Regeringskansliet

2026-05-28

Ministry of Finance

A cloud policy for Sweden – for increased security, efficiency and innovation in public administration

1. Introduction

The purpose of this policy for the use of cloud services is to contribute to increased security, efficiency and innovation in public administration.

Actors involved in public administration (public actors) require a range of IT solutions, including various cloud services, to ensure cost-effectiveness, a high level of security, and accessibility for their respective operations. These actors also need to be able to choose between different suppliers and tools based on the requirements and needs of their respective operations. Each actor must make an independent assessment and is itself responsible for its use of cloud services.

The use of cloud services can enable innovation, improve operational efficiency and enhance the resilience of public administration while it can also lead to new vulnerabilities. The policy can contribute to efforts towards cost-effective and secure IT operations, and also to efficiency in general in the organisation in question. This connects the purpose of the policy to central government administration's policy objective of an innovative and collaborative central government administration, and to the fundamentally altered security situation. The uncertainty in the geopolitical situation is affecting many different areas, including the digital, and is something that Sweden needs to address and navigate in the best way possible. Sweden is a highly digitalised country, with digital technology now affecting virtually every aspect of Swedish society. All in all, this highlights the need for central government to have access to and control over essential systems, services and functions that are vital to society at all times.

The policy can be used to support public actors in their use of cloud services. The term "public administration" refers to central government agencies under the Swedish Government as well as to municipalities and regions. Under the Instrument of Government, the obligations of municipalities and regions are, as a general rule, regulated by the Riksdag. With this in mind, the aim is that this policy will also provide support for, and be of benefit to, municipalities, regions and private sector actors that run publicly funded activities.

Cloud services

'Cloud services' refers to digital services and resources that can be accessed remotely, usually via the Internet. The policy covers cloud services in the broad sense, such as infrastructure services for storage and networks, and platform services, such as those used for software development (applications).

It is important for public administration to make use of the opportunities offered by digitalisation in order to develop and improve the efficiency of its activities, and to ensure the provision of high-quality services to the community, citizens and business.

The growth of cloud services has been an important part of the digitalisation of society that has taken place in recent years. For example, cloud services have come to play a significant role in the development and use of artificial intelligence (AI). AI has great potential to enhance the quality of the services provided by government agencies, reduce the administrative burden, improve welfare and strengthen Sweden's competitiveness.

Cloud services can also facilitate digital integration and interoperability, i.e. the ability of different systems and applications to exchange information in an efficient and correct way. Cloud services enable scalability, meaning that computing resources can be adjusted according to workload without adversely affecting performance. This makes it possible to rapidly adapt and expand the capacity in existing systems, and to build new solutions to develop the activity.

Following an assessment of the level of control required for example, cloud services can also be used to safeguard functionality and secure the data processed in public administration. Cloud services can also be used to

conduct activities in premises or locations other than the usual for the activity. This can be extremely valuable in the event of a crisis, a heightened state of alert or even war, particularly in terms of essential services. At the same time, it is important for government agencies to be able to continue their activities even in the event of a failure in a cloud service.

Whilst there is a significant need for and benefit from cloud services, there is uncertainty about how they should be used. The AI Commission's Roadmap for Sweden highlights challenges in this area and proposes that the scope for public actors to use cloud services provided by companies outside the EU should be clarified (SOU 2025:12).

2. Cloud services in public administration

2.1 Starting points

At present, it is common for government agencies to combine different operating models in the IT area. They may use a combination of in-house IT operations, outsourcing to private contractors and coordinated IT operations with other government agencies. The use of cloud services from private contractors is widespread in public administration, although the proportion of government agencies that use privately managed cloud services has declined over time (*Stärkta förutsättningar för att följa den statliga it-driften* [Improved conditions for monitoring central government IT operations], Swedish Agency for Financial and Public Management, 2025:15).

The use of digital services in Europe is characterised by a reliance on contractors based outside the EU. This dependence has strategic implications for Europe's competitiveness, innovation and sovereignty. US companies are market leaders in cloud services in the EU. This presents challenges, such as dependencies, the risk of lock-in effects and high prices due to a lack of competition, but also the need for data security and control over data.

