SUBLIMIS

WE WALK THE RIGHT LINE WITH YOU

AWS x XQ
HDS PARTNERSHIP OPPORTUNITY
THIRD PARTY VALIDATION

Paris, October 11th, 2023

SUBLIMIS

Table des matières

1. Executive summary

The present report aims at presenting an independent third-party validation related to the business opportunity of AWS partnering with XQ Message to address health data protection in the context of US-EU cross border data transfer involved using AWS Cloud and/or hosting services.

AWS is a US head-quartered cloud provider and cloud services provider. XQ is a US head-quartered scale-up offering agile encryption services at the data level.

Main observations:

- There is today a global context of geopolitical shifts that encourages digital and data sovereignty - while a regulatory inflation is strengthening organizations responsibilities towards data processing.
- At the same time, acceleration of digital transformation moves companies to more data driven models, interconnected ecosystems and monetized hyperintelligence.
- In between, organizations have to map conflicting regulations and face increased cyber risks that requires on a yearly basis more means and budgets.
- At the end, even when investing massively in both compliance and cybersecurity, CXOs still face significant compliance and cybersecurity gaps as well as customers pushbacks to invest in tools and solutions that addresses/solve these issues. Hence, boards and top management now look at cost optimization and post breach readiness.
- AWS is today offering Cloud services and data hosting services that are compliant with one of the most stringent Health standards of the market (HDS French health data hosting framework)
- HDS certification currently covers the following AWS regions:
    - Asia Pacific (Jakarta), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Milan), Europe (Paris), Europe (Stockholm), Europe (Zurich), Middle East (UAE), South America (Sao Paulo), USA East (Northern Virginia), USA East (Ohio), USA West (Northern California), and USA West (Oregon).

- However, despite all those investments, there are today massive challenges with regards to the compliance with EU data privacy and data protection regulation when using AWS solutions and services.
- Those challenges are not specific to AWS and are raised for any US based company submitted to the US Cloud Act and/or the US Patriotic Act.
- There is an existing precedent for Microsoft vs the German Court and German Data Protection authorities with regards to the use of Office 365. EU critical organizations (health, defense, regalian entities, and many others) tend to request a limitation and localization of their data within the restricted boundaries of their states.
- While AWS has adapted to market needs, and create local data centers, this seems to not be enough, at a moment when all cross-border data flows between EU and US legal validity is under permanent threat.
- Indeed, processing the data locally is now not sufficient to address data sovereignty, data privacy and data protection compliance.
- If a US player is involved, the processed data are submitted to the US Cloud and Patriots Acts that damages the sovereign applicability of EU rules to protect EU citizens data privacy.
- Indeed, there is the fact that the data can be physically transferred to the US through the use of a US company services, but there is also the case where the data is not transferred to a US company services, the data resides is the EU, but as the services are offered by a US company, and as this US company is submitted to the US Cloud and Patriot Acts, this US company could potentially be requested to provide the US government with access to the information from those EU companies. As well, in the context of operating customers systems, the US company could as share the data internally, which means outside from EU boundaries.
- Hence, the whole model is now being questioned and requires solutions.

We do believe that there is a "third way" that can generate a significant opportunity to unlock and catalyze business through this third-party validation on how XQ can help AWS achieve in-country GDPR and HDS regulatory requirements by implementing XQ.

The present third-party validation report will explain:

- Why those regulations are being questioned.
- How XQ is addressing those compliance frameworks as a US company
- How XQ is offering a combination that genuinely solve the problem through the cumulation of two innovative approaches
    - a first-of-its-kind quantum computing enhanced zero-trust data protection protocol way to protect data that meets EU data privacy standards.
    - an innovative governance model that puts encryption keys in the hands of the customers which means that even if using AWS and XQ services, the encrypted data are never accessed neither by AWS nor by XQ, making the data out scope of applicability of US Patriot Act and Cloud Act.

- How to unlock business opportunities and scale up a winning AWS x XQ partnership model

A signed attestation is provided at the end of the report to testify, based on our audit results, that XQ is committed to EU privacy and security compliance.

2. Third-Party/reviewer Qualifications

The present request for a third-party Validation was transmitted to Sublimis by THE DIGITAL RED LINE SERVICES, a niche boutique specialized in independent advisory, arbitrage, litigation and crisis management for international tech companies or companies aiming at transforming their economical models through tech and data.
The moto of Sublimis is “we walk the right line with you”, because Sublimis is positioned at the center of a magic square between law firms that provide with legal advisory and consultancy firms that addresses the technical dimension, regulators that provides with obligations increasing in terms of complexity, and a wide range of customers from startup to big corporates. Among this, Sublimis aims at helping their customer identifying the red lines to not cross that can expose their business and brand but find in a creative manner the right line for them.

Amal MARC, Founder of Sublimis and independent advisor has 20 years track records in different position that permits to address tech companies’ issues and challenges in a pragmatic solution-oriented approach.
She is both a senior lawyer and an experienced engineer with sales experience. She can then communicate with the business, with lawyer and go deep in the technicalities of market solutions and foster innovative approach for new models to penetrate the market while complying with increasing number of regulatory constraints.

