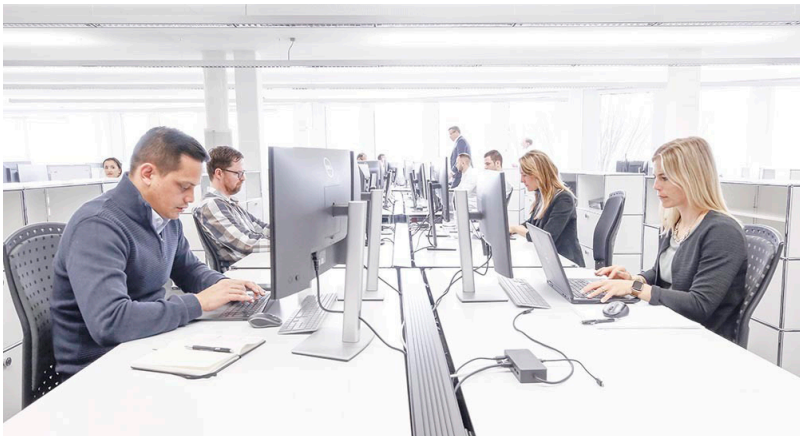
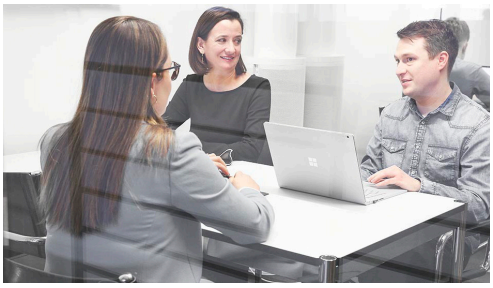
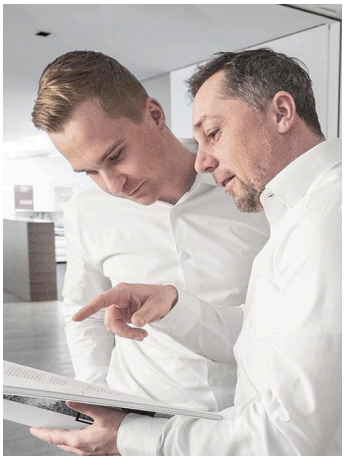
gateB

