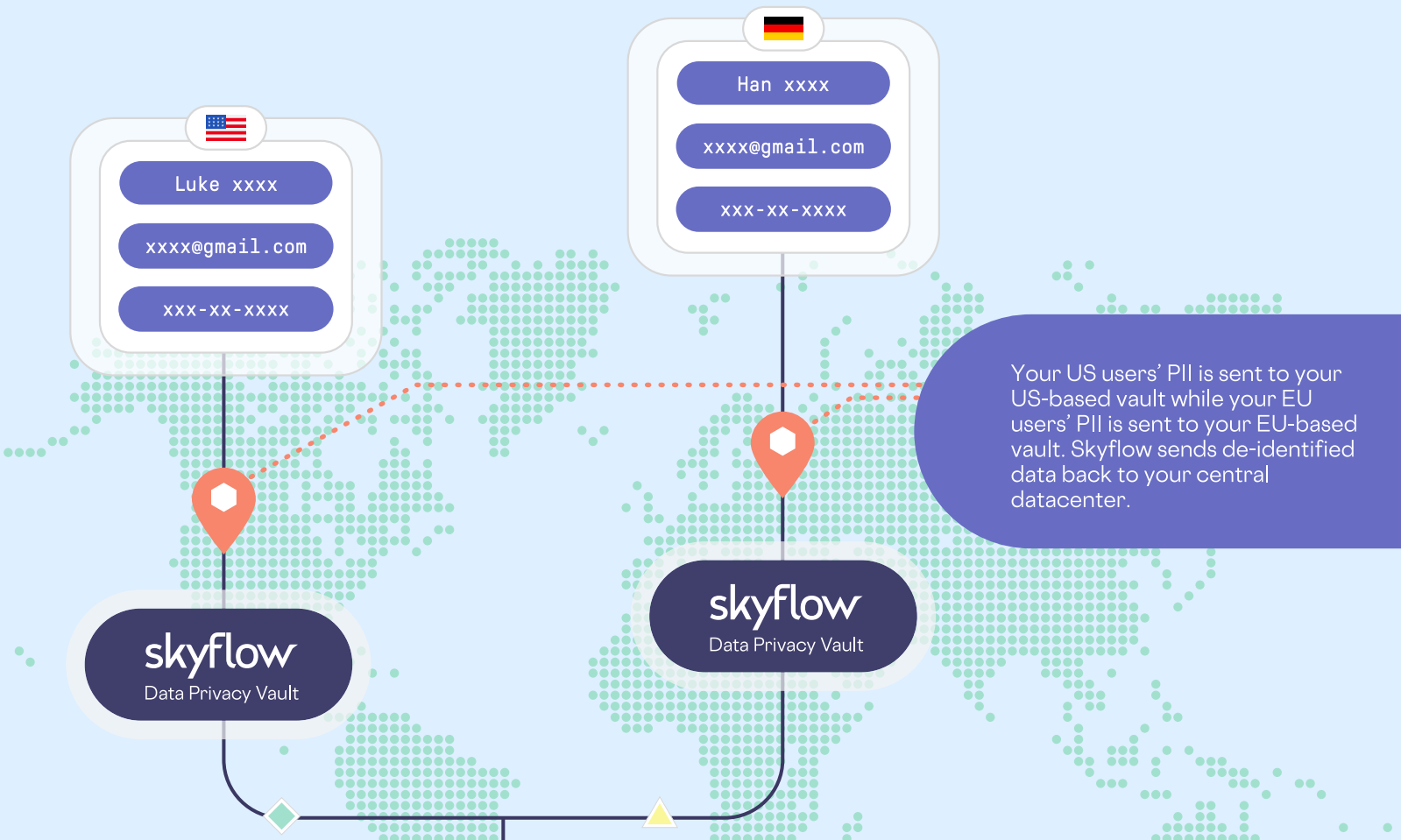
Data Residency Made Easy

skyflow

Put your Skyflow Vault where you need it and easily satisfy GDPR, Schrems II, BDSG, and other data residency requirements.



