



SOVEREIGNTY & COMPLIANCE

Sensitive data in the cloud compliance and sovereign encryption

Understand what HDS, SecNumCloud and the forthcoming EUCS scheme actually cover, measure your exposure to the Cloud Act and design an encryption architecture that holds up in front of an auditor. A practical guide for teams hosting health, financial or strategic data in the cloud.

11 pages · Regulatory analysis grid, framework comparison, encryption decision matrix and audit checklist included

6

hosting activities covered by HDS
certification

3

assurance levels planned under the
European EUCS scheme

72h

deadline to notify a data breach to the
CNIL

CONTENTS

What you will find in this document

This document starts from the European regulatory context and works down to concrete architecture choices — certifications, transfer models, key management — and closes with an actionable compliance roadmap.

01	Executive summary — the essentials on one page	p.3
02	A Regulatory Landscape Under Strain	p.4
03	HDS Certification: The Real Scope	p.5
04	HDS, SecNumCloud, EUCS: Comparison	p.6
05	Cloud Act and GDPR Transfers	p.7
06	BYOK and HYOK Encryption Architecture	p.8
07	Self-assessment grid	p.9
08	A 5-step roadmap	p.10
09	Conclusion & about Move2Cloud	p.11

Who is this document for? CTOs, CISOs, DPOs, cloud architects and platform leads in mid-caps, large enterprises and SaaS vendors handling health data, sensitive personal data or strategic assets — particularly those engaged in a migration or in bringing an IT system already hosted with a hyperscaler into compliance.

EXECUTIVE SUMMARY

The essentials on one page

Hosting sensitive data in the cloud is no longer a matter of choosing a provider, but of a key architecture you must be able to demonstrate.

Health, financial and strategic data are migrating to the cloud faster than the frameworks meant to govern them. The HDS framework covers **6 distinct hosting activities** and, since its **2024** revision, requires storage and processing to be located within the European Union; ANSSI's SecNumCloud **3.2** framework adds ownership and legal criteria; the European EUCS scheme, which provides for **3 assurance levels**, has still not been adopted.

Pressure no longer comes solely from supervisory authorities but from contracts. DORA has applied to the financial sector since **January 2025** and requires a register of critical ICT providers and exit clauses; NIS2 extends equivalent obligations to thousands of entities; and since the Schrems II ruling, any transfer outside the EU requires a documented impact assessment, including under the Data Privacy Framework. Large corporate clients and public tenders now reproduce these requirements in technical annexes, long before any regulator steps in.

The good news is that compliance depends less on the provider's flag than on control of the keys and the segmentation of processing. BYOK, HYOK, externalised HSM, confidential computing and application-level encryption make it possible to keep workloads on a hyperscaler while rendering the data unusable without a key that remains under European control. This document provides the criteria to decide which data falls under which model, and how to document that choice.

6

hosting activities covered by the HDS framework

3

assurance levels provided for by the EUCS scheme (Basic, Substantial, High)

72h

GDPR deadline for notifying a data breach to the CNIL

The question this document addresses is not "which cloud is sovereign?" but "which data, under which keys, accessible by whom, and how do you prove it to an auditor?". The following sections offer a classification method, a Cloud Act exposure grid, three encryption architecture patterns and a compliance checklist applicable to an already hosted information system.

SECTION 02

A Regulatory Landscape Under Strain

Between a revised HDS framework, an EUCS scheme still unfinished and intact US extraterritoriality, teams must decide today on architectures that will be audited tomorrow. Three dynamics explain why the subject can no longer be handled at the end of a project.

1. 1. The HDS framework has tightened

The 2024 revision of the HDS framework requires health data storage and processing to be located within the European Union, as well as transparency on any access requested by a third-country authority. Existing certificates must be realigned at the next audit cycle.

2. 2. EUCS: sovereignty deferred

Launched by ENISA in 2020, the EUCS scheme provides for three assurance levels (Basic, Substantial, High) but remains a draft, as the immunity requirements against extraterritorial laws were removed from the mandatory core. No EUCS certificate can be issued today.