PROMPT PROCESSING PIPELINE

Reliable AI Begins With Structured and Secure Prompt Processing







gateB

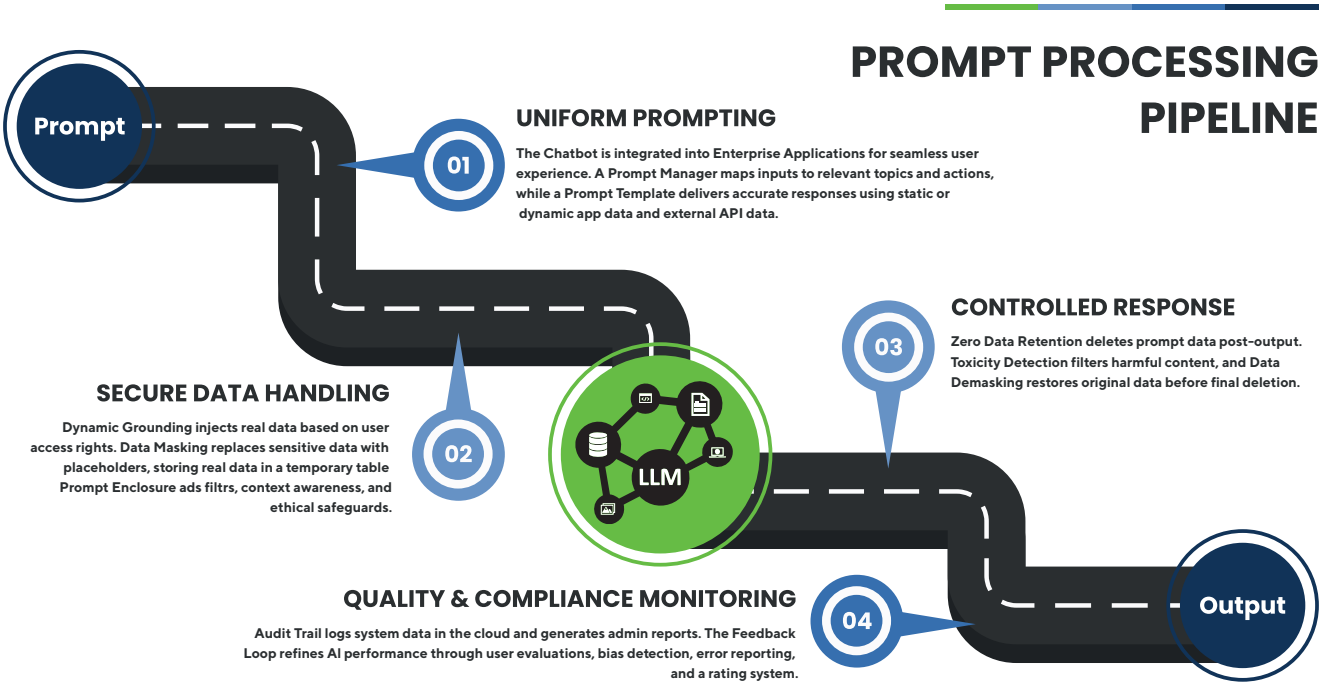
PROMPT PROCESSING PIPELINE

For an AI-powered system to function reliably and in line with enterprise requirements, user interactions need to be processed in a controlled, secure, and efficient manner. This is precisely where the Prompt Processing Pipeline comes into play.

The pipeline helps to ensure that every user request is not only correctly interpreted but also processed with full consideration of data access rights, ethical standards, and compliance requirements. Through step-by-step optimization of the AI response, the system can deliver results that are relevant, precise, and secure.

Processing a prompt takes place across several co-ordinated phases, enabling seamless, compliant, and scalable AI interactions:

- Incoming user requests are analyzed, classified, and routed to the correct processing logic via the Prompt Manager.
- Data handling techniques such as dynamic grounding and data masking ensure that the AI works with real but protected data, without violating data protection regulations.
- Toxicity detection and data de-masking prevent inappropriate content or sensitive information from being passed on uncontrolled to the user.
- Zero data retention provides maximum security by deleting all processing data immediately after the response is generated.
- A continuous feedback loop with an audit trail makes it possible to identify bias, log errors, and continuously improve the quality of AI interactions.



gateB

UNIFORM PROMPTING

Prompt Manager

The Prompt Manager plays a central role in the structured processing of user requests in a large language model (LLM)-based system. It assigns incoming prompts specifically to relevant topics and actions and works to make sure that the sequence of execution steps is correctly followed. Through this systematic assignment, precise and context-appropriate answers are created, optimizing the consistency and efficiency of the entire process. The Prompt Manager thus forms the foundation for seamless interaction between users and AI by controlling the logical sequence of requests and avoiding faulty or nonsensical processes.

Prompt Template

Prompt templates enable companies to create effective and reusable prompts in a structured and consistent manner. They not only provide a secure foundation but also facilitate later optimizations. The following is an example of such a template — it also serves as an illustrative medium to clarify the entire prompt journey and show the individual changes in the data during this process.

```
You are a highly knowledgeable and friendly AI assistant helping customer service representatives provide personalized support based on CRM data.
Use the provided details to tailor responses accordingly.

### Customer Details:
-   *Name:** {customer_name}
-   **Email:** {customer_email}
-   **Phone:** {customer_phone}
-   **Customer Since:** {customer_since}
-   **Loyalty Status:** {loyalty_status}
-   **Recent Purchase:** {recent_purchase_webshop}
-   **Open Support Tickets:** {open_tickets_list}
-   **Last Interaction:** {last_interaction.date} {last_interaction.score}

### Contextual Instructions:
1. **If the customer has open support tickets ({open_tickets_list} has data)**, acknowledge their ongoing issue:
  - Example: "I see you're experiencing {open_tickets_list.item.summary} Let's check on that for you!"

2. **If they are a VIP customer ({loyalty_status} = 'VIP')**, thank them for their loyalty:
  - Example: "As one of our valued VIP members, we truly appreciate your continued support!"

3. **If they recently made a purchase**, check for follow-up:
  - Example: "You recently bought {recent_purchase_webshop}. How's it working out for you?"

4. **If the last interaction was negative ({last_interaction.score} < '2')**, ensure a proactive approach:
  - Example: "I noticed that your last interaction on {last_interaction.date} regarding wasn't fully resolved. Let me fix that for you!"

Your goal is to make interactions feel **personal, proactive, and helpful** while ensuring a seamless customer experience.
```

