National Plan for Sovereign Cloud (PNNS)

A Modern, Sovereign and Efficient Infrastructure

Frequently Asked Questions

May 2026

REPÚBLICA PORTUGUESA

XXV GOVERNO CONSTITUCIONAL

Portuguese Republic — 25th Constitutional Government

Questions and Answers – National Plan for Sovereign Cloud (PNNS)

1. What is the National Plan for Sovereign Cloud (PNNS)?
2. What are the main objectives of the PNNS?
3. What is meant by "cloud"?
4. What does "digital sovereignty" mean?
5. What does "sovereign cloud" mean in the context of the State's digital transformation?
6. Does the PNNS imply the creation of a single State cloud?
7. Why has the Government decided to move forward with this plan now?
8. Who was involved in the definition of the PNNS?
9. Is the PNNS aligned with international practices? Which countries were considered as benchmarks?
10. How does the PNNS relate to the Programme of the XXV Constitutional Government and the Portugal Digital Strategy?
11. Who is responsible for the governance, oversight, and monitoring of the PNNS?
12. What impact will the PNNS have on citizens and businesses?
13. What is the PNNS's long-term vision for the national digital ecosystem and domestic cloud providers?
14. How is the PNNS structured?
15. What does Pillar I - Sovereign Digital Infrastructure include?
16. What is the role of the business process and data qualification model?
17. Which sovereignty levels are foreseen?
18. What requirements are associated with each sovereignty level?
19. What is the estimated distribution of data across sovereignty levels?
20. Who is responsible for designing and implementing the qualification methodology?
21. What is the role of Pillar II - Human Resources Capacity Building?
22. What does Pillar III – Legal Framework consist of?
23. What is the State's current expenditure on cloud services?
24. What is the State's current expenditure on data centres?
25. How will the PNNS be financed?
26. What savings does the Government expect from the implementation of the PNNS?
27. How does the PNNS contribute to environmental and energy efficiency objectives?
28. Will the State migrate all data centres to the cloud?
29. How does the PNNS relate to the National Data Centres Plan?
30. How will security and regulatory compliance (GDPR, NIS2, etc.) be ensured?
31. What is the overall implementation timeline for the PNNS?
32. In practical terms, what will Public Administration entities need to do?
33. How can entities verify whether they comply with the defined requirements?
34. What will be the timeline for the migration of entities?
35. What will be the cost of migration for entities?
36. Where will Portugal stand in 2030 following the implementation of the PNNS?

1. What is the National Plan for Sovereign Cloud (PNNS)?

The PNNS is the Portuguese Government's plan to equip the State with a modern digital infrastructure, built on cloud solutions that ensure sovereignty, security, and control over critical Public Administration data and systems. It stems from the Resolution of the Council of Ministers approving it as a central instrument for the technological transformation of the State.

2. What are the main objectives of the PNNS?

The PNNS pursues five core objectives: strengthening the State's digital sovereignty and security; increasing operational efficiency and reducing structural ICT costs; modernising public digital infrastructures; accelerating the digital transformation of public services; and positioning Portugal as a trusted hub for sovereign data and AI services.

3. What is meant by "Cloud"?

Cloud Computing is a model that enables convenient, on-demand network access to shared and configurable computing resources that can be rapidly provisioned and scaled with minimal management effort and provider interaction, ensuring flexibility, efficiency, elasticity, and cost optimisation.

4. What does "Digital Sovereignty" mean?

Digital Sovereignty refers to the ability of a country or region to control its digital infrastructures, data, and technologies, making autonomous decisions aligned with its strategic objectives, while ensuring economic competitiveness, security for citizens, reduced critical external dependencies, and greater technological resilience.

5. What does "Sovereign Cloud" mean in the context of the State's digital transformation?

Sovereign Cloud refers to a cloud computing model that ensures the State retains effective control over its critical data, systems, and infrastructures, in accordance with sovereignty, security, and resilience requirements. In practice, this means ensuring that data location, access, operations, technological governance, and critical dependencies remain under arrangements compatible with the national interest and the European legal framework.