3. 3. The Cloud Act did not disappear with the DPF

The 2018 Cloud Act allows US authorities to require data held by a provider subject to United States law, regardless of the country of storage. The 2023 Data Privacy Framework legalises the transfer within the meaning of the GDPR but does not neutralise that access.

“ Compliance is not demonstrated with a certification logo, but with a map of the keys and of those who can read them. ”

The following sections detail what each framework actually covers, how to measure the legal exposure of a workload and which encryption architectures stand up to scrutiny.

SECTION 03

HDS Certification: The Real Scope

HDS certification, derived from article L.1111-8 of the French public health code, replaced the former approval scheme in 2018: it is built on an ISO 27001 foundation, supplemented by requirements inspired by ISO 20000-1 and ISO 27018 and by obligations specific to the healthcare sector.

POINT OF ATTENTION	WHAT IT MEANS IN PRACTICE
Scope of services	Certification does not cover a provider's entire catalogue: only the services listed in the appendix to the certificate are eligible, and a recently released managed service rarely appears there as soon as it comes to market.
Six distinct activities	Activities 1 and 2 concern physical sites and infrastructure, activities 3 to 6 virtualisation, the application platform, administration and backup: an infrastructure hosting provider does not carry the responsibilities of the managed service provider.
Subcontracting chain	Every link that has technical access to health data must be covered; a software vendor deploying on a certified IaaS remains responsible for its own operational activities and must be certified accordingly.

Key takeaway: Always ask for the HDS certificate itself, not the logo: check the accredited certification body, the numbers of the activities covered and the appendix listing the certified services. If your SaaS vendor operates the platform, it must hold its own certification for activities 4 to 6 — its IaaS provider's certificate does not cover it.

What HDS certification does not say

The current framework governs the hosting provider's practices: security governance, access management, traceability, backup, reversibility, appointment of a data protection officer and patient information. It does not, however, require either encryption of data at rest under a key controlled by the customer or, in its current version, exclusive localisation within the European Union or immunity from extraterritorial laws. In other words, an HDS-certified hosting provider may be a European subsidiary of a group subject to US law: the certification attests to process maturity, not legal watertightness. It is precisely this gap that the work to overhaul the framework, led by the Agence du numérique en santé, seeks to fill by introducing localisation criteria and protection against third-country access. As long as this new version is not enforceable, legal exposure must be addressed elsewhere: in the transfer impact assessment and in the key architecture.

SECTION 04

HDS, SecNumCloud, EUCS: Comparison

HDS, SecNumCloud and EUCS do not answer the same question: the first governs a sector, the second qualifies a level of trust that includes legal criteria, the third aims to harmonise the cybersecurity assessment of cloud services across Europe.

FRAMEWORK	STATUS	WHAT IT GUARANTEES	BEST SUITED TO
HDS	Certification mandatory under French law	Maturity of the processes for hosting and operating personal health data, on an ISO 27001 foundation	Any workload hosting or processing health data on behalf of a data controller
SecNumCloud	ANSSI qualification, voluntary	Reinforced technical and organisational requirements, combined with criteria of immunity from non-European laws (localisation, ownership, governance)	Strategic data, information systems of vital importance, industrial secrets and government needs
EUCS	European scheme under development under the Cybersecurity Act	Graduated assurance levels and mutual recognition between Member States, intended to replace national schemes	Anticipating the compliance trajectory: to be mapped today, not to be required contractually

Common pitfall: Confusing a "trusted cloud" with an actual qualification: an offering operated in France under licence of a US technology is not qualified until ANSSI has issued the attestation, and no certification, HDS included, exempts you from carrying out the transfer impact assessment required by Chapter V of the GDPR.

