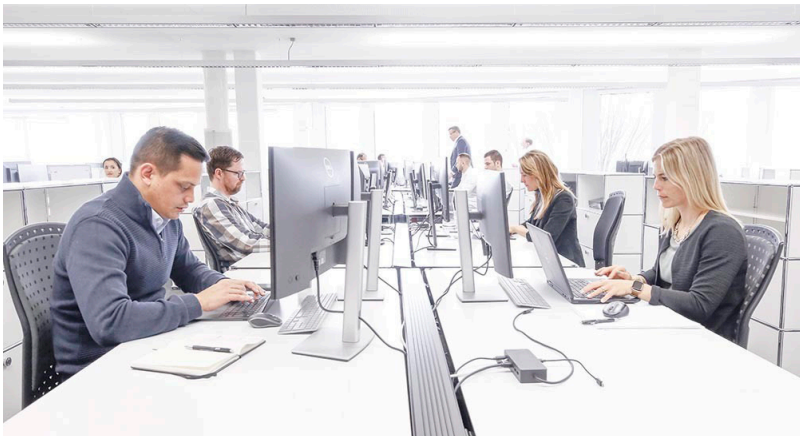
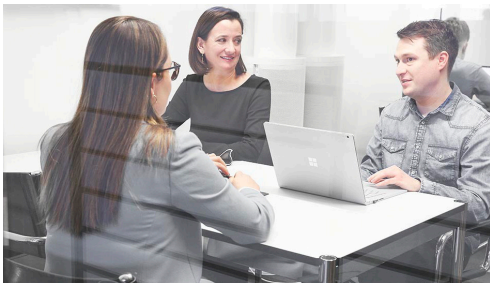
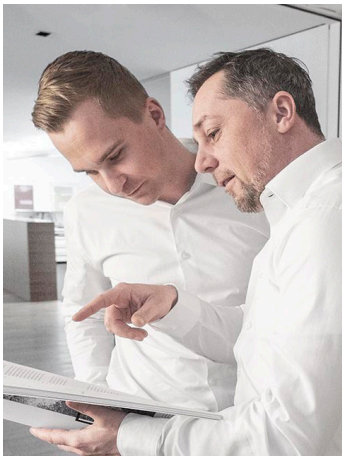
gateB

