loan Agreement and Disbursement'. Each step has a list of sub-tasks, such as 'Collect Applicant Information', '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', 'Additional Documentation Check', 'Collect Additional Documentation', 'Collect Collateral', 'Validate Collateral', 'Valuation of Collateral', 'Approve/Reject Loan', 'Loan Amount Check', 'Loan Terms Calculation', 'Loan Terms Approval', 'Prepare Loan Agreement', 'Review and Sign Agreement', 'Approve Loan Disbursement', 'Update Loan Account Information', 'Update Collateral Systems', 'Loan Disbursement', and 'Notify Applicant for Loan Disbursement'. The interface also includes buttons for 'Add Step', 'Save & Close', and 'Next'. In the top right corner, there is a circular icon with a cloud, a padlock, and a key, symbolizing security and AI.

# Pega Blueprint™ Security & Privacy Summary

We built Pega Blueprint™ with your privacy and security as priorities. We understand your processes aren't just diagrams and workflows – they're your competitive advantage.



## Access managed by your enterprise

Blueprint access can be connected to your enterprise single-sign on.

- Blueprint manages data access through role-based access control designed to ensure the Blueprints created remain private to the creator unless actively shared.
- When a user leaves your organization, they will lose access to your Blueprints when their status or roles are updated in your organization's SSO provider.

## No AI is trained on your Blueprints

Prompts, data, and designs are never fed into AI models for training.

- Blueprint leverages frontier LLMs under the hood – including Anthropic models on AWS, Google Gemini, and OpenAI on MS Azure.
- All LLM's are continually governed, performance tested and leverage provider best practices for content filtering.

## Data remains confidential

The details of your Blueprints are stored in an encrypted cloud database.

- Deployed in the cloud in the region which makes most sense for your business – US, UK, APAC, or EU.
- No data shared across Pega clients or partners.
- Blueprints remain private to the creator unless actively shared.
- Only activity-level reporting data leveraged within Pega by authorized personnel (email address, create time, create names).

## Enterprise-grade cloud security

Your Blueprint data gets the same rock-solid protection as our production Pega Cloud Environment including:

- 256-bit AES encryption for data at rest and HTTPS/TLS protection for data in transit.
- Continuous monitoring with host-based virus protection and intrusion prevention systems.
- State-of-the-art operations centers that take physical and environmental security seriously.
- Built-in safeguards against DDoS attacks and automatic blocking of known malicious IP addresses.



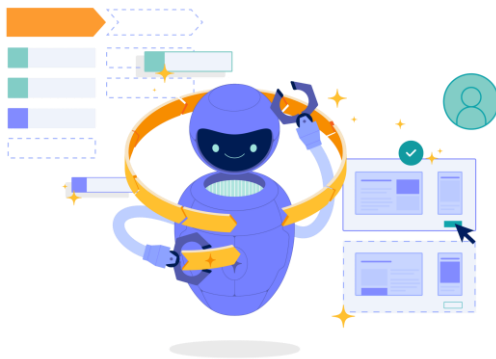
01

# What is Pega Blueprint?



# Transformation rocket fuel

**Pega Blueprint is enterprise workflow development powered by AI.** Focused on bringing people & AI together to accelerate automation & jumpstart transformation.



Dashboard

Pega + Blueprint™

RETAIL BANKING • BP-2224548 • ☆

## Complaints Management

Define workflow details for: [Complaint Management](#) 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.

Primary Stages

| Complaint Intake                                                                                                                                                                  | Classification Routing                                                                                                         | Orchestration                                                                                                                                                                                                                                                                                  | Tracking Oversight                                                                                                                                                                                                                                                                 | Outcome Review                                                                                                                                                          | Closure Learning                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Capture Complaint Details</li> <li>Extract &amp; Store Documents</li> <li>Verify Customer Identity</li> <li>Acknowledge Receipt</li> </ul> | <ul style="list-style-type: none"> <li>Auto-Classify Category</li> <li>Set Escalation Level</li> <li>Assign Officer</li> </ul> | <ul style="list-style-type: none"> <li>Spinoff Complaint Intake case</li> <li>Spinoff Complaint Investigation case</li> <li>Decide Regulatory Escalation</li> <li>Spinoff Regulatory Escalation case</li> <li>Detect Systemic Issue</li> <li>Spinoff Systemic Issue Resolution case</li> </ul> | <ul style="list-style-type: none"> <li>Wait for Complaint Intake case</li> <li>Wait for Complaint Investigation case</li> <li>Wait for Regulatory Escalation case</li> <li>Wait for Systemic Issue Resolution case</li> <li>Aggregate Statuses</li> <li>Escalate Delays</li> </ul> | <ul style="list-style-type: none"> <li>Compile Child Results</li> <li>Generate Consolidated Recommendation</li> <li>Approve Outcome</li> <li>Notify Customer</li> </ul> | <ul style="list-style-type: none"> <li>Update CRM Profile</li> <li>Capture Trend Data</li> <li>Confirm Closure</li> </ul> |