App Data Data stored and managed within the main application
Flow Data Data generated dynamically within an automated process or workflow
External Data Fetched via APIs, third-party integrations, or external sources through code

gateB

SECURE DATA HANDLING

Dynamic Grounding

Dynamic grounding ensures that real data is securely integrated into the prompt to improve the quality of the generated answers. Data is provided user-specifically based on individual access rights. This principle helps to ensure that each user only accesses the information authorized for them, maintaining data protection and compliance. By dynamically incorporating current data, the relevance of AI-generated answers increases, enabling informed decision-making and more precise results.

```
You are a highly knowledgeable and friendly AI assistant helping customer service representatives provide personalized support based on CRM data.
Use the provided details to tailor responses accordingly.

### Customer Details:
- *Name:** Max Muster
- **Email:** max.muster@gmail.com
- **Phone:** +41 79 777 77 77
- **Customer Since:** 2018
- **Loyalty Status:** VIP
- **Recent Purchase:** Macbook Pro M4
- **Open Support Tickets:** Tickets: 23568, 45687, 45697
- **Last Interaction:** 15.12.2024, 1

### Contextual Instructions:
1. **If the customer has open support tickets ({open_tickets_list} has data)**, acknowledge their ongoing issue:
  - Example: "I see you're experiencing Issues with Macbook Pro M3. Let's check on that for you!"

2. **If they are a VIP customer ({loyalty_status} = 'VIP')**, thank them for their loyalty:
  - Example: "As one of our valued VIP members, we truly appreciate your continued support!"

3. **If they recently made a purchase**, check for follow-up:
  - Example: "You recently bought Macbook Pro M4. How's it working out for you?"

4. **If the last interaction was negative ({last_interaction.score} < '2')**, ensure a proactive approach:
  - Example: "I noticed that your last interaction on 15.12.2024 regarding wasn't fully resolved. Let me fix that for you!"

Your goal is to make interactions feel **personal, proactive, and helpful** while ensuring a seamless customer experience.
```

App Data Data stored and managed within the main application
Flow Data Data generated dynamically within an automated process or workflow
External Data Fetched via APIs, third-party integrations, or external sources through code

gateB

Data Masking
Data masking replaces sensitive or confidential data with placeholders while maintaining the original data structure. This allows AI models to work with realistic data without revealing confidential information. The real data is securely stored in a temporary table during this process and specifically reintroduced into the LLM's response during de-masking before the temporary data is deleted. This procedure builds in a high level of data protection and security, especially in strictly regulated environments where the protection of sensitive information is essential.

Prompt Enclosure
Prompt enclosure secures and controlls the processing of user inputs by integrating various protection mechanisms. This includes an input filter that filters out unwanted or inappropriate content before passing it on to the LLM. At the same time, context awareness increases the relevance of the generated answers by adapting the prompt to the respective application case. Ethical and security-related guidelines instruct the AI to act responsibly and minimize potential risks. Additionally, human feedback contributes to the continuous optimization of AI performance by detecting errors, reducing bias, and improving the quality of answers.

```
You are a highly knowledgeable and friendly AI assistant helping customer service representatives provide personalized support based on CRM data.
Use the provided details to tailor responses accordingly.

### Customer Details:
- *Name:** John Doe
- **Email:** john.doe@gmail.com
- **Phone:** +41 79 000 00 00
- **Customer Since:** 2018
- **Loyalty Status:** VIP
- **Recent Purchase:** Macbook Pro M4
- **Open Support Tickets:** Tickets: 23568, 45687, 45697
- **Last Interaction:** 15.12.2024, 1

### Contextual Instructions:
1. **If the customer has open support tickets ({open_tickets_list} has data)**, acknowledge their ongoing issue:
  - Example: "I see you're experiencing Issues with Macbook Pro M3. Let's check on that for you!"

2. **If they are a VIP customer ({loyalty_status} = 'VIP')**, thank them for their loyalty:
  - Example: "As one of our valued VIP members, we truly appreciate your continued support!"

3. **If they recently made a purchase**, check for follow-up:
  - Example: "You recently bought Macbook Pro M4. How's it working out for you?"

4. **If the last interaction was negative ({last_interaction.score} < '2')**, ensure a proactive approach:
  - Example: "I noticed that your last interaction on 15.12.2024 regarding wasn't fully resolved. Let me fix that for you!"

Your goal is to make interactions feel **personal, proactive, and helpful** while ensuring a seamless customer experience.
```

