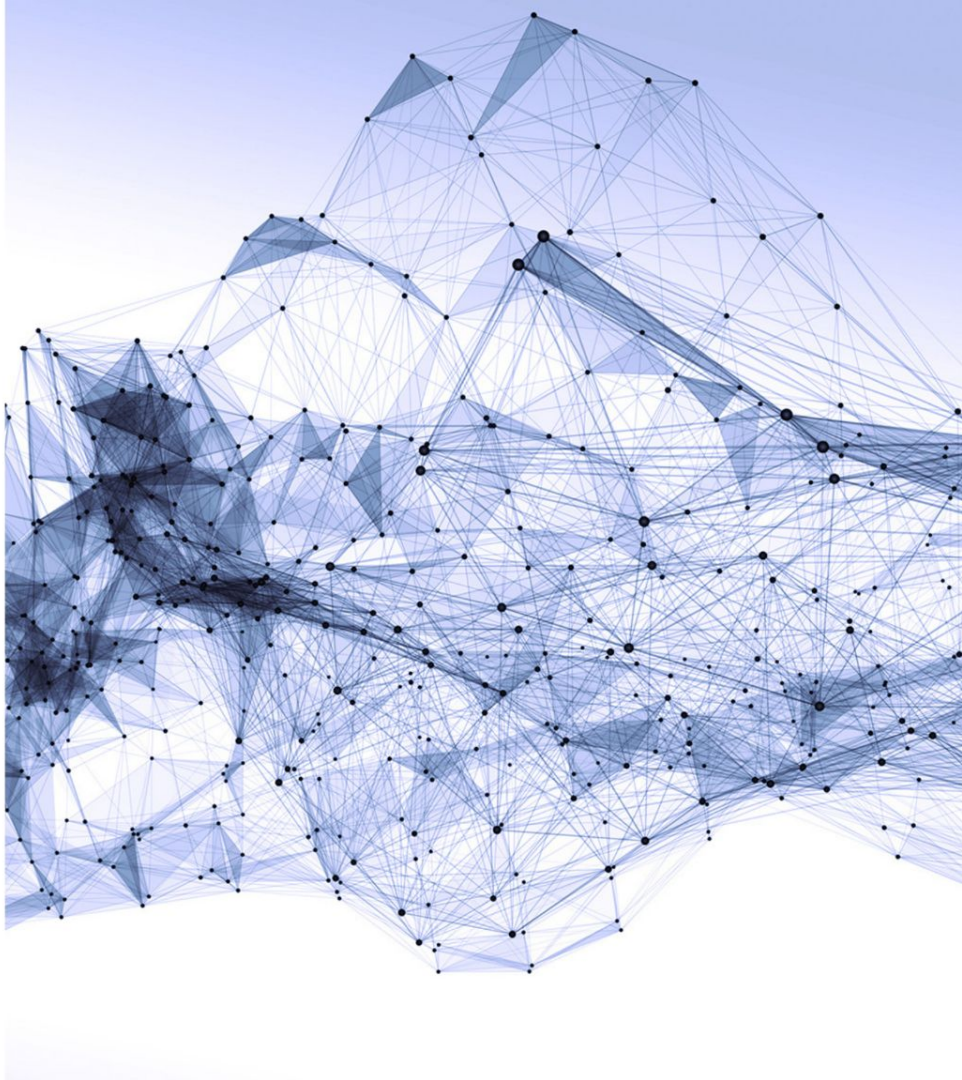
Healthcare SaaS

How to capture new markets faster with Kubernetes and cloud-native compliance

22nd June, 11.30-12.00 CEST

Healthcare SaaS challenges

1. Need for speed drives cloud adoption
2. PII breaches can cause really bad PR (Vastamoo, 1177 etc)
3. Increased GDPR and security demands in public procurements
4. Increased activity & GDPR fines by DPAs
5. International healthcare SaaS means:
    a. Many national regulations
    b. Locality requirements drives hybrid deployments across multiple public clouds + onprem
6. Hosting EU citizens PII on American cloud providers, even in EU DCs, are not legal due to the fall of Privacy Shield



