

In Europe, sovereignty is everyone's buzzword. For this defense company, it's policy.

How a fast-growing German defense company stopped trusting vendor claims, made sovereign communication a matter of policy, and built resilience other tools could never give them.



The company: where information has a price tag

Lateration GmbH is a growing German defense company, trusted by customers to manage highly sensitive operational military intelligence. In their own words, **"Discretion is key"**; the defence company's contracts rest on the confidence that what customers share stays protected.

A single exposed conversation can cost a program, a customer relationship, or a competitive advantage, benefiting anyone from scammers to antagonistic nation-states. For the company's Head of IT, Jan Schlachter, that makes communication security part of what Lateration sells, not an internal IT concern. In his view, a company handling this kind of material should never need a business case for protecting its conversations. The business case should be required for leaving them unprotected.

At a Glance

Sector

Defence Industry,
Germany

Organisation

Lateration, GmbH

Employees

50

Challenges

- Rising reliance on Microsoft 365
- End-to-end encryption costs extra
- EU legal footing is weakening
- Urgent need for a sovereign EU alternative

Solutions

- Wire: BSI-certified secure messaging
- Trusted channel for sensitive communications
- Mandatory adoption for protected exchanges

The problem: by the time there's proof, it's already too late

For Lateration the risk of depending on a foreign provider was never about one dramatic incident. It was about an unavoidable cost. Sooner or later, he believes, that dependency extracts its cost, whether as legal exposure, as lock-in pricing, or as access that vanishes overnight. So when asked to name the single moment behind the decision to stop depending on Microsoft for sensitive communication, he refuses the premise, because in his world, the demand for a clear triggering event is itself the trap. Wait for proof and you have already lost.

"You cannot nail it down to one precise moment. The moment you start digging, it just gets worse and worse."

The digging kept turning up the same pattern. Encryption that should be a baseline was sold as a paid add-on, in a proprietary implementation that would make leaving harder every month. Then the legal ground moved. For years, European risk assessments of US cloud providers leaned on the independence of American oversight bodies. On June 29, 2026, the US Supreme Court ruled in *Trump v. Slaughter* that the Federal Trade Commission's independence protections were unconstitutional, ending nine decades of precedent that had insulated the agency from at-will political control.

[Source: Supreme Court of the United States, Trump v. Slaughter, No. 25-332, decided June 29, 2026]

Every risk assessment that leaned on that independence lost its foundation overnight.

"Everybody, including the EU, built a castle in the sky. And it's falling apart. The impact is getting closer. The earlier you realize it and the earlier you act, the better."



Encryption was sold
as an add-on



Ending nine decades
of precedent



US Supreme Court ruled in
Trump v. Slaughter that the
Federal Trade Commission's
independence protections
were unconstitutional



The search: how to evaluate when every vendor claims sovereignty

It was never about if Lateration needed sovereignty. The Head of IT is one of the most committed sovereignty advocates you will ever meet. The hard part was the market noise. Suddenly, every vendor offered sovereignty, and the word had become a point in corporate bingo. The question was, how do you evaluate vendors when they claim to provide sovereignty?

His filter was verification: don't just accept vendor claims, start with the certifier. In this case it was Wire's certification by the BSI, Germany's Federal Office for Information Security. The BSI's authority and judgment were proof that can't simply be bought or faked through a landing page. It was the reason Wire outshone the competition, something that marketing claims alone could never have earned.



Certification by BSI



Authority and judgment
proof of trust



Wire outshone the
competition

Wire at Lateration: Sovereignty as policy, not preference

Today, the rule at Lateration is simple: sensitive material moves on Wire. "Every time we're talking statistics, the spreadsheets with the important numbers, it happens on Wire. I'm the one enforcing it, because that's what people pay me for. All the sensitive stuff... is happening on Wire already."

The question of quality never even came up. "We didn't have to mention sound or video quality once. Everything just works flawlessly, and that's a good sign."

But for a defense company, the deeper value is resilience. Wire gives Lateration a sovereign channel that stands on its own, regardless of what happens to the rest of the stack.

"In the military we have a PACE plan: Primary, Alternative, Contingency, Emergency. If you go on a mission with just your primary plan, good luck. It's the same with communications. If you have one source of communication and it breaks away, you're left with nothing."





The impact:

Sovereignty as a business asset

The most immediate result is protection by design: the company's most sensitive communication, from sensitive information to customer-related material, now runs through an end-to-end encrypted, BSI-certified channel as a matter of policy rather than individual discipline.

The second result is continuity. With Wire as an independent channel, a failure or compromise of the primary IT environment no longer means a communication blackout. For a defense company, that is not convenience. Its operational doctrine applied to IT.

The third result is commercial. In the defense sector, taking sovereignty seriously is itself a market signal, and Lateration ensures it's part of how the company presents itself.

"It plays into our story. We want to show that we got the message, that the wind is changing toward sovereignty, and that we are taking it seriously. We are not the ones who are just talking. We are the ones taking action."



Wire continuity



Digital sovereignty



End-to-end encryption

What this means for defense organizations

In the defense sector, the appetite for capability does not always match the appetite for security. The defense sector is growing faster than its security culture. That is the uncomfortable observation at the heart of Lateration's story, and three lessons from it apply to any organization in the sector.

1

Start with the certifier, not the vendor

In a market where sovereignty is on every slide, independent certification, in Germany the BSI, is the filter that separates architecture from marketing. Begin the evaluation at the certifier's list and let vendors earn their way onto your shortlist from there.

2

Never single-source your communications

PACE thinking, standard doctrine in the military, applies directly to IT. If your entire organization communicates through one provider's stack, a single failure or compromise leaves you silent at the worst possible moment. A sovereign, independent channel is not a redundancy expense. It is the contingency plan.

3

Reread your risk assessments before you renew them

The legal assumptions under US cloud risk frameworks are moving, and recent rulings show they can move overnight. An assessment written on last year's assumptions may already be describing a world that no longer exists.

The market signal

"Organizations like ours are moving towards data sovereignty, and we are ready to move to the providers who genuinely deliver it."

Jan puts it more bluntly for his industry:

"Defense has become fashionable. Everyone wants AI, everyone wants drones, everyone wants a place in the sector. But the price attached to that ambition is measured in national, and global, consequence. An organization unwilling to treat security as a first-order responsibility has no business operating in it."

"Sovereignty isn't a feature
- it's an obligation that
comes with the mission."



Jan Schlachter, Head of IT. Lateration GmbH