Among her major main experiences:

SAFRAN Morpho

2008 – 2011: Amal MARC has started her carrier working for the world leader in biometrics (solution provider for FBI, and governments across the world) within the EU Programs department, that needed to capture EU fundings to fuel the R&D activities through human rights and regulatory impact analysis (to be delivered in exchange of the fundings). Amal MARC joined the team to create an Ethics & Research center of competence that offered impact analysis of all new tech projects like iris on the fly identification, contactless fingerprint collection in crime scenes, real time face recognition identification from videosurveillance or image processing for criminal investigation, trusted traveler programs, abnormal behavior detections etc.

This role involved collaboration with an ecosystem of strategic partners and stakeholders (European commission, Europol, etc.) and competitors.

2011- 2012: Amal MARC joined the CIO department of the largest energy company in France that had a database of 30M customers that was facing lots of investigations and penalty risks from the French data protection agency (CNIL). She was involved in a 1year global diagnosis activity that permit to reset the internal compliance process and address compliance of the first smart grids and big data projects.

2012 – 2014: Amal MARC joined the CNIL, the French Data Protection and Data Privacy Authority, as a senior legal counsel with the international legal affairs department. She was in charge of counselling companies to comply with data privacy regulations and contributed to the upcoming GDPR.

2014 – 2016: Amal MARC joined Sogeti, which is the cybersecurity subsidiary of Capgemini group. She spent two years working for major private and public companies as a senior cybersecurity consultant. She was invited to support Capgemini group executive board to design the first ever global data privacy and data protection program. She designed the program (Binding Corporate Rules) covering 40 countries (100 legal entities) and got it approved by the CNIL and the 27 other EU Data protection authorities in less than 4 months, end to end.

2017 – to 2021: Amal joined Capgemini group and had several hats - she implemented the BCR program from the group in EU (including Morocco and Vietnam) and was in charge of IT contracts/MSA negotiation, played a role of Cybersecurity officer in charge of various large security incidents, screening more than 1000 engagements and acting as an internal and external advisor to support CEOs in identifying compliance and technical risks in the most critical projects (move to cloud, design platforms, blockchain, and AI).

She supported across the years multiple customers from the financial services sector, telco, retails, defense, life science incl pharma chemicals etc. The 2 last year, Amal took over a role of global account executive in charge of the second largest business services account (close to 30M -1000 FTEs) and was in charge of delivery in 9 geographies (India, China, Latam) and dealing with global and local partnerships (Azure, AWS, Mulesoft, Snow, etc.).

After Covid she launched her activity and is now advising CEOS from different industries on how to align cybersecurity threats, digital compliance increased pressure, sustainability goals while growing profitable and ethical business.

Amal MARC invited to this third-party review a senior independent consultant Anthony COQUER who is a French white hacker, cybersecurity SME who worked for 15 years in critical industries both for end customers and law firms as a tech SME. He helped deepening the product tech review.

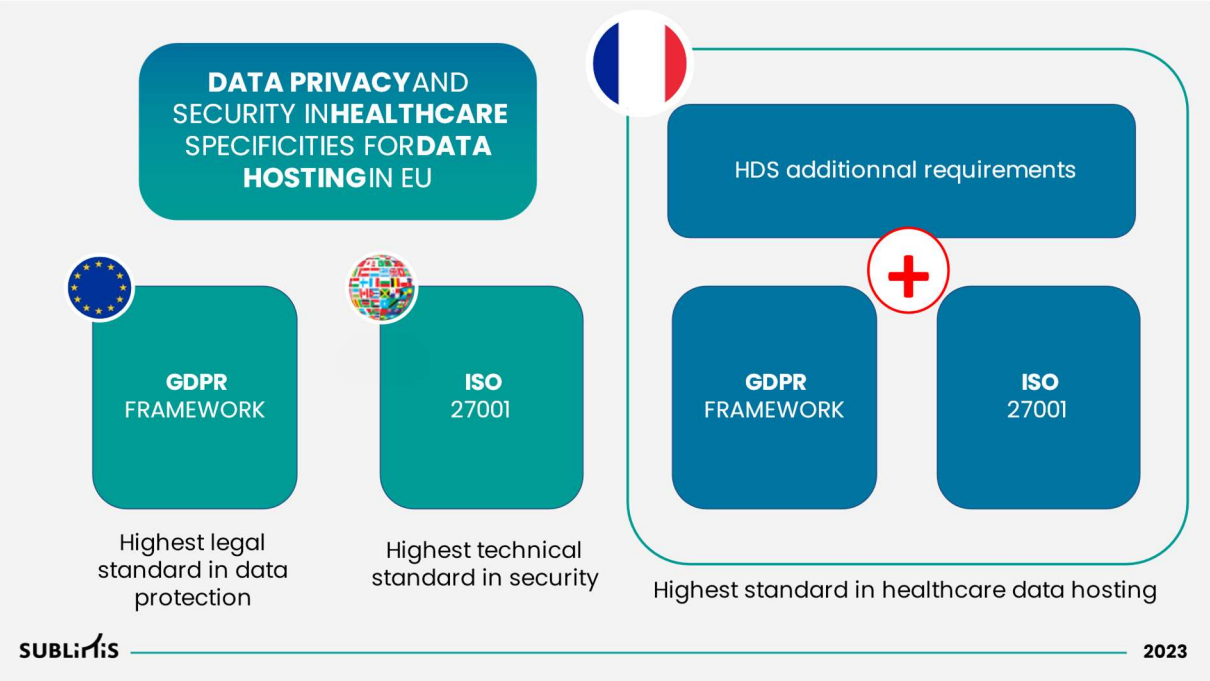
3. Summary of the methodology used for the third-party review.

