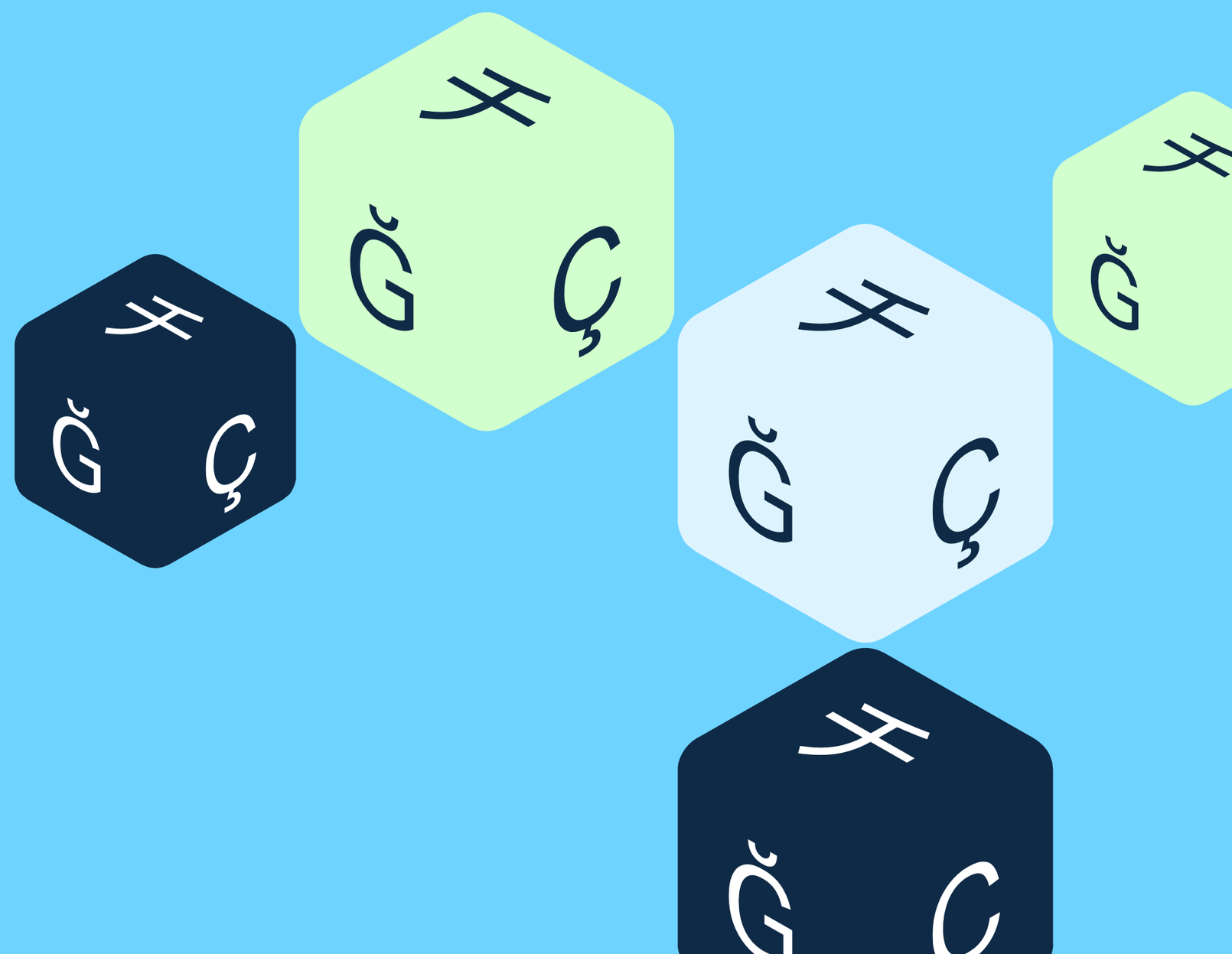
DeepL

Bericht

Whitepaper zu Sicherheit und Datenresidenz: Das hybride Infrastrukturmodell

Sichere Architektur für die Kombination von AWS und privaten Rechenzentren



Überblick

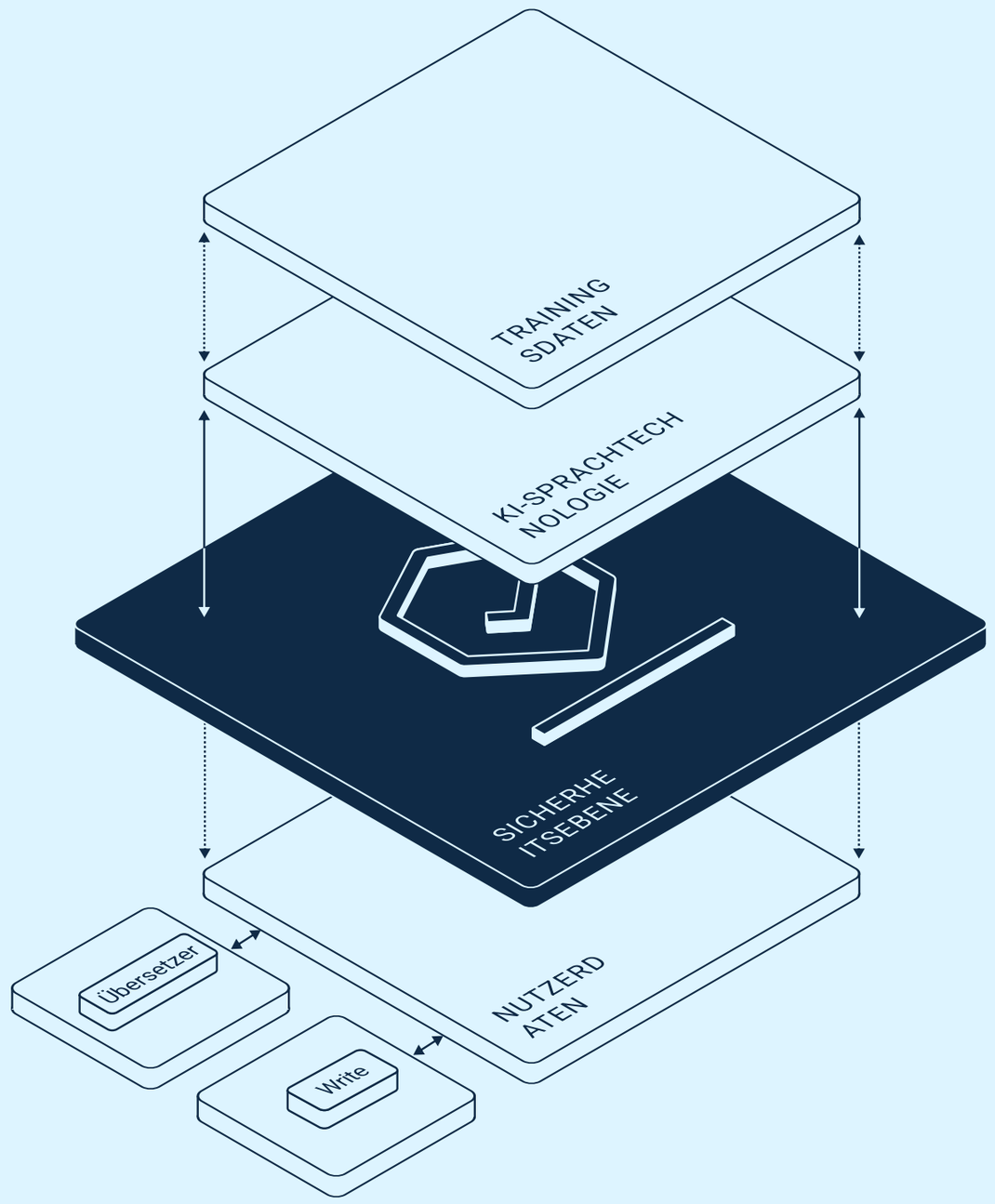
Wenn Sie auf eine hybride Infrastruktur umsteigen wollen, brauchen Sie hierfür ein Sicherheitsmodell, das genauso leistungsfähig ist wie das Ihres lokalen Rechenzentrums. Unsere Architektur wurde speziell für Unternehmen mit hohen Datenschutzanforderungen entwickelt: Sie kombiniert die Skalierbarkeit von AWS mit der Datenhoheit unserer privaten Rechenzentren.