Sweden and Europe need to increase their digital sovereignty, and the Government has therefore signed the Declaration for European Digital Sovereignty (Fi2025/02129). In addition, Europe's digital competitiveness and technological autonomy need to be strengthened, and this should be done in an open manner. Sweden must be able to act independently and in

line with European values, whilst at the same time reaping the benefits of collaboration with global partners.

Within the EU, initiatives are also underway aimed at strengthening digital sovereignty, such as the Cloud and AI Development Act, which the European Commission intends to present in 2026. Among other things, this initiative is intended to ensure that Member States have access to digitally sovereign cloud services for activities meriting especially high protection. The Government intends to play an active role in the negotiations on this Act. The Government welcomes increased competition in this area, as well as the fact that Swedish and European cloud service providers are developing services for the Swedish and European markets, which supports our independence and control over these services.

Sweden's geopolitical situation has deteriorated and characterised by considerable uncertainty. The rapid developments in the world around us have affected our security. As stated in the Government's Statement of Foreign Policy of 18 February 2026, Europe must be strengthened. The Government recognises a growing need for international cooperation at the intersection between technology, innovation, trade and security. It is important to reduce the vulnerabilities associated with one-sided economic dependencies.

Increasing our digital sovereignty does not mean that Sweden should isolate itself from the rest of the world. Given the varying conditions in public administration and the need for different types of IT operations, including cloud services, and by adopting a risk-based approach, public administration will continue to be able to use market-leading products and services, even if they are provided by companies domiciled outside the EU. When a public actor chooses a solution, operating model and provider, the choice should be guided by the requirements applicable to the activity in question in terms of functionality, security, control, sovereignty, robustness and cost-effectiveness, for example.

2.2 Guidelines for the use of cloud services in public administration

It is important for public administration to have access to, and the conditions needed for using, modern, efficient and secure cloud services that meet legal and security requirements. The Government considers that the

following principles can serve as a guide for the use of cloud services in public administration.

2.2.1 Adopt a risk-based approach to cloud usage

In the current security situation, the threat to Sweden is wide-ranging and serious. In the National Security Strategy, the Government notes that hostile actors, both state and non-state, are constantly attempting to exploit vulnerabilities in Swedish society in order to achieve their objectives (Govt Comm. 2023/24:163). Dependencies in areas such as technology and information and communications technology (ICT) infrastructure may pose risks to national security. This places heavy demands on government agencies' cyber security work, regardless of the service, solution or operating model that is used.

In connection with public procurements, it is important for public actors to bear in mind that, under the regulations in certain countries, companies in those countries may, under certain circumstances, be required to disclose data to the relevant national authorities, even if that data is processed and stored outside those countries.

In light of this, it is important that public actors, in accordance with current regulations, work actively with systematic information and cyber security which also includes planning to ensure continuity even under adverse conditions. In this context, it is important that the information intended to be processed via a cloud service is assessed on the basis of how important it is to protect it, and relevant information security considerations. It is also essential that the solutions used are robust, i.e. resilient to errors, disruptions and changes.

Processing of personal data in US cloud services

In 2022, the EU concluded an agreement concerning an EU-US Data Privacy Framework (EU-US DPF). Following the agreement, the European Commission adopted an 'adequacy decision' in 2023 based on the framework, meaning the transfer of personal data to US organisations on the EU-US DPF list of organisations is permitted. This decision simplifies the transfer of personal data to the US by permitting such transfers to take place, under certain conditions, without the need for additional safeguards.