Intro

Dimitri Fagué, Product Marketing Manager @ OVHcloud

Robert Winter, CEO @ Elastisys

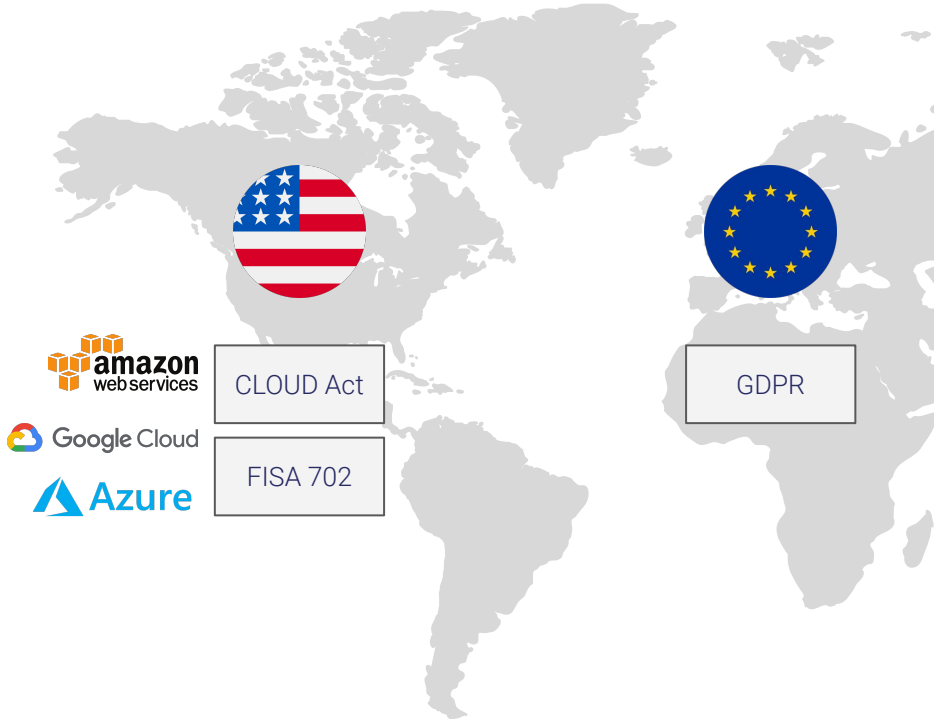
FISA, Cloud Act and the Fall of Privacy Shield

CLOUD Act: US law to compel US entities to provide access to information under their control, regardless of location.

GDPR: EU data privacy law. EDPB updated data transfer recommendations (21/6 2021).