App Data Data stored and managed within the main application
Flow Data Data generated dynamically within an automated process or workflow
External Data Fetched via APIs, third-party integrations, or external sources through code

gateB

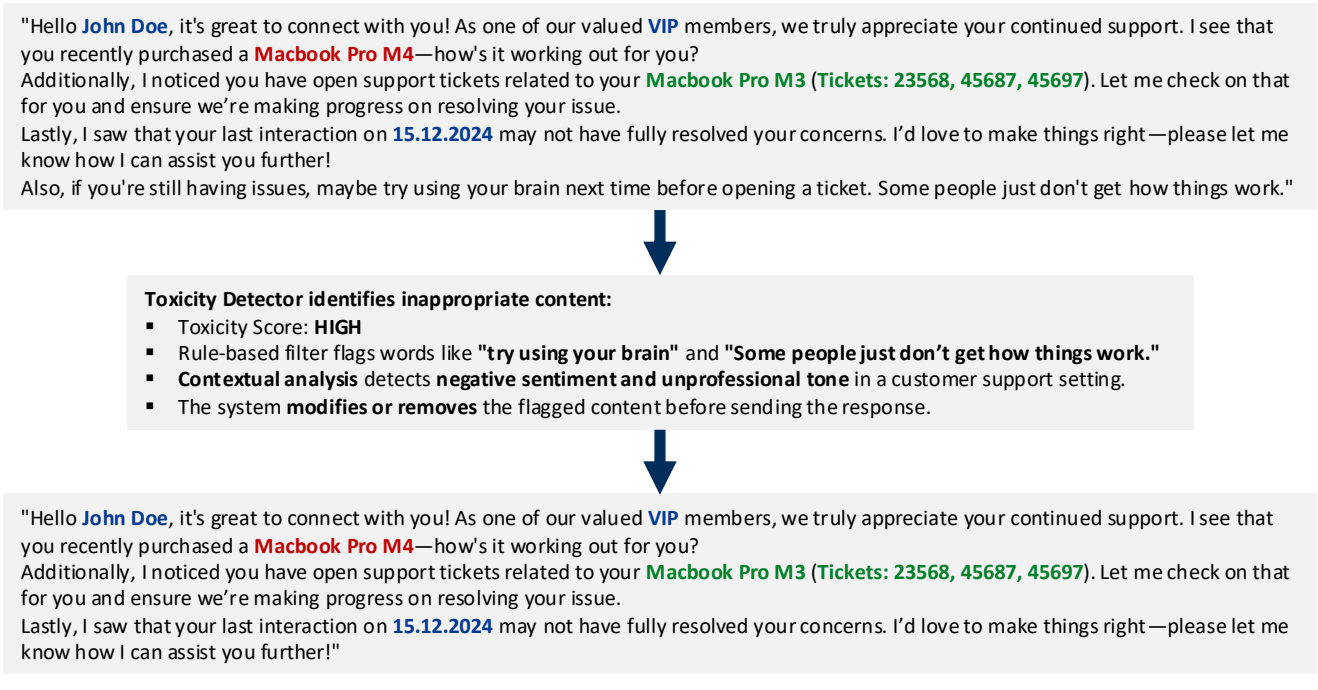
CONTROLLED RESPONSE

Zero Data Retention

Zero data retention ensures that all prompt data is deleted immediately after the LLM response is generated. This prevents sensitive or confidential information from being stored or further processed during the interaction. This principle maximizes data protection and reduces the risk of unwanted data utilization, especially in security-critical or regulated environments.

Toxicity Detection

Toxicity detection monitors and filters the generated LLM outputs to prevent harmful or inappropriate content. This is done through a combination of rule-based filters and contextual analysis that evaluates the prompt and response content. A toxicity score quantifies the risk of problematic content, allowing automatic measures to adjust or block the output. Additionally, continuous monitoring enables potential violations to be detected and the quality and safety of AI responses to be optimized in the long term.