Mit einem hybriden Ansatz können wir Kunden besser unterstützen: Wir können uns die Erfahrung zunutze machen, die AWS im Betrieb leistungsstarker Datenbanken hat, und uns stattdessen stärker darauf konzentrieren, Kunden zuverlässigere und effektivere Lösungen bereitzustellen.

Unser Engagement für Sicherheit wird durch branchenübliche Zertifikate bestätigt. So können Sie sich sicher sein, dass Ihre Compliance nicht unter der Umstellung auf das neue, hybride Modell leidet.

- Compliance-Standards: Wir sind vollständig nach SOC 2 Typ II und ISO 27001 zertifiziert.

- Wir erfüllen den BSI-Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) für die relevanten Services und Regionen, einschließlich AWS Stockholm (eu-north-1).



Hybride Sicherheitsarchitektur

Das folgende Diagramm veranschaulicht den allgemeinen Ablauf unserer Infrastruktur sowie die Integration zwischen unserem sicheren Edge, AWS Stockholm, und unseren privaten Rechenzentren.

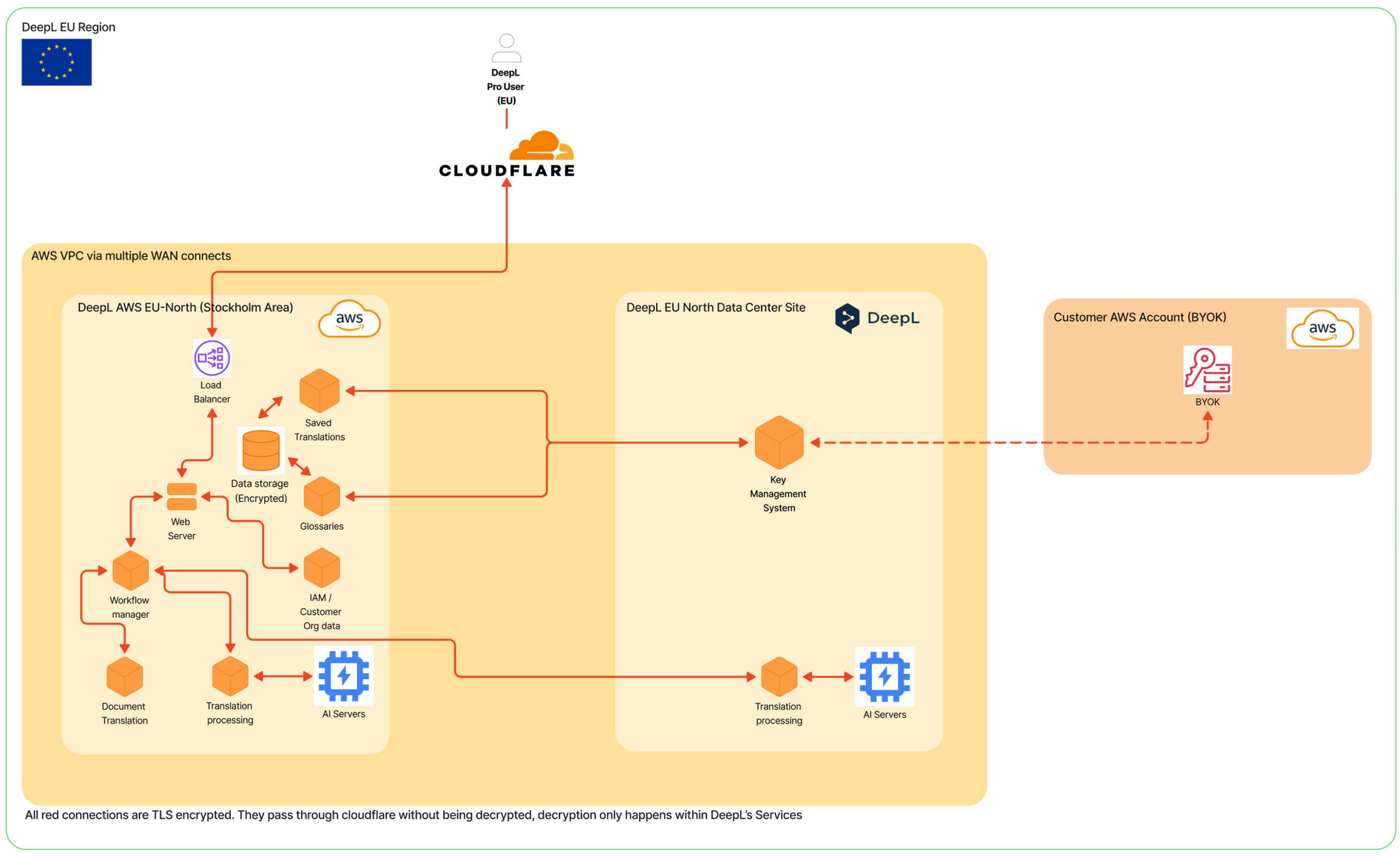


Abbildung 1

Wie Sie in Abbildung 1 sehen, durchlaufen Anfragen erst einmal unser Cloudflare-CDN, das uns eine zusätzliche Sicherheitsebene bietet, indem es schädliche Bot-Anfragen herausfiltert.
Nach dem Filtern kommen die weiterhin verschlüsselten Anfragen bei unseren Servern an. Statische Webinhalte wie Bilder und JavaScript werden direkt von Cloudflare bereitgestellt, um die Seitenladezeiten für alle Kunden zu verbessern.