To provide with independent review of the opportunity of using XQ as an embedded feature in AWS hosting or cloud services, we wanted to initially de-risk the XQ model with regards to the company's own compliance to EU privacy and security standards.

3.1. Presentation of the standards used for the review.

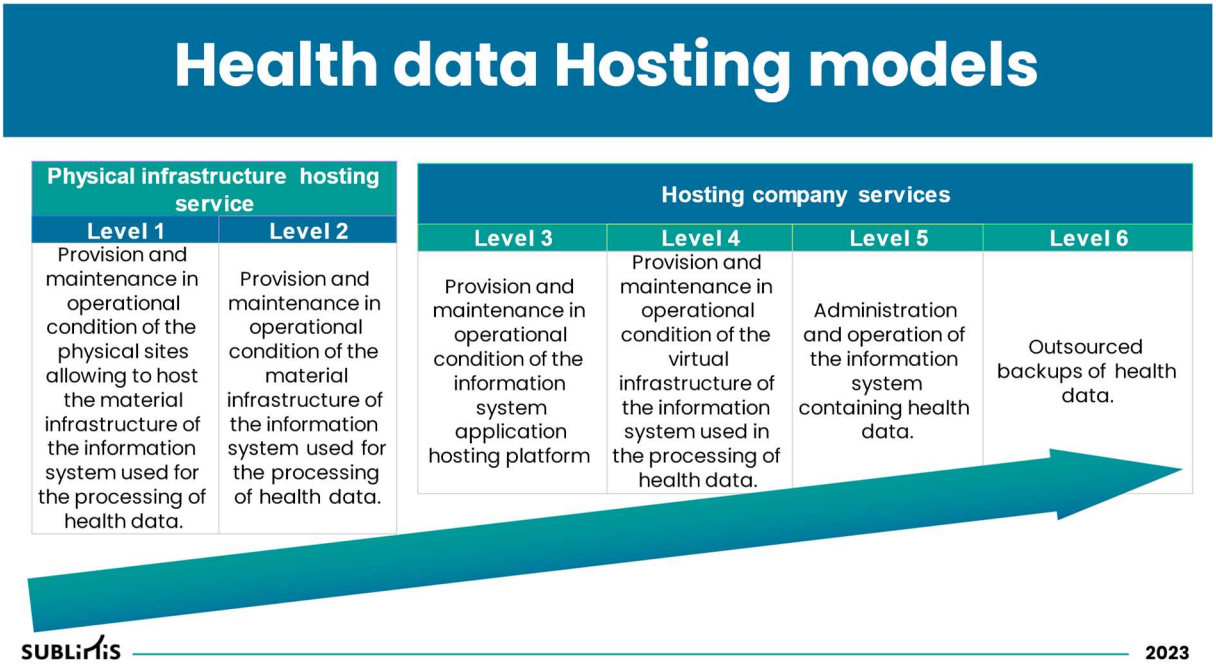
We proceeded to the review of the applicable compliance and security framework to perform an audit. We selected:

- All applicable articles of the GDPR to address EU privacy and data protection standards, GDPR being an EU data privacy framework, but also a reference as the highest standard in data privacy in the world.
- ISO 27001 being the highest data protection and worldly accepted security standard.
- The HDS framework for health data hosting which is a French local regulation but again being identified as one of the highest standards in health sector in the EU.



While GDPR and ISO 27001 are well known framework we propose to break down the HDS framework. It is composed of ISO27001 framework, GDPR provisions and add specific healthcare provisions.

With regards to what HDS covers, it offers multiple options to certify different health data hosting models.



3.2. AWS compliance framework

3.2.1. AWS GDPR and data protection Program

Over the last years, AWS has invested massively in GDPR compliance, both from a "paper based" approach and in investigating the best-in-class techs to covers their compliance as a company, as a provider offering solutions to EU citizens, and as a company innovating in offering solutions their customers facing regulatory issues.
More information to be found in AWS website
https://aws.amazon.com/fr/compliance/gdpr-center/

3.2.2. AWS HDS Certification

AWS collaborated with an independent third-party audit firm to reinforce the security and protection of personal health data of French citizens.

HDS certification shows that AWS should guarantees data confidentiality, integrity and availability to its customers and partners for data hosting.

What geographies does AWS HDS certification covers:

- Asia Pacific (Jakarta), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Milan), Europe (Paris), Europe (Stockholm), Europe (Zurich), Middle East (UAE), South America (Sao Paulo), USA East (Northern Virginia), USA East (Ohio), USA West (Northern California), and USA West (Oregon).

What are the health data hosting activities covered by AWS:

A "physical infrastructure hosting" certificate for activities involving the provision of physical hosting premises and hardware infrastructure.

