

How Caplena wins Europe's most regulated companies

With a third of its customers in banking and insurance, Caplena redacts every comment before its AI ever sees it: 11M+ rows anonymized through October 2026. Here's how a 24-person Swiss company set a privacy bar higher than its customers' own.

11M+

more than 11 million rows in the first ten months of 2026

10×

more rows than in all of 2022


97%

adjusted recall in German (2026 benchmark)

50+

languages supported, from Europe to Southeast Asia and the Middle East

AT A GLANCE

Company

Caplena, a Zurich-based AI platform for voice-of-customer and employee feedback analysis

Team

24 people, plus roughly 100 AI agents

Customers

Global brands, with roughly a third in banking and insurance

Security

SOC 2 Type II certified and GDPR compliant, with servers in ISO 27001-certified data centers

Partner since

2022

Scale

More than 11 million rows in the first ten months of 2026, 10x more than in 2022

Deployment

Limina runs on Caplena's own infrastructure, at the entrance of its data pipeline

Coverage

Feedback in dozens of languages, including European languages, Chinese, Arabic and Hindi

01 THE CHALLENGE

Personal data hiding in open text

Caplena is an [AI Voice of Customer analysis platform](#) that helps companies understand what their customers and employees are telling them. Its AI reads open-ended survey comments, finds recurring topics and sentiment, and surfaces insights that would take a person weeks to find.

But people write personal details into those comments, even when surveys ask them not to. A customer names the sales rep who helped them, or the mechanic who serviced their car. Another shares a bank account number.

“All this information is relevant for our customers to redact. They have obligations to redact them,” says Pascal de Buren, Co-Founder and Co-CEO of Caplena. “It’s just a risk that they really need to avoid.”

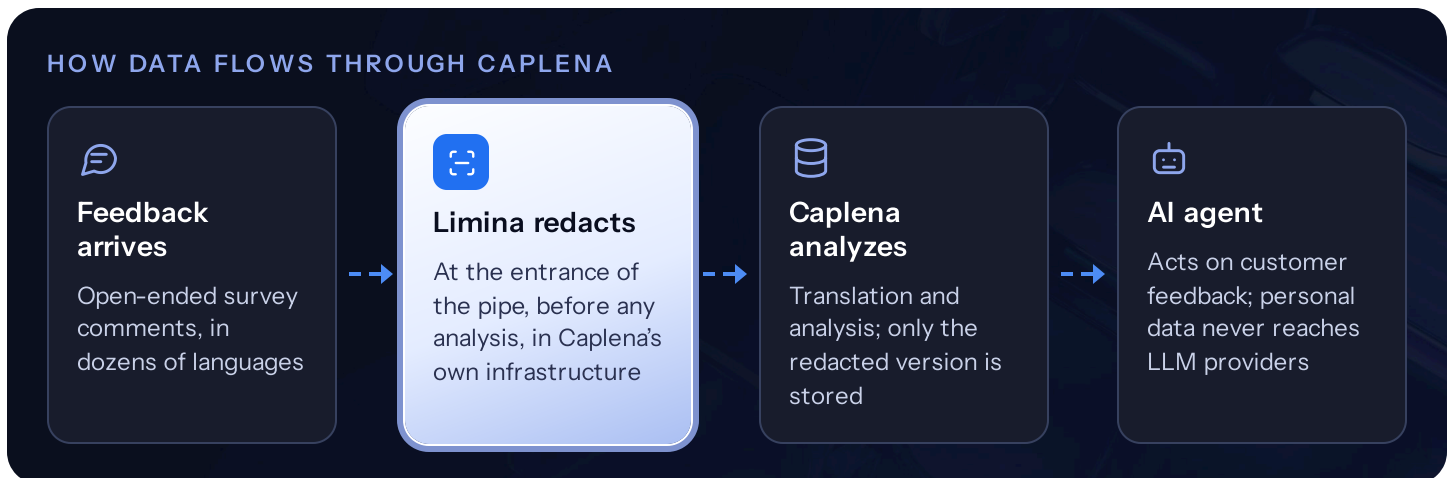
For Caplena’s customers, the stakes are high. Employee feedback can’t be used to monitor individual staff. Financial details can’t be stored or viewed. And Caplena’s home market, the DACH region, is among the most privacy-sensitive in the world.