Anfragen werden von unseren Load Balancern entschlüsselt und anschließend an nachgelagerte Services weitergeleitet, wo sie über unsere interne TLS-Verschlüsselungsebene verarbeitet werden.

Übersetzungsanfragen werden geprüft, beispielsweise auf Sprachkombination, bevor sie zu unseren Übersetzungsengines gesendet werden. Die Übersetzungsengines befinden sich sowohl bei AWS als auch On-Premises. So haben wir die Möglichkeit, Rechenkapazitäten möglichst effektiv zu nutzen.

Wenn Anfragen zwischen Rechenzentren übertragen werden, werden sie über schnelle VPN-Verbindungen (TLS-Anwendungsebene + MACSec-Fallback) verschlüsselt.

Wenn Kunden Glossare oder gespeicherte Übersetzungen nutzen, werden diese Inhalte mit unserem intern verwalteten KMS verschlüsselt (Envelope-Verschlüsselung). Standardmäßig kommen hierbei von DeepL verwaltete Verschlüsselungsschlüssel zum Einsatz, die in unserem lokalen Dienst gehostet werden. Es stehen auch BYOK-Optionen zur Verfügung, bei denen Kunden eigene Schlüssel über ihr AWS-Konto bereitstellen.

Die Envelope-verschlüsselten Daten werden außerdem auf Geräten gespeichert, die ruhende Daten zusätzlich verschlüsseln. Die Verschlüsselung ruhender Daten wird von AWS bereitgestellt, unter Verwendung von AWS-Schlüsseln und -KMS.