Back Preview my app Save & Close Next



# Where does Blueprint fit in the SDLC?

Accelerate your AI Transformation



## Pega Blueprint™

Business & IT collaboration to design agentic workflows and re-imagine how work will be completed in the agentic era.



## Pega Infinity™ Pega Infinity Studio™

Deep configuration of integration, automation, etc. to turn Blueprints into complete apps with AI assisted development.



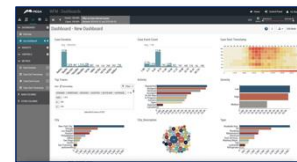
## Pega Infinity™ Pega Deployment Manager

Automated DevOps pipelines orchestrating route-to-live, including tests, approvals, security scans, and more.



## Pega Infinity™ OOTB Portal or DX API

Secure end-user experiences to access workflows (locked down through role & access based controls).



## Pega Infinity™ Pega Process Mining

Analyze workflows to uncover process gaps & inefficiencies.

Reimagine

Build

Test & Deploy

Operate

Optimize

No PII \*

No PII \*

No PII\*

Potentially sensitive

Potentially sensitive

Operated securely by Pega Cloud®

Private client deployment

Private client deployment

Private client deployment

Operated securely by Pega Cloud®

02

# Blueprint architecture.



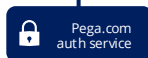
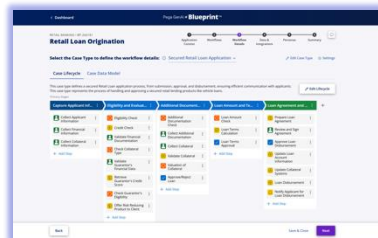
# Pega Blueprint™ Architecture

Blueprint runs securely in Pega Cloud® on AWS – managed & operated following [leading cloud standards](#).

## High level architecture:

- Blueprint authentication connects to your enterprise single-sign on protocol (SSO).
- Pega offers geographically segmented data residency services specific to its Pega Cloud offering. Blueprint geographic region is based on your enterprise location ([within either US, UK, European Union, Australia, Singapore, or Japan](#)).
- Blueprint processing runs on a secure, reliable Pega Infinity application, fully backed by the operational strength of Pega Cloud services, delivering enterprise grade [reliability](#), [compliance](#), [security](#), & [disaster recovery](#).
- Blueprint leverages LLM's based on use case & performance. Primarily Claude models running on [AWS Bedrock](#).
- No AI is trained on your Blueprint data.
- Blueprint data is [encrypted in transit](#) with TLS.
- Blueprint data is [securely stored](#) & [encrypted at rest](#).

Pega.com  
front-end web app



Your  
SSO

Your employee  
{user}@{your-org}.com



Fully isolated in region across:  
US – EU – AUS – UK – JP – SG



### Blueprint application

Core processing of user requests & Blueprint functionality  
Built on Pega Infinity™

### Industry knowledge service

Retrieval augmented generation service which provides Blueprint with information on workflow & data model best practices based on user request.

Built on Pega Knowledge Buddy™. Contains Pega industry IP.  
Does not store any client or user data.



### Pega Cloud AI Orchestration service

Orchestrates calls to LLM's

Built on AWS. Does not store any prompts, client data, or user data.



**AWS Bedrock**  
Primary LLM provider  
Claude Haiku & Sonnet



**Google Gemini**  
Flash



**Azure OpenAI**  
GPT

Various LLM's leveraged based on use case / performance. All processing in region.  
No AI trained on user or enterprise data.



### Secure data storage

Enterprise private data-at-rest encryption (DARE)

All client data stored in volumes, databases encrypted with 256-bit encryption. By default, encryption keys are rotated on a regular basis and are securely stored in a secure FIPS 140-2 compliant KMS.

Enterprise private encryption keys available on request.



### Private file storage

Connect to your Pega Cloud repo

All files related to Blueprint activity - for example uploaded documents & video - are stored in an enterprise private Pega Cloud File Storage folder. By default - this is managed on behalf of the enterprise by Blueprint.