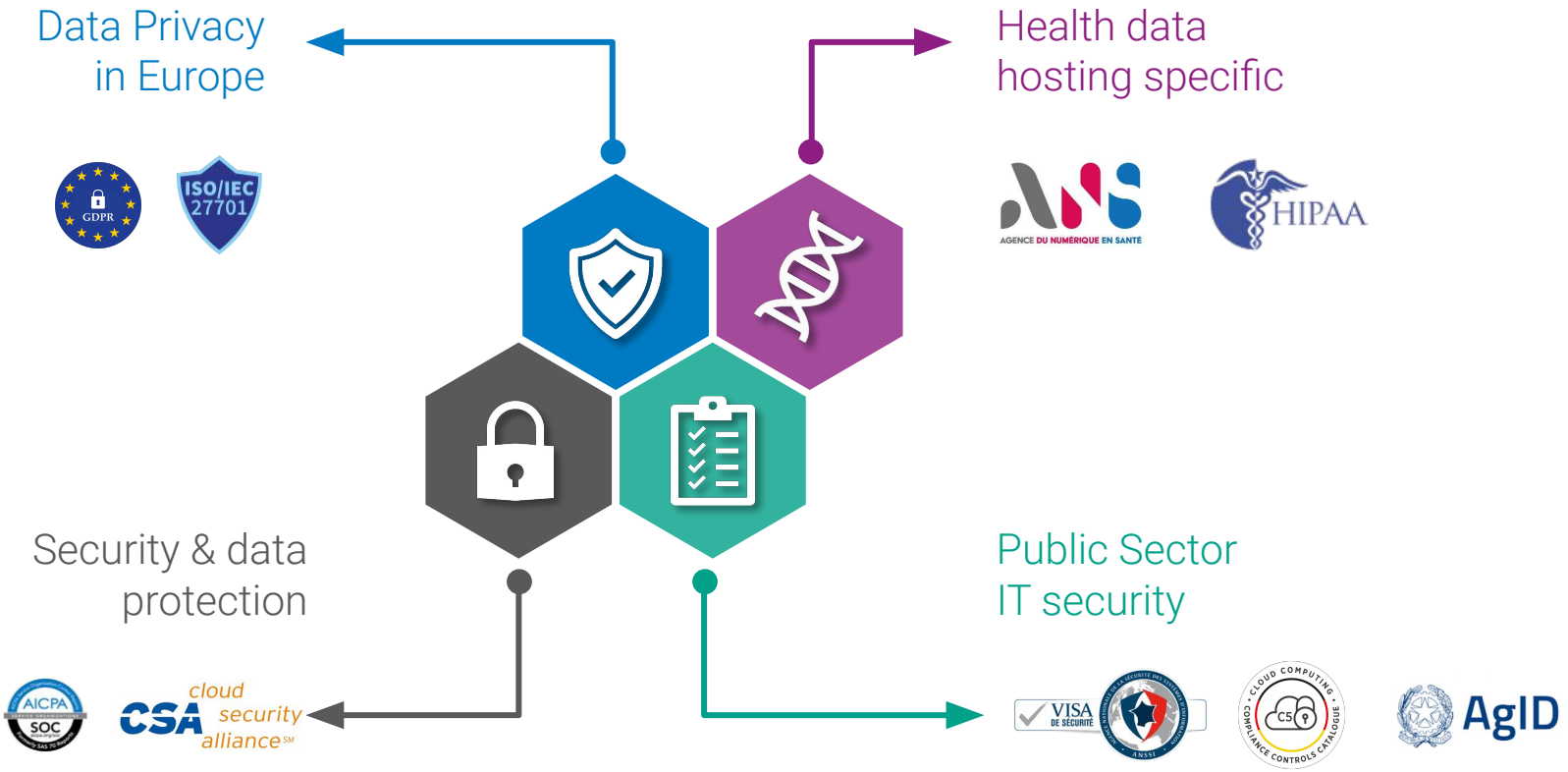
Privacy Shield: Previous US-EU personal data transfer framework, invalidated by the European Court of Justice in July 2020.

FISA: Foreign Intelligence Surveillance Act. US amendment; section 702 authorizes foreign surveillance by the NSA which was deemed incompatible with the GDPR.



Data sovereignty: Your cloud provider's HQ plus territories where your data can be transferred