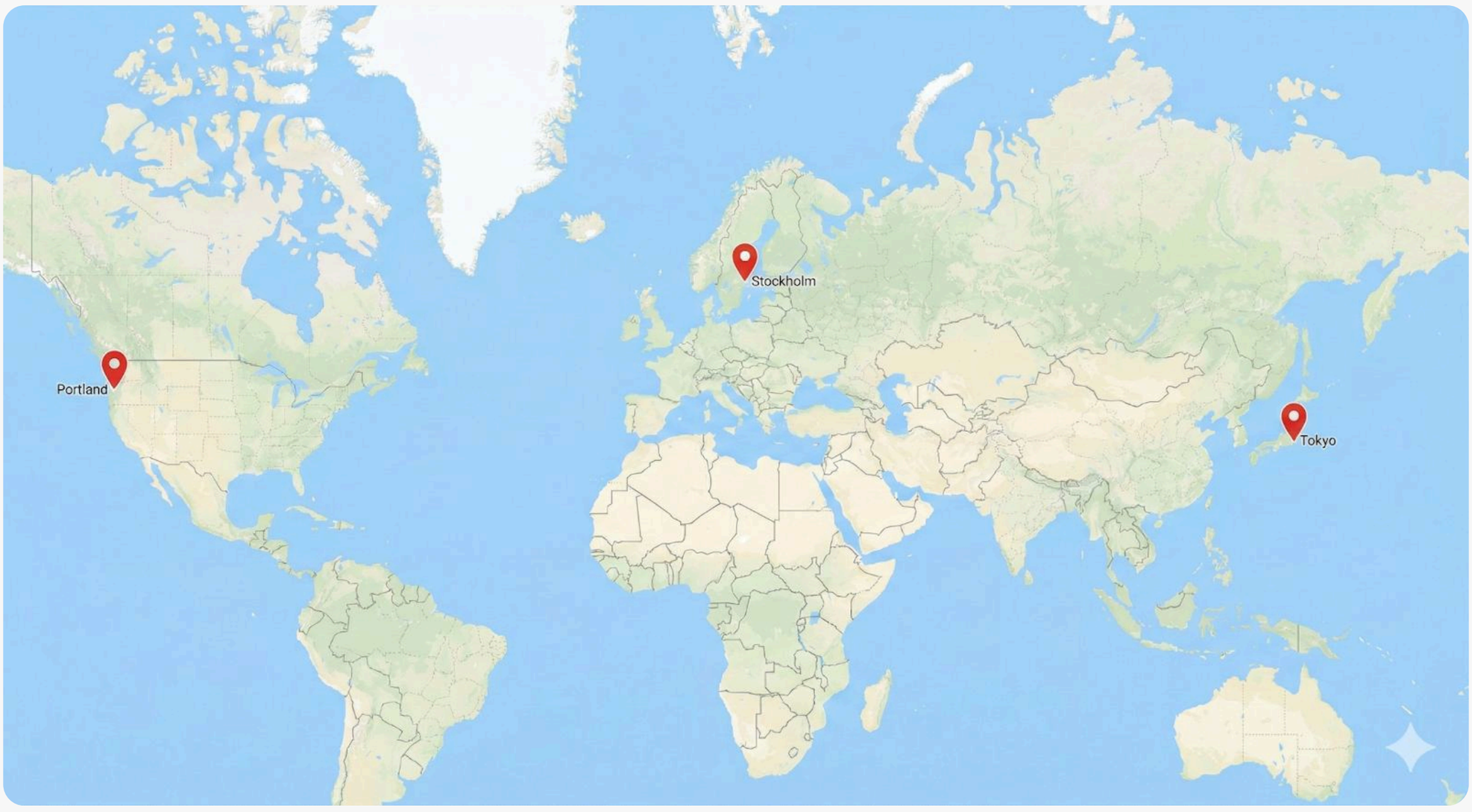


Abbildung 2

Abbildung 2 zeigt die Regionen, die DeepL in seiner globalen Umgebung verwendet. Oregon und Tokio sind die AWS-basierten Regionen für unsere regionalen Kundenservices. Stockholm ist unsere hybride Region, die AWS mit unserem eigenen Rechenzentrum verbindet, mit dem wir europäische Datenresidenz unterstützen.