Pega Cloud client-side Blueprint-related files are restored by default in their existing private Pega Cloud File Storage repository associated with their Pega Cloud instance.

# Pega Blueprint™ Regional Data Residency (EU, UK, US)

## Enterprises located in the European Union

- Storage & compute: **AWS EU-Central(Frankfurt)**
- [AI Model Execution](#)

|                                                                                  | Provider                                              | Model / provider | LLM regions                     |
|----------------------------------------------------------------------------------|-------------------------------------------------------|------------------|---------------------------------|
|  | <b>AWS Bedrock</b><br><small>Primary provider</small> | Anthropic        | AWS Bedrock: European Union     |
|  | <b>Google Cloud</b>                                   | Gemini           | Google Vertex: European Union   |
|  | <b>Microsoft Azure</b>                                | OpenAI GPT       | Microsoft Azure: European Union |

## Enterprises located in the United Kingdom

- Storage & compute: **AWS EU-West (London)**
- [AI Model Execution](#)

|                                                                                   | Provider                                              | Model / provider | LLM regions                     |
|-----------------------------------------------------------------------------------|-------------------------------------------------------|------------------|---------------------------------|
|  | <b>AWS Bedrock</b><br><small>Primary provider</small> | Anthropic        | AWS Bedrock: European Union     |
|  | <b>Google Cloud</b>                                   | Gemini           | Google Vertex: European Union   |
|  | <b>Microsoft Azure</b>                                | OpenAI GPT       | Microsoft Azure: European Union |

## Enterprises located Across the globe

- Storage & compute: **AWS US-East**
- [AI Model Execution](#)

|                                                                                     | Provider                                              | Model / provider | LLM regions                    |
|-------------------------------------------------------------------------------------|-------------------------------------------------------|------------------|--------------------------------|
|  | <b>AWS Bedrock</b><br><small>Primary provider</small> | Anthropic        | AWS Bedrock: United States     |
|  | <b>Google Cloud</b>                                   | Gemini           | Google Vertex: United States   |
|  | <b>Microsoft Azure</b>                                | OpenAI GPT       | Microsoft Azure: United States |

### For Pega Partners

Define which enterprise you're creating a Blueprint on behalf of in the organization name field on the functional description page of blueprint and those Blueprints will be stored & managed within region on behalf of that enterprise, automatically.

### Determining which region a Blueprint is stored within

Check out the Blueprint ID – which will have a regional identifier if it is stored & managed within the EU, AU, UK, JP, or SG.

# Pega Blueprint™ Regional Data Residency (APAC)

## Enterprises located in the Australia

- Storage & compute: **AWS: Australia - Sydney**
- [AI Model Execution](#)

|                                                                                  | Provider                                              | Model /<br>provider | LLM regions                   |
|----------------------------------------------------------------------------------|-------------------------------------------------------|---------------------|-------------------------------|
|  | <b>AWS Bedrock</b><br><small>Primary provider</small> | Anthropic           | AWS Bedrock:<br>Australia     |
|  | <b>Google Cloud</b>                                   | Gemini              | Google Vertex:<br>Australia   |
|  | <b>Microsoft<br/>Azure</b>                            | OpenAI<br>GPT       | Microsoft<br>Azure: Australia |

## Enterprises located in the Japan

- Storage & compute: **AWS: Japan - Osaka**
- [AI Model Execution](#)

|                                                                                   | Provider                                              | Model /<br>provider | LLM regions                                      |
|-----------------------------------------------------------------------------------|-------------------------------------------------------|---------------------|--------------------------------------------------|
|  | <b>AWS Bedrock</b><br><small>Primary provider</small> | Anthropic           | AWS Bedrock:<br>Japan/APAC                       |
|  | <b>Google Cloud</b>                                   | Gemini              | Google Vertex:<br>Japan                          |
|  | <b>Microsoft<br/>Azure</b>                            | OpenAI<br>GPT       | Microsoft<br>Azure: Japan /<br>European<br>Union |

## Enterprises located Singapore

- Storage & compute: **AWS: Singapore**
- [AI Model Execution](#)

|                                                                                     | Provider                                              | Model /<br>provider | LLM regions                              |
|-------------------------------------------------------------------------------------|-------------------------------------------------------|---------------------|------------------------------------------|
|  | <b>AWS Bedrock</b><br><small>Primary provider</small> | Anthropic           | AWS Bedrock:<br>APAC                     |
|  | <b>Google Cloud</b>                                   | Gemini              | Google Vertex:<br>Singapore              |
|  | <b>Microsoft<br/>Azure</b>                            | OpenAI<br>GPT       | Microsoft<br>Azure:<br>European<br>Union |

### For Pega Partners

Define which enterprise you're creating a Blueprint on behalf of in the organization name field on the functional description page of blueprint and those Blueprints will be stored & managed within region on behalf of that enterprise, automatically.