Combining frameworks without stacking costs

Stacking frameworks is expensive and delays releases into production. The effective approach is to segment: identify the workloads genuinely concerned by each obligation, then size the level of requirement accordingly. A healthcare platform can perfectly well combine an HDS foundation for production environments processing patient data, a non-qualified public cloud for development environments fed with anonymised data sets, and a SecNumCloud enclave reserved for the most sensitive processing or for operational secrets. This segmentation presupposes a formal data classification and explicitly controlled cross-zone flows — failing which the least demanding zone ends up receiving, through copies or logs, the very data that was supposed to be isolated.

SECTION 05

Cloud Act and GDPR Transfers

The 2018 CLOUD Act requires any provider subject to US jurisdiction to hand over to the authorities data in its "possession, custody or control", whatever the country where that data is physically stored.

The decisive criterion: control, not geography

It is not the location of the datacentre that determines exposure, but the control relationship between the entity served with the request and the data. A European subsidiary owned by a US parent company remains in scope as soon as it can technically access the data in the clear.

Transfer is not limited to storage

Under the GDPR, remote access from a third country already constitutes a transfer. Level 3 support, administrator on-call duty, product telemetry, operational logs and billing metadata are all flows to be inventoried in the same way as the database itself.

Supplementary measures that genuinely hold up

Since Schrems II, the European Data Protection Board's recommendations identify robust encryption, with keys held and administered exclusively within the EU by an entity beyond the reach of third-country law, as the strongest supplementary measure — provided it is effective.

EXPOSURE VECTOR	MITIGATION MEASURE
Remote administrator access	Restrict operations to teams located in the EU, log and approve every access through a lockbox-type mechanism.
Telemetry, logs and backups	Disable optional reporting, keep logs within the region and encrypt backups with a key separate from the service's.

SECTION 06

BYOK and HYOK Encryption Architecture

Between encryption at rest enabled by default and exclusive control of the keys, there are three distinct models whose legal guarantees are very unequal.

BYOK: a governance control, not a cryptographic barrier

With BYOK, the key is generated by the customer then imported into the provider's hardware module. It is handled in the clear there during cryptographic operations: the control provided is essentially contractual and operational — traceability of calls, controlled rotation, revocation capability resulting in cryptographic destruction of the data. It does not constitute a barrier against a legal request targeting the provider, since the latter technically holds the key material. It is a good level of control for internal governance and the separation of environments, not an answer to extraterritorial risk.

HYOK and externalised keys: the real cost of watertightness

External key mechanisms — remote key store, key management service outside the cloud, client-side application-level encryption — keep the key material in an HSM that the provider does not administer; every operation triggers an outbound call. The cost is real: added latency on the critical path, strict dependency on the availability of the key broker, complexity of caches and recovery plans, and above all the loss of managed functions that require access in the clear (indexing, search, native analytics). Before generalising this model, you must test a deliberate shutdown of the broker and measure the time to return to normal.

Key takeaway: For each flow, document a single answer: who can decrypt, with which key and under which jurisdiction. It is this table, not the provider's certification level, that will hold up before an auditor or a supervisory authority.

The operational hierarchy is simple to set out. Provider-managed encryption at rest remains the default for the vast majority of workloads: it protects against media loss and physical theft. BYOK applies as soon as you need to prove the traceability of cryptographic operations and have a revocation lever. HYOK, an external key store or client-side application-level encryption are reserved for data whose reading by a third party would be unacceptable — and whose temporary unavailability is preferable to disclosure. Each of these choices must be recorded in the transfer impact assessment, along with the associated revocation and restoration tests: a key architecture that has never been tested is not a supplementary measure, it is an intention.

SECTION 07

Self-assessment grid

Review these six points before committing a new sensitive workload to the cloud, or ahead of your next HDS audit or CNIL inspection.