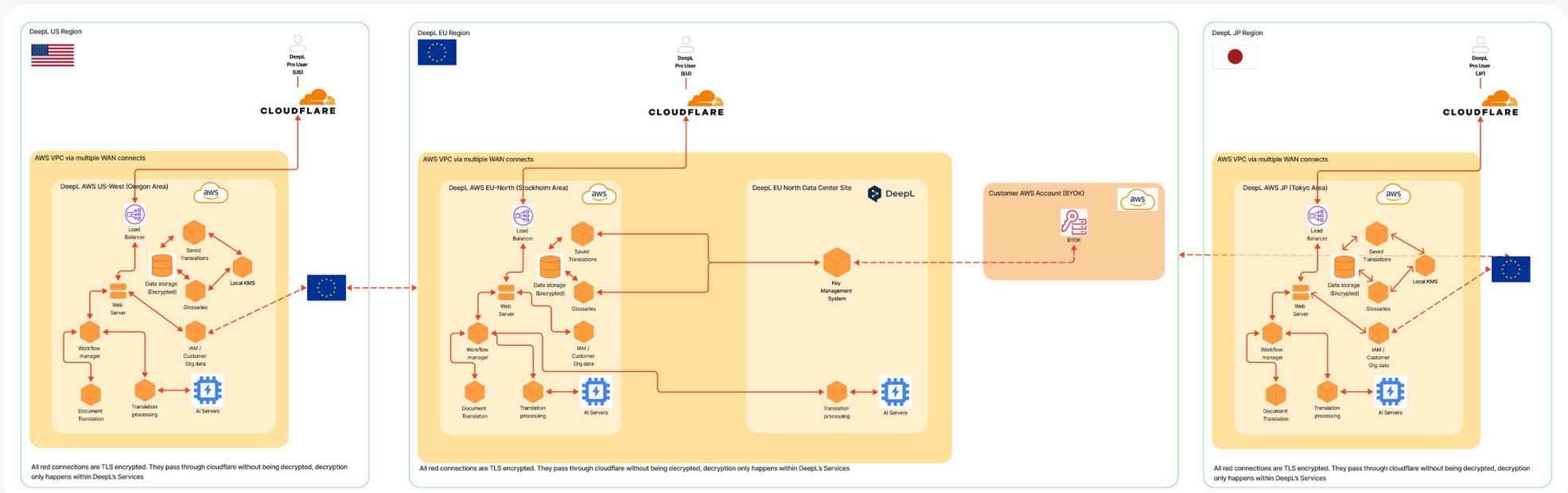


Abbildung 3

Wie Sie in Abbildung 3 sehen, decken unsere regionalen Bereitstellungen den gesamten Stack ab und gewährleisten, dass Kundeninteraktionen immer innerhalb der bevorzugten Region verarbeitet werden. Nur in Europa werden die Schlüssel außerhalb von AWS verwaltet. Die Option „Bring Your Own Key“ ist in allen Regionen verfügbar und basiert auf AWS. Die Konfiguration des IAM (Authentifizierung, Lizenzen) erfolgt über eine einseitige Synchronisierung über den europäischen Standort.

Garantierte Datenverarbeitung

Wir bieten garantierte Datenresidenz als kostenpflichtiges Add-on an, um die Einhaltung von Vorschriften zu vereinfachen und interne Audit-Anforderungen zu erfüllen. Kunden, die sich für Datenresidenz entscheiden, haben folgende Optionen:

- **Regionsspezifische Verarbeitung über kostenpflichtiges Add-on:** Hiermit werden Inhalte von Kunden exklusiv innerhalb der von ihnen gewählten Region verarbeitet und gespeichert.

- **Hybride Datenhoheit:** Wir nutzen zwar AWS-Regionen innerhalb der EU (beispielsweise Stockholm), doch Verschlüsselungsschlüssel werden über unseren anbieterunabhängigen KMS außerhalb von AWS in europäischen Rechenzentren gespeichert, sofern sich Kunden nicht für das BYOK-Modell entscheiden, für das eine AWS-Funktion zum Einsatz kommt.

- In anderen Regionen wird das Schlüsselmaterial mithilfe unseres anbieterunabhängigen KMS-Dienstes auf AWS gespeichert.

- Bei EU-Kunden ohne das Datenresidenz-Add-on behält sich DeepL das Recht vor, Daten in allen unseren Regionen zu verarbeiten.

Sicherer Zero-Trust-Edge

Wir setzen bei unserem globalen Datenverkehr auf das Zero-Trust-Modell. Wir nutzen zwar Cloudflare für seine erstklassige Verfügbarkeit, doch Ihre Inhalte bleiben für den Edge-Anbieter eine Blackbox.

- **Verschlüsselte Übertragung:** Cloudflare kümmert sich um die Bot-Erkennung und DDoS-Abwehr, kann dabei jedoch nicht Ihre Übersetzungsanfragen entschlüsseln.