Public actors have stringent requirements governing the secure processing of personal data, and information- and cyber-security. It is therefore important for public administration to have access to, and the means to make use of, modern, efficient and secure cloud services or other services that meet the legal and security requirements. Public actors need to determine factors such as the extent to which the services involve the transfer of personal data to countries outside the EU, and to ensure that such transfers are done in accordance with the requirements set out in Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Guidance

- The Swedish Civil Defence and Resilience Agency has produced a methodological guide for systematic information security work. Further information on this is available on the Agency's website.
- The Agency also offers cyber security advice and has developed support for working with cyber security for municipalities, among others. Further information is available on the Agency's website. On 1 July 2026, the Agency's cyber security activities will be transferred to the National Cyber Security Centre (NCSC), which is part of the National Defence Radio Establishment (FRA).
- The Swedish Security Service has produced an information security guide which, among other things, provides guidance on the rules for the classification of information and obligations when disclosing security-sensitive activities to another actor. Further information on this is available on the Agency's website.
- The Swedish Authority for Privacy Protection provides information on the countries that the European Commission deems to have an adequate level of protection, and to which personal data may be transferred without specific authorisation. Further information is available on the Authority's website.

2.2.2 Choose cost-effective cloud solutions

There are many advantages to using cloud services over on-site IT solutions, including economies of scale and the potential to improve cost-effectiveness by being able to develop and launch services for citizens more rapidly. Furthermore, cloud-based solutions often offer a higher level of security. Cloud-based and standardised solutions may therefore be preferable to on-

site IT solutions in many instances. New applications and services can be developed and deployed using cloud services, and existing systems can be migrated to the cloud where appropriate.

Guidance

- Where necessary, public actors can receive support from national central purchasing bodies when procuring IT products and services, including the procurement of cloud services. The National Procurement Services (*Statens inköpscentral*) acts as a central purchasing body for government agencies, but municipalities and regions may also call off orders under its framework agreements in the area of IT. Adda AB is the central purchasing body for members of the Swedish Association of Local Authorities and Regions.
- Central government agencies can receive support when choosing an IT operating model solution. The Government has appointed the Swedish Social Insurance Agency (*Försäkringskassan*) as a coordinating authority (*samordnande myndighet*) and service provider authority (*leverantörsmyndighet*) under the *förordningen om samordnad och säker statlig it-drift* (Ordinance on coordinated and secure central government IT operations) (2024:1005). Försäkringskassan, together with the other service provider authorities – the Swedish Mapping, Cadastral and Land Registration Authority, the Swedish Tax Agency and the Swedish Transport Administration – provide IT operations services, such as cloud services, within the framework of the coordinated central government services offering and support government agencies in their choice of IT operations solution.

2.2.3 Increase benefit for the activity

A cloud service can be provided in a number of different ways. Some activities may have a greater need to make their own adaptations, whilst for others it may be more important to start using the services quickly. In public administration, therefore, different types of cloud solutions may need to be used in order to achieve good results efficiently and securely, thereby increasing the benefit for the activity.

Guidance

- The Swedish Agency for Digital Government (DIGG) has produced a methodological support for addressing data protection issues that can be used in the context of digitalisation and digital operational development. Further information is available on the Agency's website.

- By participating in collaborations, for example Ena – Sweden's digital infrastructure – public actors have the opportunity to share their experiences on matters related to digital infrastructure.

2.2.4 Promote portability and a well-functioning market

The Government considers it to be important that the cloud services market is dynamic and functions well. The use of cloud services can make it easier for public administration to process data. At the same time, there may be risks that need to be addressed if the public actor becomes locked into a cloud service and its provider.

In light of this, it is important that public actors ensure that it is possible, where necessary, to transfer data swiftly to, and manage systems operated by, another provider or in-house. The Government therefore welcomes cloud services with standards and solutions that promote portability, that is, the ability to move data, functions or services from one system to another, and reduce lock-in effects.

Furthermore, in order to reduce dependence on a specific cloud solution, it is important that new applications in public administration are developed in such a way that both applications and data can be transferred between, for example, different IT systems. When using proprietary services – i.e. services where the user does not have free access to the source code – it may also be necessary to have a pre-determined strategy for how the service can be replaced should the need arise. It is also important that contracts with cloud service providers contain exit clauses that enable the actor, if necessary, to migrate applications and data to another provider or to take over management themselves, for example.

It is important for public administration to maintain a good dialogue with the suppliers of cloud services. If government agencies, municipalities and regions clearly communicate their needs to the market, this will improve the market's ability to meet those needs.