6. Does the PNNS imply the creation of a single State cloud?

No. The PNNS does not envisage the creation of a single, centralised State cloud. Instead, it is based on a model composed of different digital infrastructure solutions, organised in an interoperable manner and tailored to the sovereignty levels required for each type of process, data set, and system. This model ensures flexibility, efficiency, and appropriate control, avoiding a one-size-fits-all approach.

7. Why has the Government decided to move forward with this plan now?

Portugal faces a combination of challenges, including fragmented infrastructures, ageing technological assets, growing cybersecurity threats, and strong dependence on non-European

providers. At the same time, digital transformation and Artificial Intelligence require a robust, energy-efficient, and sovereign technological foundation centred on data; otherwise, the State risks losing decision-making capacity and competitiveness.

8. Who was involved in the definition of the PNNS?

The PNNS was developed through an extensive consultation process coordinated by the State Technological Reform Agency (ARTE, I.P.), involving more than 100 public and private entities. More than 25 working sessions were held with cloud service providers, ICT sector associations, Public Administration entities across mainland Portugal, and representatives from critical sectors, ensuring a collaborative approach aligned with the real needs of the State's digital public services.

9. Is the PNNS aligned with international practices? Which countries were considered as benchmarks?

Yes. The PNNS is aligned with international Sovereign Cloud and digital sovereignty practices. Its design was informed by direct consultation and comparative analysis of 11 countries with different levels of maturity in this area.

Emphasis was placed on Germany, France, Italy, and the United Kingdom, which have more consolidated and structured approaches to Digital Sovereignty, as well as Estonia, recognised as a benchmark for public sector digital transformation. The analysis also included Spain, the Netherlands, Denmark, Ukraine, Israel, and Singapore, enabling a broad and comparative understanding of different national approaches and contexts.

The best practices identified were adapted to the Portuguese context and underpin the model defined under the PNNS.

10. How does the PNNS relate to the Programme of the XXV Constitutional Government and the Portugal Digital Strategy?

The PNNS operationalises the political priority established in the Programme of the XXV Government to position Portugal among Europe's most digitally advanced countries. It is integrated into the 2026–2027 Action Plan of the Portugal Digital Strategy, which includes measures related to cloud centralisation and rationalisation, data qualification, and the development of sovereign cloud capabilities.

11. Who is responsible for the governance, oversight, and monitoring of the PNNS?

Under the Government diploma establishing the new governance model for the State's digital transformation, the strategic coordination of the PNNS is embedded within the structure created to ensure integrated leadership of digital policies and public technological investment.

In this context, the *Rede de Simplificação e Tecnologias do Estado* is responsible for the cross-governmental monitoring and coordination of the plan's measures, promoting cooperation between public entities and the coordinated implementation of strategic initiatives.

In addition, the National Cybersecurity Centre (CNCS) and ARTE, I.P. hold technical responsibilities regarding the definition of reference frameworks, as well as the qualification and accreditation of solutions, in coordination with sectoral authorities and operational entities.

12. What impact will the PNNS have on citizens and businesses?

The PNNS will enable simpler and better integrated digital public services, with higher availability, fewer failures, faster response times, and greater trust in data protection.

By modernising the State's technological infrastructure and reducing fragmentation, the plan will free up resources currently devoted to maintaining dispersed systems, redirecting them towards innovation and the continuous improvement of public services. For citizens and businesses, this will result in a more agile, efficient, and responsive Public Administration.

13. What is the PNNS's long-term vision for the national digital ecosystem and domestic cloud providers?

In the future, both market-based cloud solutions and solutions provided directly by Public Administration may be accredited, provided they comply with the requirements to be defined.

This approach promotes an open and competitive ecosystem, fostering the development of the national cloud market, strengthening technological autonomy, and creating opportunities for the growth of digital capabilities in Portugal.

14. How is the PNNS structured?

The plan is organised around three pillars of action:
(I) Sovereign Digital Infrastructure;
(II) Human Resources Capacity Building; and
(III) Legal Framework.

Each pillar comprises a set of concrete initiatives with clearly defined objectives, responsibilities, and timelines.

15. What does Pillar I – Sovereign Digital Infrastructure include?

Pillar I includes: a uniform qualification model for business processes and their associated data and systems, the development of a national sovereign cloud offering, including AI capabilities, a phased adoption plan for Public Administration, the creation of a unified cloud services catalogue, and improved procurement mechanisms for cloud services.