Caplena needed redaction that met two requirements. First, it had to be accurate on the hardest cases: names, and numerical PII like account numbers. Second, it had to run on Caplena’s own infrastructure, so customer data never passed through another cloud service before it was anonymized.

02 THE SOLUTION

Redaction at the front door

Caplena chose Limina (then Private AI) in 2022 and built it into the very start of its data ingestion.



“If you have a pipe flowing into Caplena, it sits right at the entrance of that pipe,” says de Buren. “Before we touch the data with any kind of logic on our side, translation, any kind of analysis, it is first redacted.”

Only the redacted version is ever stored. The unredacted original never reaches Caplena’s database, its analysis, or the LLM providers behind its AI agent.

Caplena goes further than many customers require. Redaction cleans the open text, but customers also segment results by structured details like country or subscription tier. So Caplena adds its own safeguard: dashboards stop showing results when filters narrow far enough to point to a single person.

Caplena gives customers control, too. Using Limina's configuration options, customers choose which entities to redact, based on the analysis they need. A company comparing competitors can keep organization names; one analyzing sensitive employee feedback can redact more.

Entity	Comparing competitors	Sensitive employee feedback
PERSON NAME	✓ Redact	✓ Redact
ORGANIZATION	Keep	✓ Redact
ACCOUNT NUMBER	✓ Redact	✓ Redact

Illustrative example of entity configuration per analysis.

With a team of 24 people, plus roughly 100 AI agents, Caplena keeps its focus on its core product. Building redaction in-house was never on the table.



24 people + ~100 AI agents



For us, it was always clear we work on what makes our beer taste better. Whenever we had cases that didn't work, we could just send them over, and Limina would create synthetic data and fine-tune its models. If we had to do that all by ourselves, that would just be a great hindrance.

Pascal de Buren · Co-Founder and Co-CEO, Caplena

03 THE RESULTS

Privacy as the foundation for growth

Over four years, redaction has gone from an optional setting to a standard that customers ask for.

"It's become more of a standard," says de Buren. "Much more people do it, much more people ask for it. It is a must-have feature for them."

The rise of AI has raised the stakes further. Caplena's [AI agent now acts on customer feedback](#), and customers want assurance that personal data never reaches LLM providers.

"It's all about who needs to know what," says de Buren.

“

*Without a redaction solution, there would probably be **zero growth**.*

Pascal de Buren · Co-Founder and Co-CEO, Caplena

The results show up in four places:



Customer growth

Redacting customer data is, in de Buren's words, “non-negotiable,” and it underpins Caplena's growth.



Customer confidence

More customers are comfortable uploading data that may contain PII. In 2026 alone, Caplena has anonymized **more than 11 million rows** of feedback in the first ten months of 2026, **10x more** than in all of 2022.



Security reviews

When prospects ask about accuracy, Caplena shares Limina's benchmarks by language and industry. In German, Caplena's home-market language, Limina's 2026 benchmark shows an **adjusted recall of 97%**. Adjusted recall measures how much sensitive data is caught and removed, even if it's labelled slightly differently. Customers rarely set a specific threshold, but they've always been satisfied with the numbers they see.



Global reach

As Limina expanded to **more than 50 languages**, Caplena extended redaction to customers in Southeast Asia and the Middle East.

04 WHAT'S NEXT

Caplena is already looking at the next frontier: attributes that could identify someone in combination, such as gender or sexual orientation inferred from a comment. As de Buren puts it, the goal is to remove anything that, even in aggregate, could lead back to an individual.

Put your most protected data **to work.**

TALK TO A TECHNICAL EXPERT →

ALSO TRUSTED BY