Health data compliance key aspects



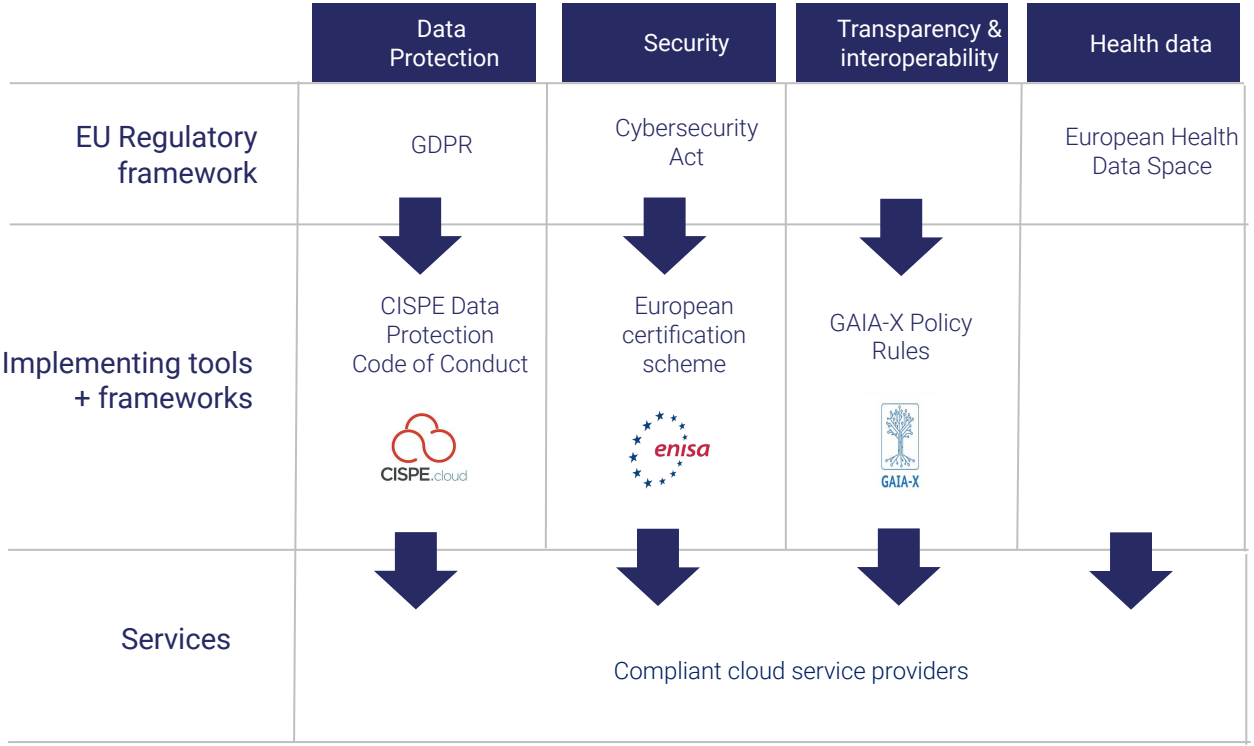
Health data compliance across EU and USA






	France	Germany	Poland	Italy	UK	USA
GDPR?	✔	✔	✔	✔	✔ (temp)	✘
Personal data hosting national regulations	Loi Informatique et Libertés 1978	§ 203 StGB criminal law (2019)	PDPA 1997	IDPA 196/2003	DPA 2018/2021	CA CCPA & NYC Shield Act
Health data hosting national regulations	HDS certification	Landers State Hospitals Acts	Articles 13 - 14 of the Act on Patients Right	No	NHS Data Security protection toolkit	HIPAA
Health data storing and processing localization	EU only (SCC not applicable)	EU only (SCC not applicable)	GDPR SCC applicable	GDPR SCC applicable	UK, EU, US	US
CSP security national certifications	ANSSI SecNumCloud	BSI CS, IT-Grundschutz Catalogues, SaaS Sicherheitsprofile	Zuch framework	AgID Cloud certification	Cyber Security Essentials Plus	FEDRamp
Health public sector GTM for CSPs	CAIH, unIHA, RESAH	Landers level	ZUCH marketplace	AgID Cloud marketplace	G-Cloud	

European initiatives

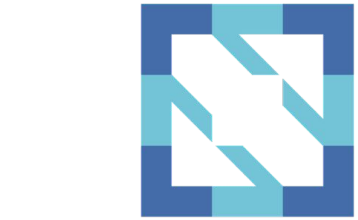


Cloud native to the rescue: compliance everywhere!

Cloud native:

- Innovation speed
- Scalability
- High availability
- Cloud agnosticity through open source

Often achieved using containers and Kubernetes. Needs to be **customized** to run in a compliant manner.