# PROMPT PROCESSING PIPELINE

**Verlässliche KI beginnt mit einer strukturierten und sicheren Prompt-Verarbeitung.**







gateB

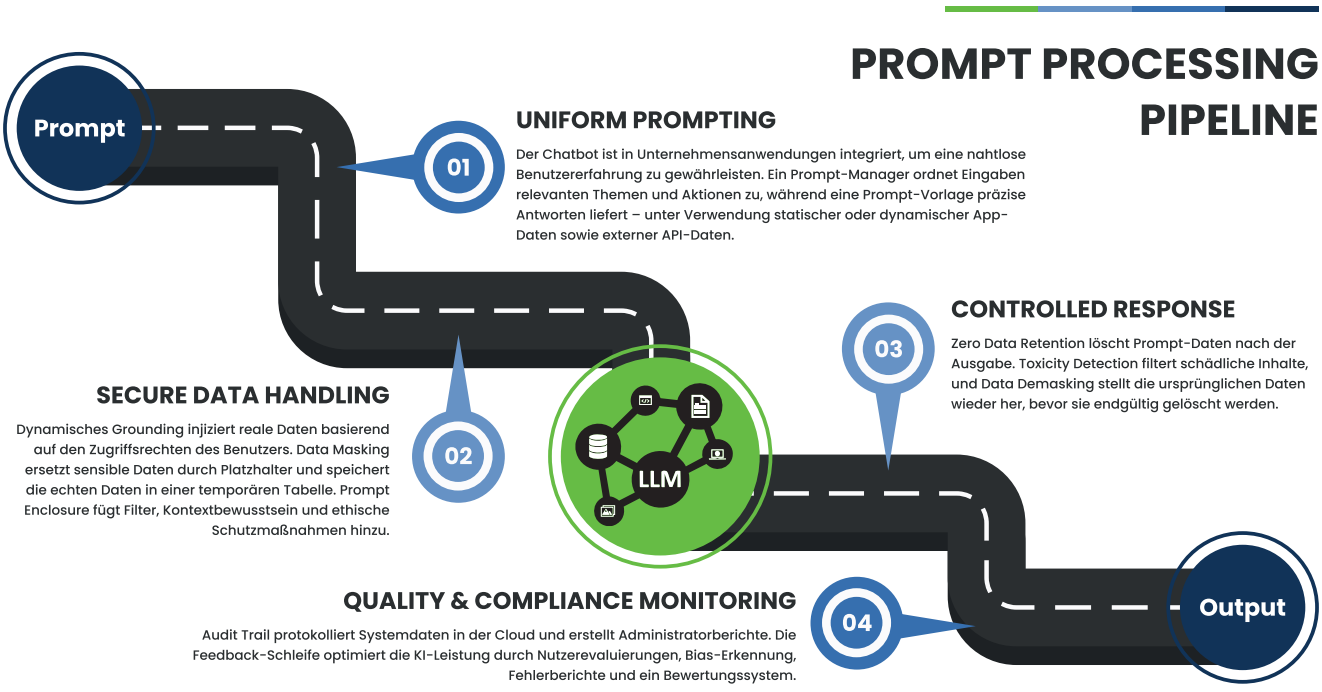
## PROMPT PROCESSING PIPELINE

Damit ein KI-gestütztes System zuverlässig und unternehmensgerecht funktioniert, müssen User-Interaktionen kontrolliert, sicher und effizient verarbeitet werden. Genau hier setzt die Prompt Processing Pipeline an.

Diese Pipeline stellt sicher, dass jede Benutzeranfrage nicht nur richtig interpretiert, sondern auch unter Berücksichtigung von Datenzugriffsrechten, ethischen Standards und Compliance-Vorgaben verarbeitet wird. Durch eine schrittweise Optimierung der KI-Antwort wird gewährleistet, dass das System relevante, präzise und sichere Ergebnisse liefert.

Die Verarbeitung eines Prompts erfolgt in mehreren aufeinander abgestimmten Phasen, die eine nahtlose, regelkonforme und skalierbare KI-Interaktion ermöglichen:

- Eingehende Benutzeranfragen werden über den Prompt-Manager analysiert, klassifiziert und an die richtige Verarbeitungslogik weitergeleitet.
- Datenhandling-Techniken wie Dynamic Grounding und Data Masking stellen sicher, dass die KI mit realen, aber geschützten Daten arbeitet, ohne Datenschutzrichtlinien zu verletzen.
- Toxicity Detection und Data De-masking verhindern, dass unangemessene Inhalte oder sensible Informationen unkontrolliert an den Nutzer weitergegeben werden.
- Zero Data Retention sorgt für maximale Sicherheit, indem sämtliche Verarbeitungsdaten unmittelbar nach der Antworterstellung gelöscht werden.
- Eine kontinuierliche Feedback-Schleife mit Audit-Trail ermöglicht es, Bias zu erkennen, Fehler zu protokollieren und die Qualität der KI-Interaktionen fortlaufend zu verbessern.



gateB

## UNIFORM PROMPTING

### Prompt Manager

Der Prompt Manager spielt eine zentrale Rolle bei der strukturierten Verarbeitung von Benutzeranfragen in einem LLM-basierten System. Er ordnet eingehende Prompts gezielt den relevanten Themen und Aktionen zu und stellt sicher, dass die Abfolge der Ausführungsschritte korrekt eingehalten wird. Durch diese systematische Zuordnung werden präzise und kontextgerechte Antworten gewährleistet, wodurch die Konsistenz und Effizienz des gesamten Prozesses optimiert wird. Der Prompt Manager bildet somit das Fundament für eine nahtlose Interaktion zwischen Nutzern und der KI, indem er die logische Sequenz von Anfragen steuert und fehlerhafte oder unsinnige Abläufe vermeidet.

### Prompt Template

Prompt-Templates ermöglichen Unternehmen, effektive und wiederverwendbare Prompts auf strukturierte und konsistente Weise zu erstellen. Sie bieten nicht nur eine sichere Grundlage, sondern erleichtern auch spätere Optimierungen. Im Folgenden wird ein Beispiel für ein solches Template vorgestellt – es dient zugleich als anschauliches Medium, um die gesamte Prompt-Journey zu verdeutlichen und die einzelnen Veränderungen in den Daten während dieses Prozesses aufzuzeigen.

```
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 sorgt dafür, dass reale Daten sicher in den Prompt integriert werden, um die Qualität der generierten Antworten zu verbessern. Dabei werden Daten gezielt und benutzerspezifisch bereitgestellt, basierend auf individuellen Zugriffsrechten. Dieses Prinzip stellt sicher, dass jeder Nutzer nur auf die für ihn autorisierten Informationen zugreift, wodurch Datenschutz und Compliance gewahrt bleiben. Durch die dynamische Einbindung aktueller Daten erhöht sich die Relevanz der KI-generierten Antworten, was eine fundierte Entscheidungsfindung und präzisere Ergebnisse ermöglicht.