16. What is the role of the business process and data qualification model?

The qualification model is the core pillar of the sovereignty strategy. It enables Public Administration processes and data to be assessed according to their impact on citizens, State stability, and information exposure.

Based on this assessment, a sovereignty level (0 to 3) is assigned, determining the minimum security, resilience, and control requirements applicable to the infrastructures and cloud services used.

17. Which sovereignty levels are foreseen?

There are four categories:

- Neutral (Level 0, with no specific sovereignty requirements);
- Standard (Level 1, baseline requirements);
- Critical (Level 2, enhanced operational and data sovereignty requirements); and
- Strategic (Levels 3.a and 3.b, with maximum sovereignty requirements, including software sovereignty and, where justified, nationally scoped software sovereignty).

18. What requirements are associated with each level?

Sovereignty and security requirements vary according to the qualification level assigned to each process, increasing progressively in stringency as sovereignty levels rise.

Broadly, these requirements include aspects such as data localisation and jurisdictional control, encryption, identity and access management, network and operational security, regulatory compliance, as well as interoperability, portability, and control over software and infrastructures.

19. What is the estimated distribution of data across sovereignty levels?

Based on international experience, it is estimated that most Public Administration data will fall within the lower sovereignty levels:

- approximately 70% at the Neutral level (Level 0);
- 20% at the Standard level (Level 1);
- around 7.5% at the Critical level (Level 2); and
- approximately 2.5% expected to be qualified as Strategic (Levels 3.a and 3.b), requiring the highest standards of sovereignty, security, and control.

These percentages are indicative and intended to illustrate the logic of the model. The actual distribution will be determined through the qualification process.

20. Who is responsible for designing and implementing the qualification methodology?

The methodology is developed by the National Cybersecurity Centre (CNCS) and ARTE, I.P., which are responsible for defining the scoring methodology, producing a pre-qualification framework based on the Public Administration process catalogue, and establishing the sovereignty and security requirements associated with each level.

21. What is the role of Pillar II – Human Resources Capacity Building?

Pillar II addresses the shortage of technological skills within Public Administration. It includes a dedicated competency framework for sovereign cloud, training programmes for technical staff and senior officials, internships, and digital sovereignty capacity-building initiatives, with clear targets regarding the proportion of trained specialists and the number of qualified public sector leaders by 2030.

22. What does Pillar III – Legal Framework consist of?

Pillar III focuses on removing legal and financial barriers to cloud adoption. It simplifies the procurement of cloud services, aligns the Public Procurement Code with the requirements of centralisation and scale, and clarifies the accounting treatment and eligibility of sovereign cloud and sovereign AI services for public and European funding.

23. What is the State's current expenditure on cloud services?

There is not yet a comprehensive view of public expenditure on cloud services across the entire Public Administration. However, based on the Public Administration Cloud Adoption Report 2025 conducted by ARTE, I.P., annual expenditure across 262 central and local Public Administration entities was estimated at approximately €35 million.

24. What is the State's current expenditure on data centres?

Based on the available budgetary information, the State's annual expenditure on digital infrastructure components is currently estimated at approximately €70 million. This figure corresponds to estimated ICT infrastructure-related costs, excluding energy, facilities, human resources, software, and cloud operational costs.

In addition, the energy component alone of Public Administration data centres is estimated at approximately €6 million per year, highlighting the efficiency gains associated with the modernisation and consolidation of these infrastructures. These figures are indicative and exclude extraordinary investments financed through the Recovery and Resilience Plan (RRP).

25. How will the PNNS be financed?

The estimated overall investment amounts to approximately €217 million over the 2026–2030 period, combining State Budget resources and private-sector investment. Approximately €117 million is expected to be financed through the State Budget, covering infrastructure, cloud migration and adoption, as well as capacity-building and governance initiatives, while prioritising the use of European funds whenever possible.

26. What savings does the Government expect from the implementation of the PNNS?

Direct savings of approximately €28 million per year are expected, mainly through data centre consolidation and improved energy efficiency. These will be complemented by indirect savings estimated at approximately €165 million per year, resulting from economies of scale, technological modernisation, automation, and the reduction of duplication across public entities.