Faster Time to Market

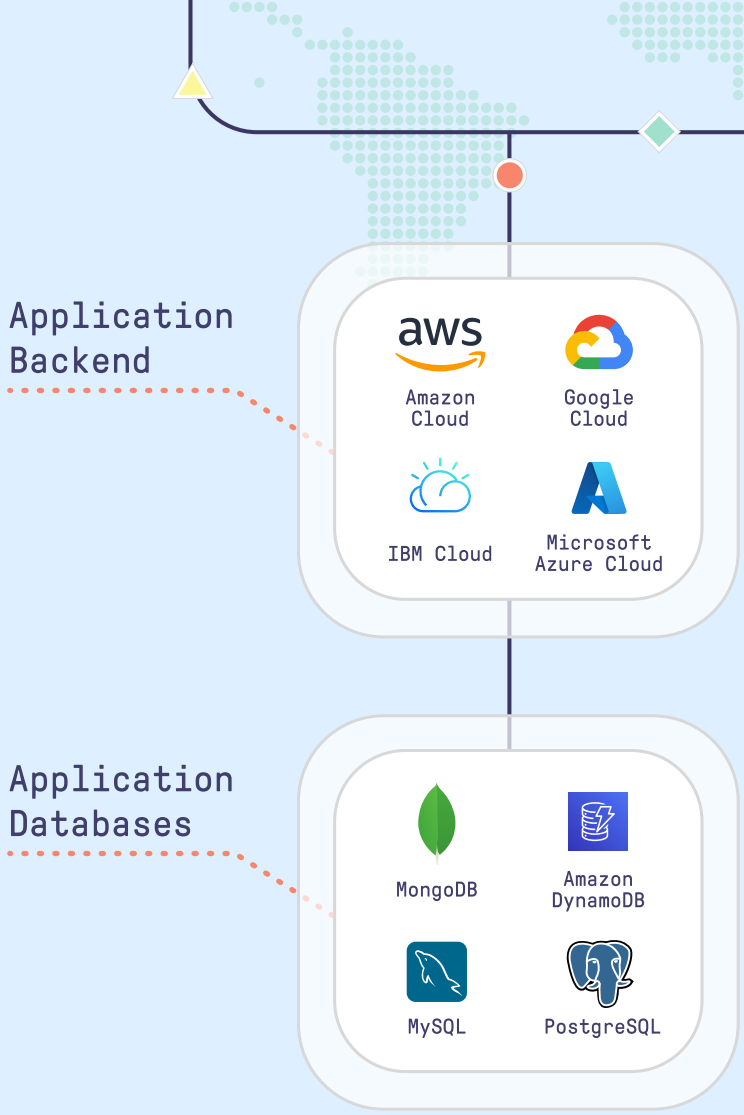
Deploy vaults for different regions to isolate just your sensitive customer data. Expand to new markets with ease, and avoid messy infrastructure migrations.

Localization with No Complexity

Satisfy data residency requirements without having to replicate your entire infrastructure in every region.

Minimize Data Handling Risk

Your customer data is only shared with application users in the same region, reducing the compliance scope and security burden.



De-identified data is sent to the application backend and stored within the application database.

De-identified and other non-sensitive data are sent to downstream services to power analytics and machine learning. Only Skyflow needs to be deployed based on customer location, because the backend infrastructure is insulated from PII.

Data residency is a common feature of many data privacy laws. Data residency requirements govern the **location, control,** and **security** of sensitive data within a country or region.

	Data Residency Need	Skyflow Solution
Location	Control where data is stored	Host your Skyflow vault VPC anywhere in the world
Control	Set policies to govern data access and ensure auditability	Skyflow's Data Governance Engine and Audit Logs ensure control and auditability of data stored in your vault
Security	Protect data through extensive digital and physical security measures	Skyflow's polymorphic encryption, tokenization, and redaction secure data in your vault, and Skyflow leverages the physical datacenter security of AWS

Learn more at www.skyflow.com