Management hands you a list like this

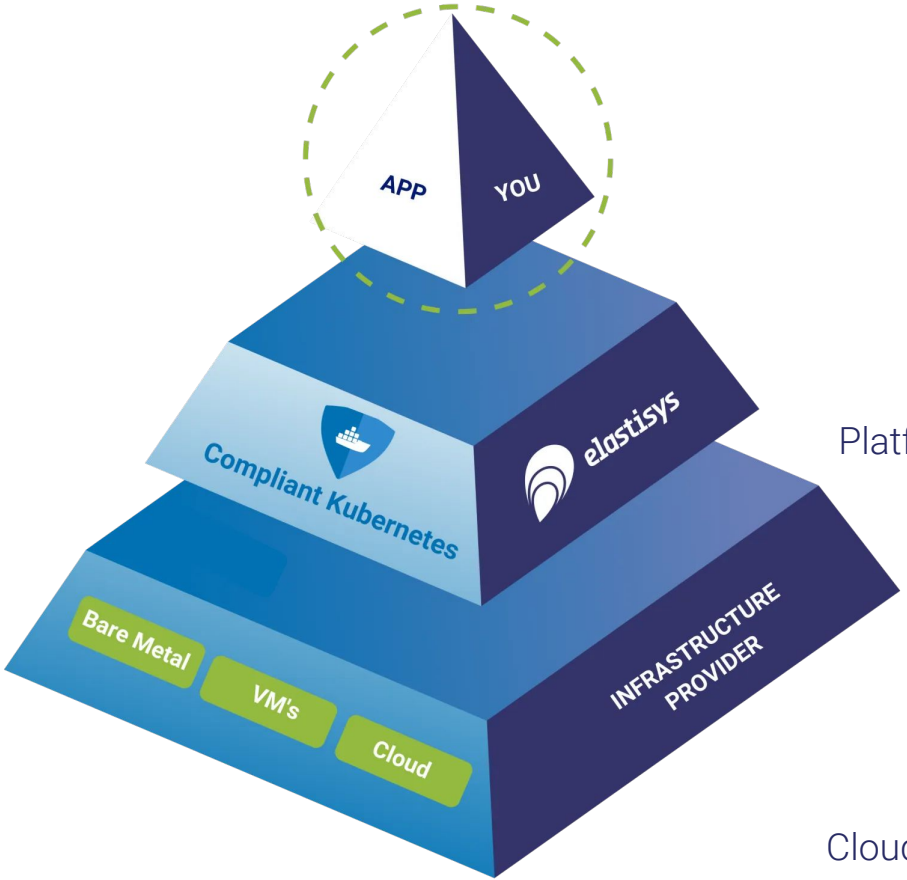
ISO 27001

Control A.5: Information Security Policies
Control A.6: Organisation of Information Security
Control A.7: Human Resource Security
Control A.8: Asset Management
Control A.9: Access control
Control A.10: Cryptography
Control A.11: Physical and Environmental Security
Control A.12: Operations Security
Control A.13: Communications Security
Control A.14: System Acquisition, Development & Maintenance
Control A.15: Supplier Relationships
Control A.16: Information Security Incident Management
Control A.17: Information Security Aspects of Business Continuity Management
Control A.18: Compliance