1) Provision and maintenance in operational condition of physical sites for hosting the physical infrastructure of the information system used to process health data.

2) Provision and maintenance in operational condition of the physical infrastructure of the information system used to process healthcare data.

A "managed hosting provider" certificate for virtual infrastructure provisioning, software platform provisioning, administration/operation and outsourced backup.

3) Provision and maintenance in operational condition of the information system's application hosting platform

4) Provision and maintenance of the virtual infrastructure of the information system used to process healthcare data

5) Administration and operation of the health data information system

6) Backup of health data

More information available in AWS website https://aws.amazon.com/fr/compliance/hds/

3.2.3. AWS pending challenges.

AWS activities are submitted to the US Cloud Act and Patriot Act even with and HDS certification.

AWS activities are submitted to the US Cloud Act and Patriot Act which is raising increased concerned towards customers that want to embark in the data sovereignty journey, and the same applies to EU Data Protection Authorities that expressed increased concerns towards the current cross data transfers between US and EU considered as not relevant and not anymore respectful of EU citizens rights, and secrecy affairs of EU companies, especially the most sensitive ones.

AWS HDS model is covering only AWS and customers still have to take appropriate steps to address their own compliance.

Jurisdictional precedent of German state banning the use of an hyperscaler's solution across German public sector

Microsoft is currently going through a complex jurisdictional process with German court and German data protection authorities because of the use of office365 considered as not offering the appropriate level of data privacy and data security for German citizens.
This is not specific to Microsoft and could apply the same to AWS cloud services.

Amazon huge fines for not complying with GDPR.

In 2021, Luxembourg Data protection authority issued a €746 Million GDPR Fine to Amazon for not complying with the regulation based on 10 000 cases filled EU citizens.
Despite the data not being breached or exposed as defended by Amazon, the damage to the brand was made and, through a contagious mechanism, was questioning AWS compliance, despite being two separate companies with two different operating models.

In conclusion, while being well equipped, and being among the most mature companies in the market, complying with GDPR, ISO and obtaining an HDS certification, AWS models are still exposed to the weaknesses of EU-US data flows mechanisms, and still must be submitted to the US Cloud and Patriot Act.

3.3. XQ Compliance model

XQ is a US company as well, that seems to face the same challenges as AWS.
However, we wanted to take XQ through de-risking the company operating model until complying with GDPR and ISO and then question the HDS certification.

3.3.1. XQ's approach to address privacy and security compliance

After having spent time discussing about XQ customers, we see a significant untapped opportunity to address a new approach to GDPR compliance. Instead of having to combine layers of manual reports that do not cover shadow IT, nor shadow processing, the risks of gaps between what is processed by legal departments and what is being screened by security teams, needs to offer a single path for effective data privacy compliance.

So far, market practices tend to align with paper-based frameworks. This has shown significant limits with Privacy shields, Schrems I and II precedents and more recently the legality of EU-US data transfer mechanisms being questioned again.

So, if contracts, legal clause cannot be sufficient to offer the right level of protection, we do believe that the right combination of doctrine, governance, tech can solve the issue.

This being said, as a US company XQ teams are very much conscious of the challenges that can raise the use of a US-headquartered software company, to address the EU privacy market. This is why, having this in mind we have worked on an innovative combination of the best security tech in the market and a liability model that keeps XQ customers data away from XQ's hands.
XQ value proposal is based on applying Zero Trust fundamentals to address GDPR compliance. Zero Trust protects client protects personal data by verifying the identity of the endpoint user, employing constant verification and crypto-agile, quantum-resistant encryption along with real-time logging and notifications while never having the client data, nor the access to personal data.

XQ is the first company to extend the Zero Trust Architecture for data protection. XQ encrypted data is wrapped with meta-tags that resolve to a Policy Control Point where identity and authorization records are kept. XQ ensures that stolen data cannot be read as a hacker would not have the correct identity nor authorization or they are in the wrong geo-location.

With this approach XQ can protect data everywhere, while never having access to it.

Why is XQ's approach different from the existing solutions available on the market?

Over the last years, customers have seen a lot of privacy solutions emerged on the market. They faced a lot of disappointment, especially towards the ones that required heavy complex manual set-up, with low adhesion from users to feed the tools. Security solutions had a similar success, so highly dependent on continuous use and update.
We see that the market is only at the beginning of a new area where security, governance and compliance tools can be merged to address the protection challenge at the data level.

XQ is addressing the challenge of protecting data no matter where it goes anywhere in the world by providing data-centric protection and state-of-the-art Zero Trust technology to prevent unauthorized access.

XQ never hold customers data. XQ only handles policy-based key distribution, wrapping the data in metatags and policies and generating and managing keys via a backend key cache. Even if a data breach occurs, no one would be able to access our customer personal data because they cannot not.

The XQ backend only forwards key and never touches the data nor knows anything about the edge devices except identity and authorization. Every customer has their own XQ key cache which can be cloud hosted or running on a physical server.