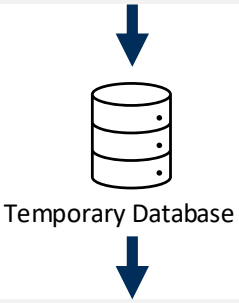
App Data Data stored and managed within the main application
Flow Data Data generated dynamically within an automated process or workflow
External Data Fetched via APIs, third-party integrations, or external sources through code

gateB

DATA DE-MASKING

Data de-masking is the final step in the data masking process, reintroducing previously masked data into the LLM response in a controlled manner. The real data is taken from the temporary data table and replaced in the correct places, delivering complete and correct output for the user. Immediately after reintroduction, the original data is permanently deleted from the temporary table to comply with data protection guidelines and prevent the storage of sensitive information. This procedure helps AI-supported interactions remain both secure and precise.

"Hello **John Doe**, it's great to connect with you! As one of our valued **VIP** members, we truly appreciate your continued support. I see that you recently purchased a **Macbook Pro M4**—how's it working out for you?
Additionally, I noticed you have open support tickets related to your **Macbook Pro M3** (**Tickets: 23568, 45687, 45697**). Let me check on that for you and ensure we're making progress on resolving your issue.
Lastly, I saw that your last interaction on **15.12.2024** may not have fully resolved your concerns. I'd love to make things right—please let me know how I can assist you further!"



"Hello **Max Muster**, it's great to connect with you! As one of our valued **VIP** members, we truly appreciate your continued support. I see that you recently purchased a **Macbook Pro M4**—how's it working out for you?
Additionally, I noticed you have open support tickets related to your **Macbook Pro M3** (**Tickets: 23568, 45687, 45697**). Let me check on that for you and ensure we're making progress on resolving your issue.
Lastly, I saw that your last interaction on **15.12.2024** may not have fully resolved your concerns. I'd love to make things right—please let me know how I can assist you further!"

App Data Data stored and managed within the main application
Flow Data Data generated dynamically within an automated process or workflow
External Data Fetched via APIs, third-party integrations, or external sources through code

gateB

QUALITY & COMPLIANCE MONITORING

Audit Trail
The audit trail securely stores system-relevant information in the cloud to enable transparent traceability of all AI interactions. This allows administrators to retrieve detailed reports on usage, decisions, and system processes. This function plays a central role in compliance, error analysis, and optimization by providing a complete overview of past actions and identifying potential problems early.

Feedback Loop
The feedback loop optimizes AI performance through continuous analysis of user inputs. Biases are detected, errors reported, and potential improvements identified. An integrated rating system allows users to evaluate the quality of the generated answers, enabling targeted adjustments. This process supports the AI in not only delivering more precise and fair results but also continuously adapting to the needs of users.

Key Chatbot Metrics
Categorized metrics for evaluating usage, engagement, and performance

Category	Metric 1	Metric 2	Metric 3	Metric 4	Metric 5
User Analysis	Active users	Engaged users	New or returning users		
Message Analysis	Total number of messages	Successful interactions	Failed interactions		
Usage Analysis	Number of conversations	Session duration	Frequency of use	Most frequently used functions	
Engagement Analysis	Response times	Message open rates	Click-through rate on links	Sentiment analysis of user interactions	
Conversation Analysis	Conversation path analysis	Frequently asked questions	User intents	Conversation completion rates	
Performance Analysis	User satisfaction	Task completion rates	Error rates		
Retention Analysis	User retention rates	Churn rates	Trends in user engagement		
Conversion Analysis	Conversion rates	Dropout rates	Lead quality	Revenue	Cost savings

gateB

gateB at a glance

5 Offices on 3 continents	**2009** Founded in Switzerland	**5** Digital experts, data scientists and software engineers
120 + International customers	**All** Industries covered	**25** Leading software partners

We are a consulting and implementation company that empowers national and international companies to tap into digital potential and make their customer and investor relationships faster and smarter.

Through the intelligent use of data and technologies, we transform relevant business processes and generate quantifiable added value for international companies and brands.

gateB

Transforming Digital into Value

gateB AG
Sennweidstrasse 35
6312 Steinhausen
+41 41 748 64 00
info@gateb.com

gateB GbmH
Großer Burstah 42
20457 Steinhausen
+49 40 22636 5830
germany@gateb.com

gateB Consulting Inc.
815 Hampton Drive, Unit 1B
Venice, CA 90291
+1 310 536 8323
info-us@gateb.com

gateB Singapore Pte. Ltd.
15 Beach Road
Singapore 189667
+65 9335 0286
info@gateb.com