- **TLS-Verschlüsselung übertragener Daten:** Jede Anfrage wird per TLS-Verschlüsselung geschützt (dargestellt durch die roten Linien im Diagramm) – von Ihrem Terminal bis hin zu unserer sicheren Umgebung.

Flüchtige Datenverarbeitung

Bei API-, Website- und App-Interaktionen halten wir uns strikt an den Grundsatz der Datenminimierung.

- **Keine Speicherung:** Textvorgänge werden einfach direkt während der Übertragung verarbeitet. Ihr Ausgangstext oder Ihre Übersetzungen werden hierbei nicht auf Datenträgern gespeichert.

- **Just-in-Time-Entschlüsselung:** Daten werden nur entschlüsselt, während sie in unseren Services verarbeitet werden, und anschließend sofort wieder verschlüsselt.

Datenhoheit (KMS und BYOK)

Mit unserem individuellen Schlüsselmanagement-Ansatz verbinden wir die Flexibilität der Cloud mit der Kontrolle lokaler Rechenzentren.

- **Anbieterunabhängiger KMS:** Unser Key Management Service (KMS) funktioniert unabhängig von AWS. In Europa wird er in unseren eigenen Rechenzentren betrieben. So stellen wir sicher, dass die Vertrauensgrundlage stets unter unserer physischen Kontrolle bleibt, selbst wenn AWS-Infrastruktur zum Einsatz kommt.

- **Bring Your Own Key (BYOK):** Übernehmen Sie die volle Kontrolle, indem Sie Ihre eigenen Unternehmensschlüssel direkt aus Ihrem AWS-KMS importieren.

- **Schutz auf Dokumentebene:** Bei gespeicherten Inhalten nutzen wir die sogenannte Envelope-Verschlüsselungsmethode, bei der die Client-Anwendung den Schlüssel besitzt. So wird sichergestellt, dass Inhalte doppelt verschlüsselt werden – einmal auf Objektebene und einmal auf Speicherebene (Verschlüsselung ruhender Daten) – und für unbefugte Dritte unzugänglich sind. Bei der Dokumentübersetzung kommt eine ähnliche doppelte Verschlüsselung zum Einsatz, jedoch mit symmetrischer Verschlüsselung auf Dokumentebene statt mit Envelope-Verschlüsselung.

Sicherheitsübersicht

Funktion	Schutzmechanismus	Sicherheitsvorteil
Übertragene Daten	TLS 1.2+	TLS gilt als Standardmethode zur Verschlüsselung übertragener Daten und wird weltweit von Institutionen mit höchsten Standards eingesetzt.
Edge-Schutz	CDN ohne Entschlüsselung	Wir verwenden ein CDN, um die Bereitstellung statischer Inhalte wie Bilder und JavaScript zu beschleunigen und so die Performance zu verbessern. Darüber hinaus erhalten wir mit dem CDN eine zusätzliche Verteidigungslinie gegen Bots und DDoS-Angriffe. Unser CDN hat jedoch keinerlei Einblick in Ihre verschlüsselten Verbindungen zu unseren Services.
Gespeicherte Daten	Anbieterunabhängiger KMS + BYOK-Option	Zusätzlich zur normalen Verschlüsselung ruhender Daten, die in unserem Speicher zum Einsatz kommt, nutzen wir eine weitere Verschlüsselungsebene, mit der wir die Kontrolle über Schlüssel und kryptografische Elemente behalten – sowohl On-Premises als auch in der Cloud.
Verarbeitung	Just-in-Time-Datenentschlüsselung	Wir entschlüsseln Datenverkehr erst zum letztmöglichen Zeitpunkt und arbeiten ständig daran, dieses Prinzip noch stärker in unseren Services umzusetzen.

Glossar

AWS
Amazon Web Services

BSI
Bundesamt für Sicherheit
in der Informationstechnik

BYOK
Bring Your Own Key

DSGVO
Datenschutz-Grundverordnung (EU)

DDoS
Distributed Denial-of-Service

KMS
Key Management System

TLS
Transport Layer Security

VPC
Virtual Private Cloud

WAN
Wide Area Network

IAM
Identity and Access Management

DeepL

DeepL SE
Maarweg 165
50825 Köln
info@deepl.com