### Determining which region a Blueprint is stored within

Check out the Blueprint ID – which will have a regional identifier if it is stored & managed within the EU, AU, UK, JP, or SG.

03

# Access & authentication.



# Pega Blueprint™ Access & Auth

## Set up access to Blueprint with your single-sign on (SSO).

Enabling users to authenticate against your Organization's IDP ensures that only authorized users are accessing ALL Pega sites and applications, such as Blueprint, My Support Portal, etc.

When Federated Authentication is enabled, at log in, users will not be prompted to provide a password and will be redirected to authenticate against their Identity Provider.

IT leads at the client Organization can work with our integrated account team to enable Federated Authentication.

## What we need from you: SAML 2.0 Configuration details or OAuth Configuration details

Login to following applications will use Federated Authentication: Blueprint, Pega.com, community.pegacorp.com, academy.pegacorp.com, support.pegacorp.com, docs.pegacorp.com, partners.pegacorp.com, saleshub.pegacorp.com, partner-logo-generator.pegacorp.com, My Support Portal, My Pega Cloud, My Pega, PDC, Deployment Manager, Pega Trials

## Blueprints are only visible to the creator, unless actively shared.

By default, Blueprints are not visible to anyone beyond the user who created them (the Blueprint *owner*).\*\*

Blueprint owners have the ability to share the Blueprint with additional stakeholders (e.g. teammates, partners, etc.). They can invite users via email as either *editors* or *viewers*.

**Share this Blueprint**

**Invite Collaborators**  
Only collaborators with a business email address will be able to access Pega GenAI Blueprint

Editor

Send

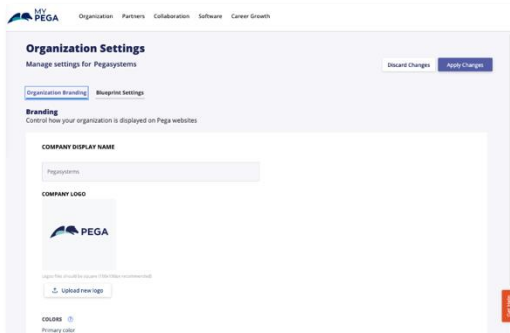
## When a user leaves your org, their Blueprints don't leave with them.

If an enterprise has federated their SSO with Pega digital properties (e.g. Blueprint), only users with active access to their SSO will be able to log into Blueprint.

If a user changes the domain registered with their pega.com profile – for example switches organizations, the Blueprints that they created within their old domain will no longer be visible.

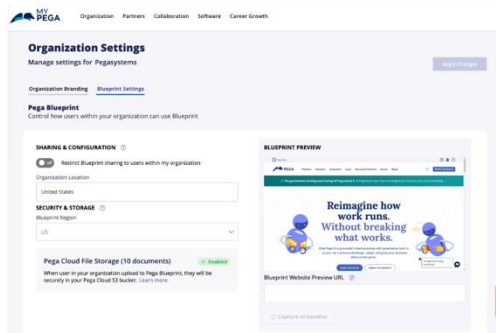
Access to those Blueprints can be restored for other users within the organization upon request.

# Pega Blueprint™ Organizational Control Pane



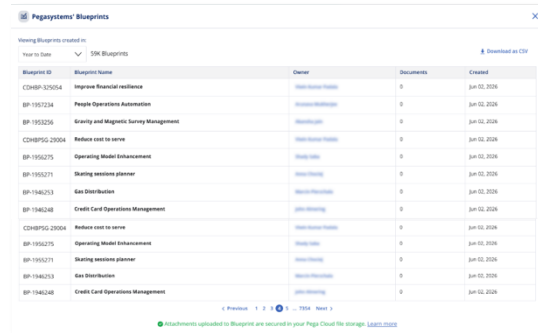
## Tune your organizational branding

Have full control of your company display name, colours and logo. The Blueprint administrator has full capability to update branding and accelerate delivery of Production grade applications with all branding taken care of.



## Manage your storage and sharing

Have confidence in blueprint security controls as you can restrict Blueprint sharing outside of your organization. Review Default Organization location and nominate the data residency region for security & storage.