- ☐ **Do you have an up-to-date classification of the data you host, distinguishing personal health data, financial data and strategic data?** Without classification, no regulatory requirement can be tied to a specific processing activity and protection measures end up applied at random.
- ☐ **Have you obtained and read the HDS certificate of each of your providers, including the certification body, the activities covered and the annex listing the certified services?** The logo is not proof: only the certificate lets you verify that the services actually used fall within the scope.
- ☐ **Have you formalised a transfer impact assessment (TIA) documenting each provider's and sub-processor's exposure to an extraterritorial jurisdiction?** Chapter V of the GDPR requires it regardless of any certification, and it is the first document requested during an inspection.
- ☐ **Do you know, for each sensitive workload, who physically holds the encryption keys and where the cryptographic operations are executed?** Encryption whose keys remain under the provider's control offers no additional guarantee against a legal order.
- ☐ **Have you tested, under real conditions, the revocation of a key followed by the restoration of the associated service?** A BYOK or HYOK architecture that has never been tested is merely an intention and will not withstand an auditor's scrutiny.
- ☐ **Do you keep an up-to-date list of your providers' sub-processors, together with an exit plan costed in effort and lead time?** Real exposure often lies at the second tier of the chain, and a dependency with no exit path rules out any decision to leave.

How to read your answers: Two "no" answers call for a documented remediation plan; three or more signal a regulatory exposure to be addressed as a priority, before any new deployment.

SECTION 08

A 5-step roadmap

This trajectory is run in increments, without interrupting existing platforms: each step produces a deliverable that can be used immediately, even if the next one is postponed.

1

Map sensitive data

List your processing activities, their nature (health, financial, strategic), their legal basis and their criticality level. Map each dataset to the cloud services that store, process or back it up, including logs and test environments.

2

Verify actual certifications

Collect the HDS certificates, SecNumCloud attestations and audit reports of each provider, and compare the activities and services covered against your actual usage. Identify the uncovered areas, particularly among SaaS vendors operating the platform.

3

Run the transfer impact assessment

Document, for each provider and sub-processor, its jurisdictional attachment, the transfer mechanisms invoked and the supplementary technical and organisational measures. Conclude with a reasoned decision — maintain, reinforce or relocate — for each processing activity.

4

Design the key architecture

Apply the defined hierarchy: provider-managed encryption by default, BYOK as soon as traceability and revocation are required, HYOK or client-side encryption for data whose disclosure would be unacceptable. Formalise key governance, roles, rotation and separation of duties.

5

Test and govern

Organise revocation and restoration exercises, measure the impact on applications and record the results in the compliance file. Build these tests into the annual audit cycle and tie them to the exit plan of the provider concerned.

CONCLUSION

Demonstrable compliance rather than declarative sovereignty

Organisations that tackle these topics head-on gain more than a certificate: they gain the ability to document, to an auditor as much as to an investment committee, why a given dataset is hosted where it is, under what cryptographic control and with what exit lever. This traceability turns a diffuse risk into explicit decisions that can be weighed and revisited.

The regulatory landscape will keep moving — the ramp-up of EUCS, changes to the HDS framework, case law on transfers. The architectures that will survive these changes are not the most sovereign on paper, but the most explicit: delimited perimeters, keys controlled where it matters, known dependencies and tested reversibility. This is as much an engineering task as a compliance one, and it is better carried out upfront than in reaction to an inspection.

Move2Cloud	is a consulting firm specialised in infrastructure, cloud and IT transformation. We support organisations in the audit, compliance and security of their cloud environment.
Contact	Move2Cloud — Paris · move2cloud.fr
Next step	An audit of a few weeks is usually enough to turn the "no" answers from the previous grid into a costed remediation plan: mapping of sensitive data, review of certificates and contracts, transfer impact assessment and target key management design.

Sources

ANSSI — Référentiel SecNumCloud v3.2 (2022) — Ministère de la Santé / ANS — Référentiel de certification Hébergeur de Données de Santé — ENISA — European Cybersecurity Certification Scheme for Cloud Services (EUCS), draft scheme — CNIL — Doctrine and recommendations on data transfers outside the EU — EDPB — Recommendations 01/2020 on supplementary measures (post-Schrems II)

Document written by Move2Cloud as an example and illustration, for educational purposes. The EUCS scheme is still being adopted: its assurance levels and immunity requirements may change. This document does not constitute legal advice.