Strengthening cloud sovereignty of public administrations

In this non paper, the Netherlands advocates the need for coordinated EU action in the development and deployment of sovereign cloud technologies for public administrations. Cloud is critical enabler for our digital society and is used in almost every public administration. The use of cloud technologies enhances flexibility, efficiency, scalability and serves as a foundational layer for Artificial Intelligence. However, the increasing reliance and use of cloud technologies may also create significant strategic dependencies on non-EU cloud providers, which may compromise Europe's digital sovereignty and resilience.

Large dependencies on a few select suppliers, without any other options, may pose significant risks to (national) security, the digital economy and the overall resilience of our society. They may also affect the continuity of (digital) public services, the protection of fundamental rights, and the (effective) functioning of the government. It is therefore imperative that the EU and her Member States take concrete and coordinated steps to become more independent in the use of cloud technologies by public administrations. In this context, the Netherlands expresses its strong support for the Commission’s initiative to issue a recommendation on EU-wide cloud policy for public administrations and procurement.

A more harmonised approach

Given the crucial role of cloud technologies and their far-reaching impact on society, it is of vital importance to strengthen cloud sovereignty of public administrations in an open and future-proof manner. Several member states are therefore developing or seeking to adopt sovereign cloud platforms and -applications to the needs of public administrations. While the Netherlands fully supports these efforts, a more coherent and harmonised approach at the EU level -while respecting the principles of subsidiarity and proportionality- is necessary. This is justified by the inherently cross-border nature of cloud technologies, the current absence of viable European alternatives and the common challenges faced by governments across the EU. In this context, the Netherlands encourages the Commission to stimulate initiatives that support the effective and secure migration of public administration across the EU to sovereign cloud solutions – throughout the EU, for example, by fostering the development, uptake and availability of competitive European alternatives. A more modular approach is required to enhance open strategic autonomy, ensure operational flexibility, and enable redundancy where needed.

Supporting public administrations

We also call on the Commission to support member states by steering the development and use of sovereign cloud technologies and its applications into the right direction. In this regard, we call on the Commission, within the context of cloud use in public administration, to:

- Develop a common definition with criteria on cloud sovereignty. This is necessary to reduce the vast grey zone between sovereign and not-sovereign cloud and it will form the basis for collective European action in this field. The cloud market witnesses an increasing supply of ‘sovereign cloud offerings’ by cloud providers. These offerings are based on diverging principles and characteristics, as there is no set definition of what constitutes a sovereign cloud. In that light, it would be beneficial to determine a uniform definition of ‘sovereign cloud’ for public administrations. The Netherlands is of the view that the definition and associated criteria for cloud sovereignty is best defined and operationalised within the broader legislative framework of the forthcoming EU Cloud and AI Development Act. [1] This definition should entail the following criteria: clarity on the difference between sovereign and not-sovereign cloud, access to and ownership of data, and clarity on exclusive EU or member states jurisdiction for EU based cloud infrastructures. For example: “sovereign cloud should be considered as a collection of cloud services within a jurisdiction that meets the requirements for data localisation and operational autonomy. The sovereign cloud must ensure that its data, operations, infrastructure components and technology cannot be influenced by other jurisdictions and must be protected from direct influence or access by governments from third countries”.

[1] It is important to keep a distinction between policy efforts addressing sovereignty concerns related to public cloud services, and on the other side technical certification under the Cyber Security Act. This would allow technical assurance and political risk screening to be addressed through distinct but complementary channels. See for more details ‘Non paper on the review of the Cyber Security Act’, June 2025.

- Consider a two-tiered approach to the development of cloud measures in light of the urgency. The first step would be to develop measures aimed at ensuring national security in the member states. These experiences would form the basis to – secondly – formulate which measures are sufficient to ensure 'cloud sovereignty' under different use-cases (with more focus on the availability, integrity and confidentiality of cloud services).
- Consider the use of certain critical cloud applications by public administrations as a strategic (or highly critical) use case in cloud technologies. In many cases public administrations store critical and highly sensitive data. Defining public administrations as a strategic use case for certain critical sovereign cloud solutions could attract innovation and investment opportunities for this specific use of cloud technologies from European cloud providers – in turn also enhancing the competitiveness of the EU cloud sector.
- Enhance digital sovereignty in an open manner by supporting the use of open standards and solutions within public administrations, including the CSA cloud standard NVN-CEN/TS 18026:2024, developed by CEN/CENELEC at the request of the European Commission. The aim is to optimise the freedom of choice, improve interoperability, organise the availability of various cloud services and reduce vendor lock-in.
- Develop a common risk assessment for the use of cloud by public administrations. This would give guidance to public administrations to make conscious decisions on the use of public cloud technologies. This risk assessment should be combined with common minimum standards for different types of cloud applications in order to ensure common levels of security, privacy, and sovereignty. For example: the Netherlands has developed implementation guidelines on making well-considered decisions on the use of cloud by public administrations.[2]
- Provide financial instruments for innovation, scaling-up, and use of critical cloud technologies by public administrations, for example under the current Digital Europe Programme (DEP) and Connecting Europe Facility (CEF Digital). Financial instruments aimed at innovation and use of cloud technologies should be prioritised on European technological solutions. Besides, it is of importance that cloud technologies (used by public administrations) form part of a limited set of digital technologies for investments under the next Multi-annual Financial Framework (MFF).[3]
- To use the strength of public administrations in public procurement in order to accelerate investments in the development and scaling of cloud applications for the most essential and critical cloud solutions used in public administrations. The revision of the public procurement directives should therefore include more possibilities to limit the risks to (national) security, steer more on strengthening sovereignty and to guarantee the continuity of government services, whilst being in line with the international (trade) commitments of the EU.

[2] Implementatiekader risicoafweging cloudgebruik, January 2023.
[3] Non paper 'Financing the European digital economy', December 2024.