```
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 ersetzt sensible oder vertrauliche Daten durch Platzhalter, während die ursprüngliche Datenstruktur erhalten bleibt. Dadurch können KI-Modelle mit realitätsnahen Daten arbeiten, ohne dass vertrauliche Informationen offengelegt werden. Die echten Daten werden währenddessen sicher in einer temporären Tabelle gespeichert und beim De-Masking gezielt wieder in die Antwort des LLMs eingeführt, bevor die temporären Daten gelöscht werden. Dieses Verfahren gewährleistet ein hohes Mass an Datenschutz und Sicherheit, insbesondere in streng regulierten Umgebungen, in denen der Schutz sensibler Informationen essenziell ist.

**Prompt Enclosure**
Prompt Enclosure sorgt für eine sichere und kontrollierte Verarbeitung von Benutzereingaben, indem es verschiedene Schutzmechanismen integriert. Dazu gehört ein Input-Filter, der unerwünschte oder unpassende Inhalte herausfiltert, bevor sie an das LLM weitergegeben werden. Gleichzeitig erhöht die Kontextbewusstheit die Relevanz der generierten Antworten, indem sie den Prompt an den jeweiligen Anwendungsfall anpasst. Zudem gewährleisten ethische und sicherheitsbezogene Richtlinien, dass die KI verantwortungsvoll agiert und potenzielle Risiken minimiert werden. Ergänzend trägt menschliches Feedback zur kontinuierlichen Optimierung der KI-Leistung bei, indem es Fehler erkennt, Bias reduziert und die Qualität der Antworten verbessert.

```
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 stellt sicher, dass alle Prompt-Daten unmittelbar nach der Generierung der LLM-Antwort gelöscht werden. Dadurch wird verhindert, dass sensible oder vertrauliche Informationen über die Interaktion gespeichert oder weiterverarbeitet werden. Dieses Prinzip maximiert den Datenschutz und reduziert das Risiko einer unerwünschten Datenverwertung, insbesondere in sicherheitskritischen oder regulierten Umgebungen.

### Toxicity Detection

Toxicity Detection überwacht und filtert die generierten LLM-Ausgaben, um schädliche oder unangemessene Inhalte zu verhindern. Dies geschieht durch eine Kombination aus regelbasierten Filtern und kontextueller Analyse, die den Prompt und die Antwort inhaltlich bewertet. Ein Toxicity Score quantifiziert das Risiko problematischer Inhalte, sodass automatisch Massnahmen zur Anpassung oder Blockierung des Outputs ergriffen werden können. Zusätzlich ermöglicht ein kontinuierliches Monitoring, dass potenzielle Verstösse erkannt und langfristig die Qualität sowie Sicherheit der KI-Antworten optimiert werden.

"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!
Also, if you're still having issues, maybe try using your brain next time before opening a ticket. Some people just don't get how things work."

**Toxicity Detector identifies inappropriate content:**

- Toxicity Score: **HIGH**
- Rule-based filter flags words like **"try using your brain"** and **"Some people just don't get how things work."**
- **Contextual analysis** detects **negative sentiment and unprofessional tone** in a customer support setting.
- The system **modifies or removes** the flagged content before sending the response.

"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!"

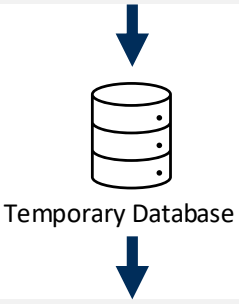
**App Data** Data stored and managed within the main application
**Flow Data** Data generated dynamically within an automated process or workflow
**External Data** Fetched via APIs, third-party integrations, or external sources through code

gateB