Guidance

- Direct awards of contract can be an opportunity for small businesses to enter into larger public sector contracts. The most cost-effective supplier is not necessarily the one used before or the best-known. It is therefore worthwhile trying to reach out to more suppliers and ensure

that they are aware of the current competition. *Färdplanen för de offentliga affärerna 2025–2030* (Roadmap for public procurement) (Fi2025/01827), which is available on the Government's website, provides guidance to procuring actors on how they can improve the conditions of their purchasing activities.

- It should be easier for customers to switch between different cloud service providers, which will improve the conditions for data sharing and interoperability within the EU. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) forms part of the EU's strategy to strengthen the data economy in Europe through common European data spaces, and entered into force on 12 September 2025.

2.2.5 Maintain appropriate control over data, IT operations and technology

It is important to strengthen Sweden's digital sovereignty, reduce strategic dependencies, and simultaneously strengthen public administration's ability to choose different types of digital solutions.

When using cloud services, it is necessary to take into account control over the data as well as the need for data sovereignty, but to varying degrees – depending on factors such as how important protection of the data is and what functionality is needed. Public actors need to choose cloud solutions that offer an appropriate level of control over data, IT operations and technology – while ensuring that the actor meets the security and compliance requirements.

Public administration's activities are diverse, and the actors involved process information that merits varying levels of protection. This may involve sensitive data such as personal data, information classified as strictly secret and other classified information. Processing such information in a cloud service requires access to specifically designed security solutions, i.e. security solutions adapted to the activity's needs, risks and what levels of protection the data merits. Furthermore, under the Protective Security Act (2018:585) and the Protective Security Ordinance (2021:955), in each individual case public actors must ensure that the applicable protective security requirements are met.

In crisis situations – such as serious geopolitical events or cyber security incidents – the capability to maintain essential services and exercise effective control by switching service providers is of crucial importance.

Digital sovereignty is about having control over data and systems and ensuring that no external party can influence, access or deny access to data or essential functionality. This type of sovereignty can be ensured through both technical and non-technical measures. Technical measures often aim to prevent the service provider from accessing the information stored in the cloud solution. An example of such a measure is encryption. It may also involve measures to prevent one user from accessing another user's data. Non-technical measures often refer to cloud services being provided from data centres located in the EU, with staff who are EU citizens and meet the necessary security requirements, and which fall under Swedish or EU jurisdiction. Such measure might also include that service providers have their headquarters in Sweden or the EU in order to maintain digital sovereignty in this regard. However, outsourcing IT operations to a European provider may also mean comprising national digital sovereignty, for example if the country in question has regulations granting national authorities the right of access to data.

In practice, digital sovereignty can be regarded as a spectrum, with higher standards of sovereignty applying where the risks are greatest, for example in relation to critical data and in services or sectors of major importance, such as essential services.

Information meriting a high level of protection and critical services with high demands on availability processed via cloud services should be processed using solutions offering a high degree of control.

Guidance

- In Chapter 10, Section 2a of the Public Access to Information and Secrecy Act (2009:400), a provision has been introduced permitting government agencies to disclose information classed as confidential to a private individual or to another agency tasked with the technical processing or storage of such information on behalf of the disclosing government agency. The amendment aims to create better conditions for government agencies to outsource or coordinate their IT operations,

and to strengthen the protection of the data disclosed to a private individual when IT operations are outsourced.
- The European Commission has developed a framework for sovereign cloud solutions known as the Cloud Sovereignty Framework. The framework can provide support to a procuring actor in posing relevant questions to the cloud service provider, thereby ensuring an appropriate degree of digital sovereignty in the service that is chosen.

2.2.6 Ensure that good and relevant requirements are imposed on providers

It is important that public actors continue to impose clear requirements on cloud service providers, including ensuring clarity regarding how data is processed, stored, transferred and protected in the entire chain of suppliers.