## Organizational Blueprint Visibility

Full visibility of the Blueprint ID's, Creators, names, documents and create dates across your enterprise.

04

# Data privacy.



# Pega Blueprint™ Data Handling

What's captured & how is it handled?

| # | Datapoint                          | Format                                                     | Processed by LLM? | Used for AI Training? | Stored in...                                         | Visible to...                       |
|---|------------------------------------|------------------------------------------------------------|-------------------|-----------------------|------------------------------------------------------|-------------------------------------|
| 1 | Creator information                | Metadata (name, email, org)                                | No                | No                    | <b>Pega Cloud Data Storage</b><br>Fully encrypted*   | Pega                                |
| 2 | App description                    | Metadata (industry, app name)                              | Yes               | No                    | <b>Pega Cloud Data Storage</b><br>Fully encrypted*   | Pega                                |
| 3 | Text based application description | Encrypted text                                             | Yes               | No                    | <b>Pega Cloud Data Storage</b><br>Fully encrypted*   | Only Blueprint creator & invitees** |
| 4 | Legacy documentation               | .PDF, .DOC, .DOCX, .md                                     | Yes               | No                    | <b>Pega Cloud File Storage</b><br>Encrypted at rest* | Only Blueprint creator & invitees** |
| 5 | Legacy videos & images             | .MOV, .MP4, .JPG, .PNG, .jpeg, .avi                        | Yes               | No                    | <b>Pega Cloud File Storage</b><br>Encrypted at rest* | Only Blueprint creator & invitees** |
| 6 | Process diagrams                   | .BPMN, .jpm, .jpeg                                         | Yes               | No                    | <b>Pega Cloud File Storage</b><br>Encrypted at rest* | Only Blueprint creator & invitees** |
| 7 | Integration & data documentation   | .YAML, .SQL, .DDL, .CRD                                    | Yes               | No                    | <b>Pega Cloud File Storage</b><br>Encrypted at rest* | Only Blueprint creator & invitees** |
| 8 | Code Analysis Documentation        | AWS Transform, Google MAT, NotestoBlueprint, .Blueprint    | Yes               | Np                    | <b>Pega Cloud File Storage</b><br>Encrypted at rest* | Only Blueprint creator & invitees** |
| 9 | Blueprint edits & final designs    | Encrypted metadata (exported as encrypted .Blueprint file) | No                | No                    | <b>Pega Cloud Data Storage</b><br>Fully encrypted*   | Only Blueprint creator & invitees** |

05

# Cloud security.





[Visit the Pega Cloud Trust Center to learn more](#)

# Pega Blueprint™ Cloud Security

Pega Blueprint runs on Pega's proven Pega Cloud® services, ensuring enterprise-grade security.

## Transformation you can rely on.

- 24/7 operations monitoring, management, and support
- Secure-by-design architecture operations with strict access controls and operational safeguards-minimizing human touch through automation
- Enterprise-grade compliance, uptime, disaster recovery, and threat modeling

## Operations

**24/7 monitoring, environment support, & proactive response**  
[Details](#)

## Access

**Environment governed by automated operational controls and strict access protocols**  
[Details](#)

## Compliance

**Strict adherence to 20+ industry standards**  
[Details](#)

## Disaster recovery

**Comprehensive data & service back-up, failover, restoration**  
[Details](#)

## Threat modeling

**Follow red team methodology based on OWASP top 10**  
[Details](#)

## Availability

**Architecture leverages built-in high availability and disaster recovery to support near continuous uptime.**  
[Details](#)

The screenshot displays the Pega Trust Center website. At the top, there's a navigation bar with links like 'Pega Sites', 'Platform', 'Solutions', 'Customers', 'Learn', 'Services & Partners', 'Events', and 'About'. Below this is a banner for 'Pega Trust Center' with the text: 'Secure. Reliable. Compliant. Pega Cloud empowers the world's biggest brands to meet - and exceed - the challenges of today and tomorrow. Learn how.' A link 'Learn more about Pega's security features:' is present. The main content area is divided into sections: 'Security' (with a 'View security bulletins' link), 'Authorization & access' (describing role-based controls and single sign-on), 'Network protection' (describing network architecture and isolation), 'Secure system integration' (describing integration with enterprise environments), 'Client-based access control' (describing control rules and data storage), 'Data encryption' (describing encryption critical to data protection), 'Supporting security documents' (listing various documents like 'Global Security Policies', 'Veracode Statements', etc.), 'Privacy' (describing privacy and compliance strategies), and 'Compliance certifications, attestations, and accessibility' (describing various certifications like APRA, CS, CSA STAR, etc.).