By being connected to the data, XQ model offers to their customers a holistic view into their data and control the policies for who, where, and when it is accessed. The system is then automatically fueled with real-time information on data flow, data access, data breach which close the gap left by the traditional manual data governance tools, as well as the uncertainty left by use of multiple solutions that do not offer comprehensive visibility on data journeys.

Finally, XQ model has been built to achieve safe, effective, scalable and cost-efficient data privacy and protection, while today, even the most expensive programs/tools do not prevent customers from data loss, reputational damage and financial penalties.

3.3.2. Our approach to review XQ GRPR compliance, cybersecurity and HDS

Given the tight timelines provided to screen the whole XQ model we decided to wrap together GDPR and ISO27001 review together focusing on each standard. We descoped the specificities

of HDS health provisions (GDPR and ISO27001 being already covered), as 1. They are already covered and 2. The GDPR review conclusion shows that XQ do not process personal data.

Hence, with regards to the methodology we've been performing a 2 steps approach

- XQ as a company
- XQ products

XQ as a company compliance results.

The main result of this assessment reveals that while there were a lot of good practices in the way XQ operates as a company, because of that "ZERO TRUST" philosophy built in the company's DNA, there was still a need to enhance documentation in case of third-party audits.
As a company, XQ do not have access to their customers data.
However, to develop legitimate commercial relationships, and to deploy the XQ solutions, XQ might collect basic data for contractual and commercial/invoicing purposes.

Still, XQ kicked off both a GDPR and ISO27001 program to formalize an auditable internal framework, to lead by example and have in place what EU customers would require as best in class practices, documentations, and operating model.

XQ's will is to provide with transparency on its approach to data protection.

XQ products compliance results.

As XQ is offering solutions to critical organizations (health, defense, etc.), we decided to go through a deep tech review including architecture, API, cloud model, data life cycle.
This review's methodology is exploiting traditional ISO27001 standards, but we added our specific know-how on innovative models.
The result of the review shows that:

- The infrastructure has been designed including the right components to permit the creation of a robust system, the security measures for backups redundancy, segregation.
- The encryption model is aligned with the market best practices and highest standards recommendations.
- Small adjustments were advised to enhance the geo-fencing identification model proposed by XQ.
- The API model is aligned with market best practices.
- The cloud approach is as well aligned with market best practices.
- The native audit trail model permits real time tracking and auditability of the system activities (XQ side and same offered to customers on their side)
- Again, XQ has lots of native good practices but have to continue the formalization of the required auditable documentation.
- While the topic of access rights management is a key differentiator for XQ, XQ has to enhance the documentation of that specific point to describe their transparent model of access rights management.

With regards to the GDPR, XQ do not have access to their customers data.

However, the newness resides in the governance model that XQ has imagined valorizing this product and which is the key to unlocking the operational constraints described in the introduction.

In conclusion, XQ has invested in bringing their company model and products aligned to market expectations, taking into account both regulatory and technical obligations, while being a US resident company.

4. The AWS x XQ partnership opportunity validity

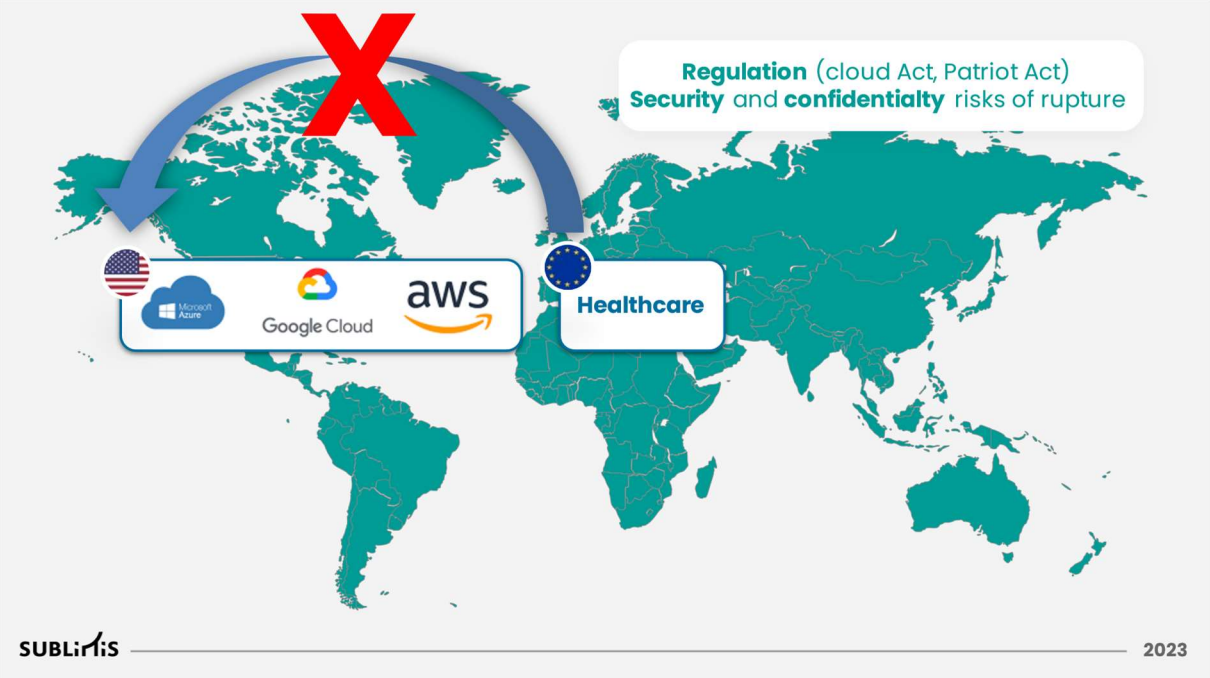
The purpose of this part will be to deep dive in the explanation of the business problem that the partnership AWS x XQ could solve and present different partnership configurations that could support, or not, achieving the goal.