27. How does the PNNS contribute to environmental and energy efficiency objectives?

The consolidation of thousands of small technical rooms and dispersed data centres into modern cloud infrastructures will significantly reduce energy consumption per computing unit through improved PUE (Power Usage Effectiveness). This will result in a lower environmental footprint, more predictable energy costs, and stronger alignment with the State's sustainability and ESG objectives.

28. Will the State migrate all data centres to the cloud?

No. The PNNS does not envisage the full migration of all data centres to the cloud. The model is based on an approach whereby cloud adoption depends on the sovereignty level associated with each process.

In certain cases, on-premises or hybrid solutions may continue to be used where justified on security, control, or efficiency grounds. The objective is to promote infrastructure consolidation and modernisation, rather than indiscriminate migration.

29. How does the PNNS relate to the National Data Centres Plan (PNCD)?

The PNNS is directly aligned with the PNCD, complementing it within an integrated approach to the modernisation of the State's digital infrastructure.

While the PNCD focuses on the rationalisation, consolidation, and physical efficiency of existing infrastructures, the PNNS adds a strategic layer centred on digital sovereignty, process qualification, and the adoption of cloud solutions tailored to different needs. Data centres meeting sovereign cloud requirements may therefore be used to host State workloads.

30. How will security and regulatory compliance (GDPR, NIS2, etc.) be ensured?

The sovereignty and security requirements defined for each qualification level apply in parallel with obligations arising from instruments such as the GDPR, the NIS2 Directive, cybersecurity legislation, and other sector-specific regulations.

Qualified solutions will need to demonstrate systematic compliance with sovereignty requirements through audit, certification, and continuous oversight mechanisms.

31. What is the overall implementation timeline for the PNNS?

Between 2026 and 2027, the qualification model, the requirements framework, and the legal framework will be defined, alongside the mapping and qualification of Public Administration business processes.

From 2027 onwards, the development of sectoral adoption plans, infrastructure consolidation, and the expansion of sovereign cloud offerings will begin.

Work will also start in 2026–2027 to ensure that a comprehensive sovereign cloud services offering exists in the market, including the development of State-owned capabilities for a set of needs requiring national control.

By 2030, the objective is for the main shared Public Administration platforms to be available in cloud environments and for a significant level of internal digital sovereignty capabilities to be achieved.

32. In practical terms, what will Public Administration entities need to do?

Entities will need to inventory their business processes, systems, and infrastructures, apply the qualification model (either through pre-qualification or by scoring their own processes), and, based on the results, either strengthen existing solutions or plan the migration and adoption of cloud solutions aligned with the sovereignty level required for each process.

33. How can entities verify whether they comply with the defined requirements?

Compliance will be ensured through the application of the process qualification model and the technical reference frameworks defined by the National Cybersecurity Centre (CNCS) and ARTE, I.P.

Entities will be required to assess the sovereignty requirements of their processes using a pre-qualification framework developed by ARTE and CNCS. Each sovereignty level is associated with a set of security and control requirements defined by ARTE and CNCS.

34. What will be the timeline for the migration of entities?

Migration will be phased and aligned with sectoral adoption plans to be developed from 2026 onwards, with progressive implementation through to 2030 based on the priorities identified during the assessment phase.

This model enables a controlled transition, tailored to the priorities and maturity level of each entity.

35. What will be the cost of migration for entities?

Migration costs will vary depending on the starting point and the specific needs of each entity. However, the PNNS foresees a coordinated and centrally financed approach at State level, reducing the need for each organisation to individually bear the required investments.

National and European funding mechanisms will help distribute the effort over time while generating efficiency gains and reducing operational costs across Public Administration.

36. Where will Portugal stand in 2030 following the implementation of the PNNS?

By 2030, Portugal is expected to have a modern, secure, and resilient digital infrastructure, with the main Public Administration platforms supported by cloud solutions aligned with the defined sovereignty levels.

The State will have greater control over its critical data and systems, increased efficiency in the management of technological resources, and enhanced capacity to innovate and develop simpler, more integrated, and citizen-centric digital public services.

At the same time, the PNNS will help position Portugal as a trusted digital hub in Europe, fostering the development of the national technological ecosystem, including cloud, data, and Artificial Intelligence services.

REPÚBLICA
PORTUGUESA