Guidance

- The Government has tasked the NCSC at FRA (Fö2026/00737) with drawing up guidelines on aspects such as cyber security related requirements in public procurement and cyber security in the supply chain for information and communication technology (ICT) products and ICT services. A report on the task is to be presented by 11 December 2026 at the latest.
- In 2025, the Government commissioned the Civil Defence and Resilience Agency (Fö2025/00390) to develop a model for monitoring digital supply chains, which is to supplement the existing structure for monitoring systematic information security management in public administration. The task has been reported on (Fö2026/00812).

3. Measures to promote the use of cloud services

The Government has taken a number of measures to make it easier for public administration to procure cloud services.

3.1 Forum for better implementation of IT purchases

It is important for government agencies and other actors that provide procurement support to be able to share their experiences and carry out collaborative initiatives with a view to increasing the impact of and consistency in procurement support, and to make the utilisation of resources more efficient.

Guidance

- The Government has tasked the National Agency for Public Procurement with facilitating the implementation of the roadmap for public procurement 2025–2030. As part of this task, the Agency is to set up a forum to coordinate procurement support linked to the purchasing category 'IT', and to help promote the achievement of the objectives of the contracting authorities' and units' IT purchases.

3.2 Preliminary study on setting up a dynamic purchasing system for innovative digital solutions

In the Government's view, public administration's purchasing of digital services needs to become more efficient and more accessible to a wider range of providers. This could strengthen competition, enhance innovation and reduce dependence on major global actors. Furthermore, to strengthen Sweden's digital sovereignty, more services need to be procured from Swedish and European providers, while thresholds need to be lowered so that small and medium-sized enterprises can more easily win public sector contracts.

Guidance

- The Legal, Financial and Administrative Services Agency has been tasked (Fi2026/00311) with carrying out a feasibility study on a dynamic purchasing system for innovative digital solutions for public administration. Suppliers can join such a system at any time, provided that they meet certain requirements. Suppliers may then submit tenders for all contract notices in the product categories for which they are approved, without having to re-qualify themselves. In the feasibility study, the Legal, Financial and Administrative Services Agency will propose measures that will make it attractive for small and medium-sized enterprises to participate in this system. Additionally, the Agency will analyse which types of products should be covered by such a purchasing system and, when making its selection, give priority to product categories in which there are many Swedish and European suppliers.

3.3 Proposal to amend procurement rules to protect Sweden from hostile states

The Government has previously concluded that Sweden's public procurement legislation should be reviewed. The current procurement rules

make no explicit distinction between suppliers from the EU and those from third countries that do not have a free trade agreement with the EU. This means that all suppliers can participate in public procurements, and are entitled to equal treatment and judicial review.

On 25 November 2025, the memorandum *Tredjelands-leverantörers tillträde till upphandlingsförfaranden* (Third-country suppliers' access to procurement procedures) (Ds 2025:29) was presented. The memorandum proposes that the public procurement acts be amended so that they do not apply to third-country suppliers from countries that do not have a free trade agreement with the EU. Contracting authorities will therefore be able to decide whether these suppliers should be permitted to participate in public procurements and whether their tenders should be treated in the same way as tenders from suppliers based in Sweden or the EU. The proposed regulation also means that suppliers from countries that do not have a free trade agreement with the EU will no longer be covered by the right of access to judicial review provided for under the public procurement acts.

3.4 AI workshop

The Government assesses that AI has the potential to fundamentally transform public administration and thus streamline processes, improve the quality of services provided to citizens, lead to a more efficient use of taxpayers' money and save resources. An AI workshop will be developed over time to provide an infrastructure that can be used across public administration, with associated support functions, to facilitate the introduction of AI into public administration.

Guidance

- As a first step, the Government has tasked Försäkringskassan and the Swedish Tax Agency with establishing an AI workshop for public administration (Fi2026/00018). It is anticipated that the workshop can be established as a hybrid solution, which involves establishing a community cloud with a high level of control that can interact with private actors' infrastructures. It is intended to serve as a platform that facilitates cooperation between public administration and the private sector, strengthens long-term governance and knowledge and skills development, and promotes innovation and sustainable digital development.