06

# AI governance.





## Pega Blueprint™ leverages frontier models to help drive Accelerated AI transformation

Models are all securely managed & incorporated into the product to balance effectiveness & performance.

As of Q3 2025

While Pega continually assesses LLM's to ensure we're using the right model for the right job, here are models currently utilized under the hood:

| Hyperscaler                                                                                                        | LLM Provider                      | Blueprint region | LLM region                      |
|--------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------|---------------------------------|
|  <b>AWS</b><br>Primary provider | Anthropic<br>Claude<br>Sonnet 4.5 | AMS (USA)        | AWS Bedrock: United States      |
|                                                                                                                    |                                   | EU               | AWS Bedrock: European Union     |
|                                                                                                                    |                                   | UK               | AWS Bedrock: United Kingdom     |
|  <b>Google Cloud</b>            | Google<br>Gemini                  | AMS (USA)        | Google Vertex: United States    |
|                                                                                                                    |                                   | EU               | Google Vertex: European Union   |
|                                                                                                                    |                                   | UK               | Google Vertex: United Kingdom   |
|  <b>Microsoft Azure</b>         | OpenAI - GPT                      | AMS (USA)        | Microsoft Azure: United States  |
|                                                                                                                    |                                   | EU               | Microsoft Azure: European Union |
|                                                                                                                    |                                   | UK               | Microsoft Azure: United Kingdom |

All agreements with hyperscalers include commitments that no prompts or data sent by Pega or clients will be accessed by either the hyperscaler or the LLM provider.

\*as of June 2025

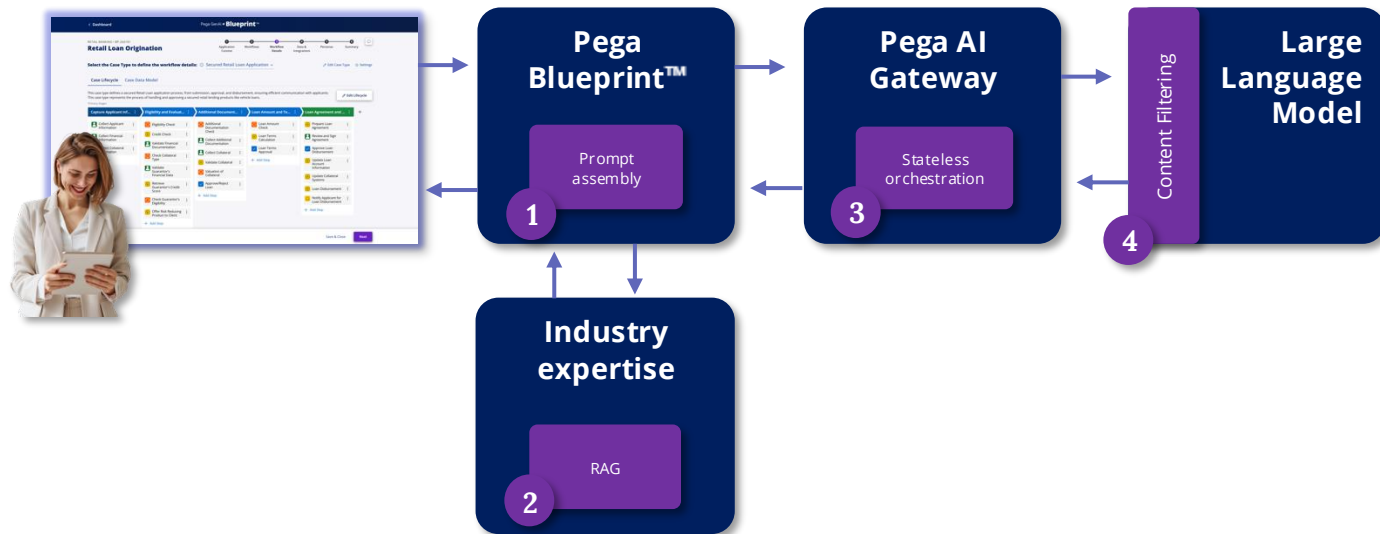
\*\*Always up-to-date on [pega.com](https://www.pega.com)

# Data Flow

## Pega Blueprint™

### Secure, safe AI handling:

1. Pega Blueprint **creates prompts** that describe the application based on user-entered information.
2. Pega Blueprint calls out to Pega's **industry expertise** knowledgebase run on Pega Knowledge Buddy to synthesize industry best practices based on Blueprinted use case and enrich LLM prompts & Blueprint creation.
3. All LLM calls are brokered by the **Pega AI Gateway Service** on Pega Cloud. This service provides a trusted layer of security, segmentation, and scalability for communication with large language providers.
4. When sending an encrypted prompt to a secure LLM, **content filtering** applies to detect and prevent harmful content in prompts and completions.