4.1. AWS HDS EU-US data transfer challenges

As presented previously, the use of AWS services for healthcare customers might involve data transfers to the US.

The obtention of the HDS certification provides guarantees that the healthcare customers data are hosted respecting the highest standards in the market.
However, this is not solving the issue of having AWS systems and all data processing being submitting the Cloud and Patriot Acts.
Those regulations offer to the US government the possibility to have access to all data, whatever the location is, as long as the solution provider is headquartered in the US.

This is unfortunately weaking the strengths of AWS solutions and raising concerns of increasing numbers of customers in the EU.



To address those concerns and offer pragmatic solutions to data sovereignty (including data localization and data residency), AWS has invested massively in building local/regional data centers for countries to have an immediate response for onsite/local data processing.
Again, this doesn't work as long as the solution provider is an US headquartered company, the Cloud and Patriot acts applies.

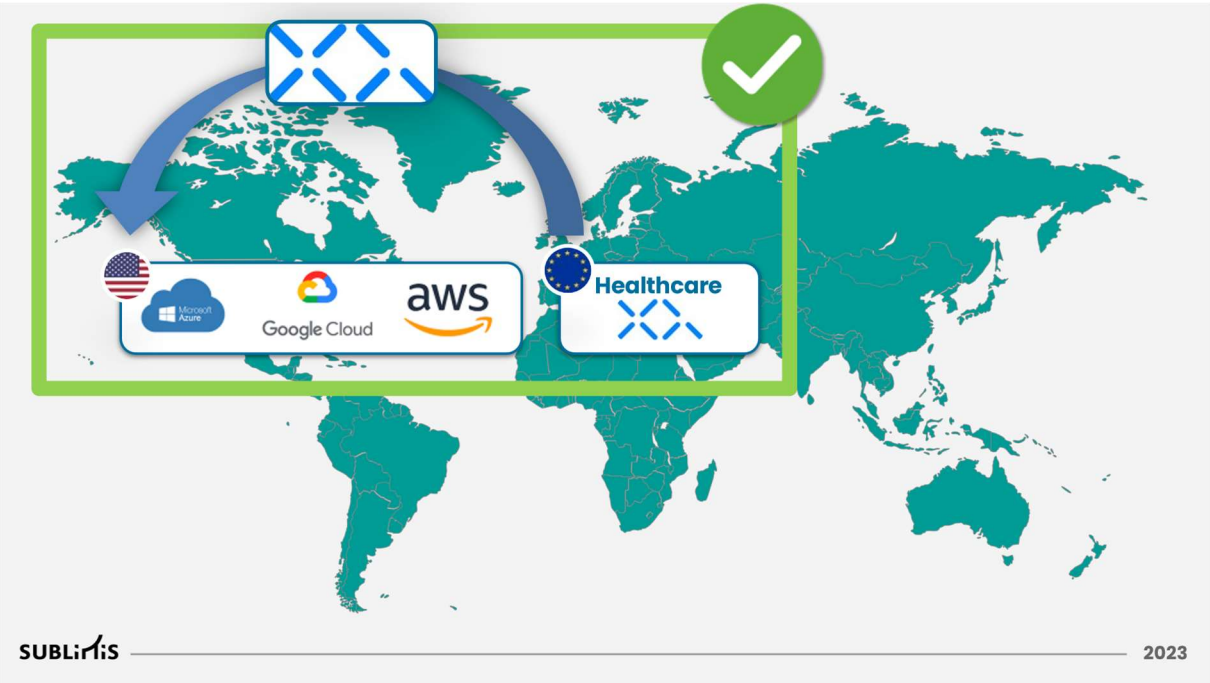
4.2. XQ's value proposal to data transfer protection

When using XQ solutions, the customers data are encrypted on customers side and then processed through cloud and HDS hosting services.