## DATA DE-MASKING

Data De-Masking ist der abschliessende Schritt im Data Masking-Prozess und stellt sicher, dass zuvor maskierte Daten kontrolliert in die LLM-Antwort wiedereingeführt werden. Die echten Daten werden dabei aus der temporären Datentabelle entnommen und an den richtigen Stellen ersetzt, sodass die Ausgabe für den Nutzer vollständig und korrekt ist. Direkt nach der Wiedereinführung werden die Originaldaten endgültig aus der temporären Tabelle gelöscht, um Datenschutzrichtlinien einzuhalten und jegliche Speicherung sensibler Informationen zu verhindern. Dieses Verfahren gewährleistet, dass KI-gestützte Interaktionen sowohl sicher als auch präzise bleiben.

"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**
Der Audit Trail speichert systemrelevante Informationen sicher in der Cloud, um eine transparente Nachverfolgbarkeit aller KI-Interaktionen zu gewährleisten. Dadurch können Administratoren detaillierte Berichte über die Nutzung, Entscheidungen und Systemprozesse abrufen. Diese Funktion spielt eine zentrale Rolle in der Compliance, Fehleranalyse und Optimierung, indem sie einen vollständigen Überblick über vergangene Aktionen bietet und potenzielle Probleme frühzeitig identifizierbar macht.

**Feedback Loop**
Die Feedback Loop optimiert die Leistung der KI durch eine fortlaufende Analyse von Nutzereingaben. Dabei werden Biases erkannt, Fehler gemeldet und Verbesserungspotenziale identifiziert. Ein integriertes Bewertungssystem ermöglicht es Nutzern, die Qualität der generierten Antworten zu bewerten, wodurch gezielte Anpassungen vorgenommen werden können. Dieser Prozess stellt sicher, dass die KI nicht nur präzisere und fairere Ergebnisse liefert, sondern sich auch kontinuierlich an die Bedürfnisse der Nutzer anpasst.

**Wichtige Chatbot Kennzahlen**
*Kategorisierte Kennzahlen zur Bewertung von Nutzung, Engagement und Performance*

| Kategorie | Metrik 1 | Metrik 2 | Metrik 3 | Metrik 4 | Metrik 5 |
|---|---|---|---|---|---|
| Nutzer-Analyse | Aktive Nutzer | Engagierte Nutzer | Neue oder wiederkehrende Nutzer | | |
| Nachrichten-Analyse | Gesamtanzahl Nachrichten | Erfolgreiche Interaktionen | Fehlgeschlagene Interaktionen | | |
| Nutzungsanalyse | Anzahl der Konversationen | Sitzungsdauer | Nutzungshäufigkeit | Am häufigsten genutzte Funktionen | |
| Engagement-Analyse | Reaktionszeiten | Nachrichten-Öffnungsraten | Klickrate auf Links | Sentiment-Analyse der Nutzerinteraktionen | |
| Konversationsanalyse | Analyse von Gesprächspfaden | Häufig gestellte Fragen | Nutzerintentionen | Abschlussraten von Konversationen | |
| Performance-Analyse | Nutzerzufriedenheit | Aufgaben-erfüllungsraten | Fehlerraten | | |
| Bindungsanalyse | Nutzerbindungsraten | Abwanderungsraten | Trends im Nutzerengagement | | |
| Conversion-Analyse | Konversionsraten | Abbruchraten | Lead-Qualität | Umsatz | Kosteneinsparungen |
| Stimmungsanalyse | Positiv-zu-negativ-Verhältnis | Nach Konversationstyp | Reaktion auf Bot-Antworten | Nach Nutzeranfragen | |
| NLU-Analyse | Genauigkeit der Intent-Erkennung | Genauigkeit der Entitätsextraktion | Fehleranalyse bei missverstandenen Eingaben | | |
| Nutzerfeedback-Analyse | Bewertungen | Rezensionen | Kommentare | | |
| Kanal-Analyse | Meistgenutzte Kanäle | Nutzerdemografie | Engagement-Muster | Konversionsraten | |

gateB

## GateB auf einen Blick

| | | |
|---|---|---|
| **5** Niederlassungen auf 3 Kontinenten | **2009** Gegründet in der Schweiz | **5** Digitalexperten, Data Scientists und Software Engineers |
| **120 +** Langjährige internationale Kund:innen | **Alle** Branchen | **25** Führende Software-Partner |

Wir sind ein Beratungs- und Implementierungsunternehmen, das nationale und internationale Firmen befähigt, das Digitalpotenzial zu erschliessen und dabei ihre Kunden- und Investorenbeziehungen schneller und smarter zu gestalten.

Mit dem intelligenten Einsatz von Daten und Technologien transformieren wir relevante Geschäftsprozesse und generieren einen quantifizierbaren Mehrwert für internationale Unternehmen und Marken.

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