### Content filtering approach

Pega relies on the most proven Large Language Model Providers in its delivery of Pega capabilities that rely on Generative AI. Within each model, are robust content filtering capabilities that will mitigate the possibilities of harmful, unethical, or toxic responses from occurring. While the capabilities are robust, these are only mitigations and the possibility for a jailbreak remains. In addition, each model provider takes a different approach to achieving the same outcome of responsible and ethical AI.

This means that the classification models, thresholds, and categories of detection can differ. When different models are used different content classification and filtering is applied. When clients are using Pega GenAI Connect, they should be aware of these possible differences and perform testing to validate them.

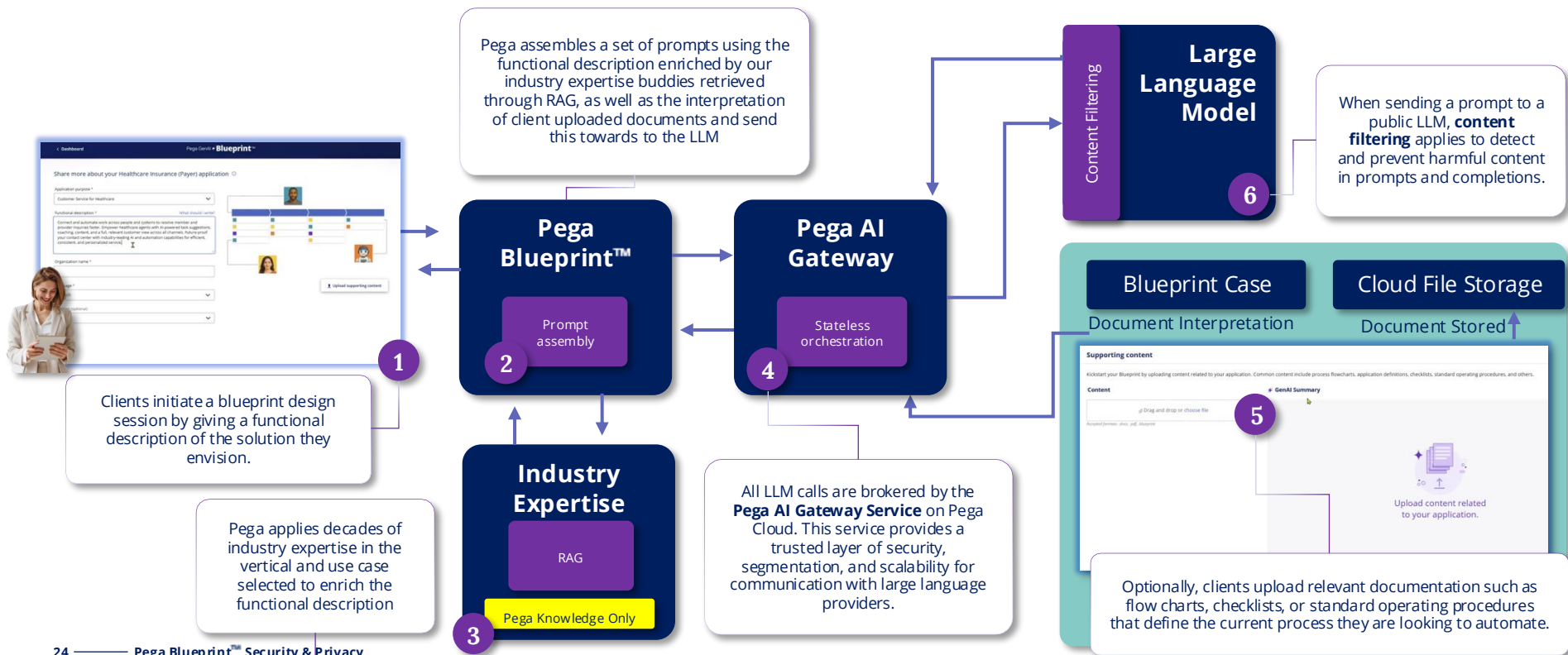
# Data Flow

## Pega Blueprint™

### Content filtering approach

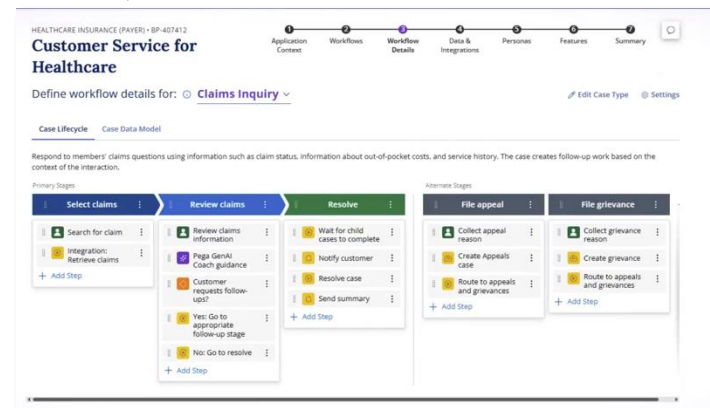
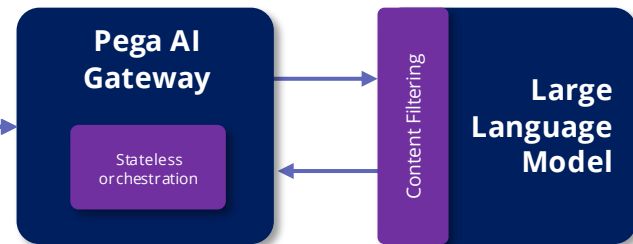
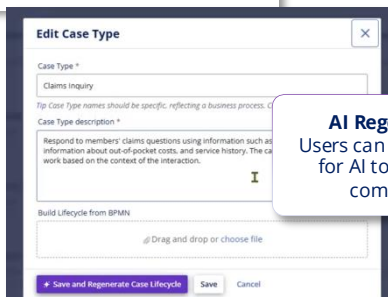
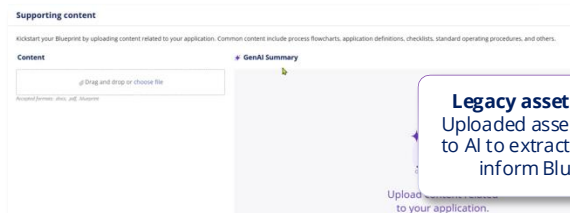
Pega relies on frontier Large Language Model Providers in its delivery of Pega capabilities that rely on Generative AI. Within each model, are robust content filtering capabilities that will mitigate the possibilities of harmful, unethical, or toxic responses from occurring. While the capabilities are robust, these are only mitigations and the possibility for a jailbreak remains. In addition, each model providers take a different approach to achieving the same outcome of responsible and ethical AI.

This means that the classification models, thresholds, and categories of detection can differ. When different models are used different content classification and filtering is applied. When clients are using Pega GenAI Connect, they should be aware of these possible differences and perform testing to validate them.