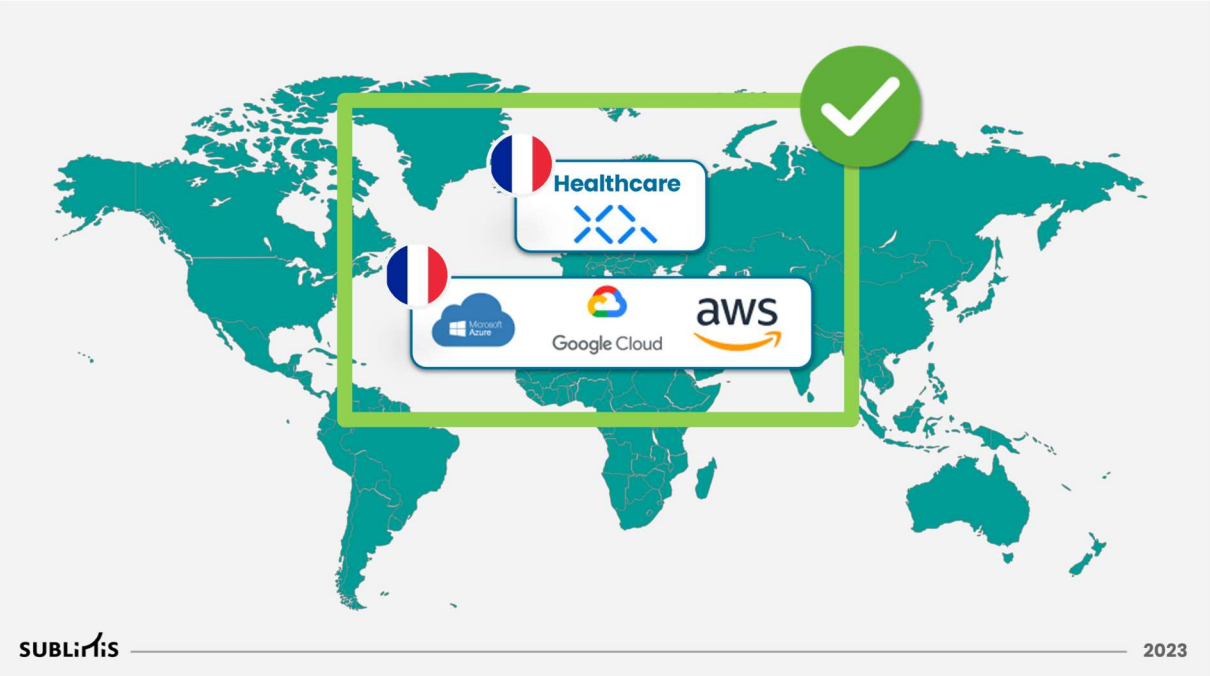
The XQ model permit to transfer the customer to remain owner of the encryption key generation, owner of their own data processing and owner of the will to use AWS products.

AWS never has access to customers data that are natively encrypted and the same applies to XQ.

In this model, even in the case of transferring the data to a US data center there is no application of the Cloud Act or Patriot Act: the data is encrypted and the encryption keys as well as the readable version of the data never touch XQ or AWS systems.
There is equally no application of the GDPR as the data are encrypted.



In the case where, the customer wants the exact same model as previously described and wants on top to benefits from local servers, the same solution applies.



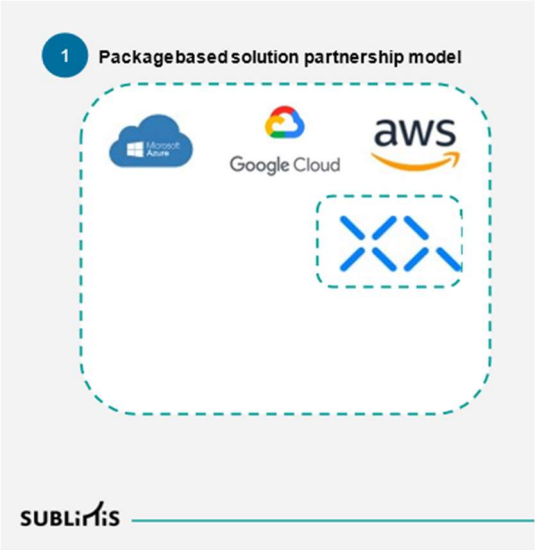
4.3. AWS x XQ winning partnership models.

To assess what could be a wining option of partnership we have analyzed 3 different models.

4.3.1. A package-based solution partnership model

In order for AWS to scale easily XQ solutions, we initially wanted to propose a package-based solution model.
In this case, XQ crypto-agile model become a native feature embedded in AWS solutions.
Regarding the commercial and legal model, XQ become a white label product, sold, and scaled by AWS.
From both legal and contractual standpoints, AWS remains solely responsible in front of their customers. XQ settings are packed and decided by AWS. XQ become a solution provider for AWS.

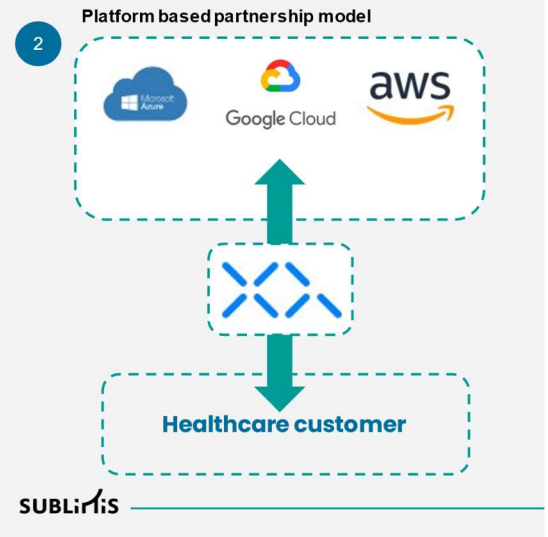
I would have been easy to scale by having XQ operating under the leadership of AWS, XQ become by “contagious mechanism” an AWS product and is as such submitted to the Patriot Act and cloud act.