GDPR

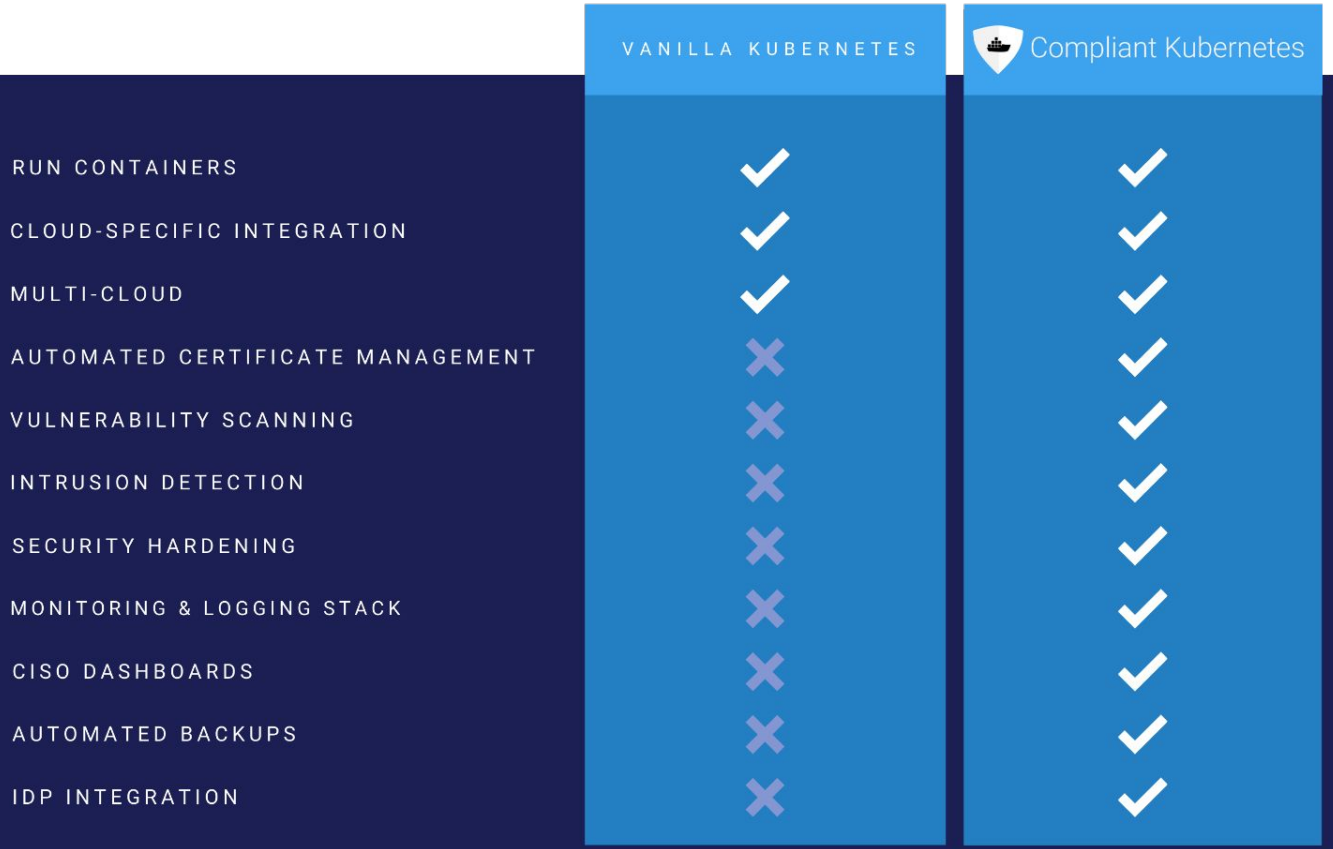
Article 5.1.e: Keep data no longer than necessary
Article 5.1.f: Prevent accidental loss, unauthorized access
Article 5.2: Accountability of processor
Article 6: Lawfulness of processing
Article 7: Conditions for consent
Article 7.3: Right to withdraw consent
Article 13.2.a: Transparent period for data processing
Article 17: Right to be forgotten
Article 20: Right to data portability
Article 25: Data protection by design and by default
Article 30: Records of processing activities
Article 32: Security of processing
Article 33: Notification of a personal data breach to the supervisory authority
Article 34: Communication of a personal data breach to the data subject

Compliance runs across the stack



	Controls	
You	Application security	Training
	Policies	Processes
Platform level	Disaster recovery	OS level patching
	Antivirus	Networking
	Secret management	Security patching
	Upgrades	Backups
	Monitoring	Logging
	Intrusion detection	Breach reporting
Cloud provider	Physical security	IaaS security

What does running a production grade container platform in healthcare mean?



What best practices should you adopt to deliver cloud-agnostic and according to all regulations?

Platform: Build or buy?

Build; everything is open source!
You can build and run it yourself

- Good to have; a 24/7 ops team with Kubernetes and container security skills
- Business case:
  - What SLOs do you have?
  - Is competence scarce or expensive?
  - Are you keeping up with the evolving landscape?

Buy

1. Buy and glue together services
   a. *American hyperscalers*: Decently easy and you can get everything on a single cloud
   b. *European clouds*: Currently not as complete service catalogues (but improving!)

2. Buy a fully managed service
   a. You can get a completely managed stack; containers, logging, monitoring, security, databases, message queues etc
   b. Enables the same experience and stack across multi-cloud

IaaS: How do you evaluate EU cloud providers?

- Legal jurisdiction
- Platform services for your use case
  - DBaaS, storage, MQaaS, MLaaS, Analytics, FaaS etc
- SLAs and uptime history
- Data center footprint for your markets
- Certifications
- Network connectivity to regional healthcare networks
- Specific controls you need to solve (disaster recovery options, multi AZ etc)

AMA

Dimitri Fagué, Product Marketing Manager @ OVHcloud

Robert Winter, CEO @ Elastisys