# Data Flow

## Pega Blueprint™



# AI Governance at Pega

## End-to-end oversight

Pega's AI Governance board is run by the Cloud Security team and oversees all AI utilization across Pega's products.

It brings together experts & owners from Product, Cloud Security, Cloud Operations, IT, Legal, & Go-to-market to ensure all utilization of AI in Pega is safe, responsible, secure.

## Strategic Partnerships

In order to deliver on the unique needs of its enterprise clients, Pega has formed strategic relationships & overarching agreements with AWS, Google Cloud, and Microsoft to drive shared AI initiatives.

Pega & its cloud providers of LLM services meet regularly to review model options, performance, security, & issues.

## Security-first

Pega's AI Governance board organizes & executes continuous security assessments of all AI powered capabilities including Pega Blueprint.

Security assessments run include:

1. ISO 42001
2. Microsoft AI Red Team Methodology
3. OpenAI Safety Best Practices
4. Microsoft required mitigations
5. OWASP Top 10 for LLM Applications
6. OWASP Cloud-Native Application Security Top 10





Pega is the leading Enterprise Transformation Company™ that helps organizations Build for Change® with enterprise AI decisioning and workflow automation. Many of the world's most influential businesses rely on our platform to solve their most pressing challenges, from personalizing engagement to automating service to streamlining operations. Since 1983, we've built our scalable and flexible architecture to help enterprises meet today's customer demands while continuously transforming for tomorrow. For more information on Pega (NASDAQ: PEGA), visit <http://www.pegas.com>