DAGENS NYHETER.

A printout from Dagens Nyheter, 2019-11-22 09:49
Origin of the article: https://www.dn.se/debatt/sveriges-digitala-suveranitet-hotas-av-it-tjanster-i-molnet/

DN Debate

DN Debate. *"Sweden's digital sovereignty is threatened by IT services in the cloud"*

PUBLISHED YESTERDAY

What the public Sweden now needs to consider is whether it is at all appropriate for Swedish authorities to relinquish control of data that is created and processed in community-based activities, writes Nils Öberg. Photo: Pontus Lundahl / TT

DN DEBATE 22/11. Today, Friday, Försäkringskassan publishes a white paper on public cloud services in public operations: Other countries' legislation, such as the US "Cloud Act", means that public actors lose control over data created and processed in community-based activities. Therefore, a clear government-wide strategy is now required, writes Nils Öberg, Försäkringskassan.

Read on later

Like other authorities, the Social Insurance Office handles very large amounts of privacy-sensitive personal data. Also, data that does not affect the privacy of individuals can, if handled incorrectly, be sensitive and therefore need protection. For this reason, there is also a comprehensive regulatory framework in place that governs what public authorities may and may not do with the information they have access to. In the EU too, a rigorous regulatory system has been introduced and developed as

these data are increasingly being processed digitally and not as before in physical paper acts. These rules place very strict requirements on how the information in question is handled and stored.

The development that is now taking place is that an increasing proportion of commercial digital services are processing and storing information in so-called public cloud services. In short, this means that service providers place both the software used, and the result of what we produce, on external servers operated by the service providers themselves. The consequence is that the digital products and services offered to public actors will no longer be controlled by us completely, regardless of whether the servers in question are located in Sweden or elsewhere.

We will no longer be able to control which foreign players, private or public, who can legally obtain access to this information. A very clear example is the US law (Cloud act) which means that US authorities have the right to request data from all US service providers, no matter where in the world the information is stored. Similar legislation also exists in a number of other countries such as Russia, India and China, to name but a few.

Sweden needs to formulate a clear authority-shared strategy and a long-term plan of action if Sweden's digital sovereignty can be maintained.

There is no doubt that these rules come into direct conflict with both international law and GDPR and are also not compatible with Swedish public and secret law. The new business models that the digital industry has been developing and offering the market for some years now are not adapted either to the needs of public authorities or to the legislation we have to adhere to. The problem is not limited to Sweden. Several large EU countries, including the Netherlands, France and Germany, have already reacted very strongly to developments and are or are in the process of taking action.

Today, Friday, Försäkringskassan publishes a white paper in which we try to clarify our view on the issue of public cloud services in public operations.

A large number of Swedish authorities, including municipalities and regions, are already using many different cloud services - even for personal data and / or data that is confidential. Of course, this does not occur as a result of an easy-going attitude to the obligations that come with exercising authority over an individual, but as a result of an ambition to streamline and modernize the business. Nevertheless, it is our assessment that

this development is not infrequently contrary to legislation governing confidentiality and personal data processing.

The debate that has taken place in Sweden has so far been devoted to trying to estimate the extent to which Swedish authorities' data contained in public cloud services can in practice be disclosed to so-called third countries (non-EU countries). In other words, will other countries' authorities really take advantage of the opportunities offered by their legislative assemblies?

All experience suggests that so it will be. Of course, authorities are expected to use all the tools they have to solve their tasks. But no matter what opinion you have in that regard, it is not the question that needs to be answered. What the public Sweden now needs to consider is whether it is at all appropriate for Swedish authorities to relinquish control over data that is created and processed in community-based activities.

Above all, there are four specific issues that we must jointly address:

1 **Is it appropriate that, as a Swedish authority, entrust parts of its community-carrying activities** to a service provider that is under the jurisdiction of another state with the possibility for that state to access information within the activity without our consent?

2 **Is it appropriate for Swedish authorities to transfer to a commercial party the** decision to contest a request for extradition to third-country authorities for information protected in Sweden?

3 **Is it appropriate that Swedish authorities do not have full control** and control over which other third countries, after agreement with the authorities in the service provider's "home country", will be able to access both privacy-sensitive information and other sensitive information in community-based activities?

4 **Is it appropriate that Sweden, in view of the access to information that arises in cloud services** , in practice assigns legislative power regarding the processing of Swedish authorities' data to a third country?

The starting point can hardly be any other than that both the Swedish state administration and municipal and regional authorities must ensure control over their digital business-critical systems. Therefore, in order to protect our community-bearing functions against the increasingly common cyber attacks, safeguard personal integrity and reduce dependence on individual services in the market, Sweden therefore needs to formulate a clear government-wide strategy and a long-term plan of action on whether Sweden's digital sovereignty can be maintained. Similar processes have been initiated in other countries that have not progressed as far as Sweden in the digitization of their public operations.

In order for Swedish authorities to continue to benefit from all the possibilities of digitalisation - through collaboration nationally and within the EU - a clear and common requirement

has to be made. The services offered must be adapted to the specific needs of the authorities and the legislation that applies in Sweden and within the EU. Only then can we continue to take advantage of the innovation power and efficiency that the use of private IT services entails while ensuring that Sweden's digital sovereignty is not undermined.

For Försäkringskassan, that requirement will guide the choice of IT services going forward. In the White Paper, we argue for our view that the Swedish state and municipal administration must in future also have sovereign control over their information. At least until the legislation governing the issue says something else.

DN Debate. November 22, 2019

Debate article

Nils Öberg, Director General of the Swedish Social Insurance Agency:
"Sweden's digital sovereignty is threatened by IT services in the cloud"

Text:

Nils Öberg , Director General of the Swedish Social Insurance Agency

View Comments (5)