4.3.1.1. A platform-based partnership model

In this configuration, XQ becomes a central platform that could connect and/or bridge AWS systems and customers systems.
XQ then act as an independent stakeholder from a technical standpoint.
From a commercial and legal standpoint, this model would require additional legal and commercial engineering:

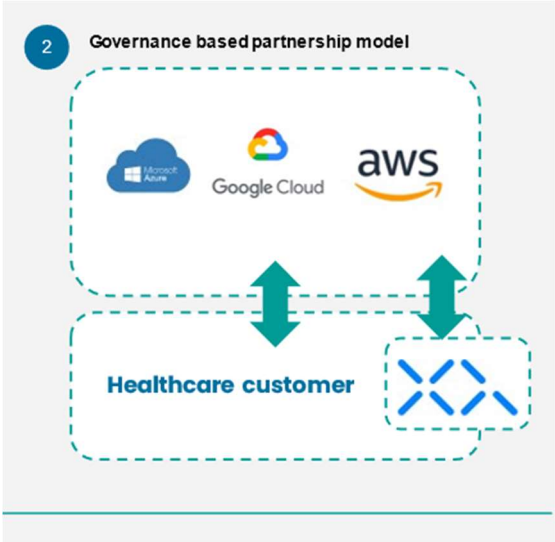
- There would need to set up a contractual triangle between XQ, AWS and a customer.
- This would involve a detailed description of roles and responsibilities, as well as a very precise liability matrix.
- From a commercial standpoint there will need to be agreements between AWS and XQ and customer and AWS and customer and XQ which would make the conversation a bit complex and create a heavy administrative process.
- The applicability of the US Patriot and Cloud Acts is a bit uncertain in this configuration.



4.3.2. A governance base model

The last model that we analyzed seemed to be the most relevant.
In this model, we see different levels of relationships:

- To pipeline customers opportunity, AWS and XQ could develop a commercial partnership, this means agreeing on jointly addressing customers, and find a reward or gain share model based on % of sales or volumes. It could also present the benefits of the collaboration, being clear on the fact that XQ is not acting under the instruction of AWS.
- However, from a legal and contractual standpoint, XQ sell their solutions directly to the customer and remains solely responsible for their products in front of the customers.
- The customer remains unique owner of the encryption key generation. The whole model escapes from the application of the Cloud act and Patriot Act wherever the data centers are based.



5. Conclusion

After an in-depth screening of XQ organizational model and solutions, we do see a real opportunity in addressing jointly with AWS the EU market which is currently suffering from a lack of solution to address the EU-US cross border data flows, data sovereignty as well as data security in a context of global geopolitical, economical and regulatory pressures.

We found at the XQ proposition is really innovative:

- As a soft provider XQ never have access to the data
- We proposed a model that will not be submitted to Patriot Act/cloud act as the encryption key pertain to EU customers.
- This becomes contagious to AWS because AWS do not access the data either nor the encryption keys.
- Data is being protected at the data level.
- Revokation mechanisms can apply
- Cybersecurity at data level is guaranteed, even if lost, the data can never be read or used.

Finally, the economic benefit is measurable:

- The partnership can be scalable and cost-efficient event if processing huge volumes of data.
- The solution is a « Plug and play » tool so very easy to implement, it is as well security environment agnostic/compatible –with no rupture in terms of security.

ANNEXURE

Sublimis by THE DIGITAL RED LINE SERVICES
3 parvis Pierre de Coubertin
92600 Asnières-sur-Seine
Amal.marc@sublimis.io
00 33 6 03 02 98 33

Brian WANE - CEO
XQ Message Inc
5416 Lawton Ave
CA
94618 OAKLAND
United States

Paris, 21st September 2023

ATTESTATION OF COMMITMENT TO EU PRIVACY & SECURITY COMPLIANCE

I, Amal MARC, CEO and Independent Advisor of Sublimis by THE DIGITAL RED LINE SERVICES a French niche boutique specialized in independent advisory for tech startups, scale-ups and innovative enterprise, in digital compliance, cybersecurity and sustainable business models, testify by the present letter that XQ Message incorporation a US headquartered startup specialized in Zero Trust Data Protection, is committed to EU privacy and security compliance.

XQ Message has submitted the entire organization to a comprehensive third-party audit that involves a deep screening of the operating, organizational, technical and legal model as well as a strong technical audit of their solutions that covers infrastructure review and cybersecurity tests.

The standards used for this audit were the GDPR framework as well as ISO27001. We also supported with best practices recommendations, to tailor, best in classes practices to a smaller organization like XQ, based on 20 years of experience working with startups worldwide.

As a result, we can testify that XQ Message, through its CEO Brian WANE and his team, is demonstrating solid grounds for GDPR compliance and EU security standards, for both the organization and the products, with a strong continuous improvement plan that will need to be followed regularly to maintain highest level of guarantees for their customers, partners and public bodies.

10/10/2023

DocuSigned by:
Amal MARC
1F5ECF1017534E4...