



## Health data in the cloud

SWEDISH MEDTECH REGULATORY SUMMIT 31 MARCH 2022

## Team



**Niklas Follin**

Partner

- +46 70 298 02 25
- niklas.follin@setterwalls.se



**Carl Broberg**

Associate

- +46 73 079 87 99
- carl.broberg@setterwalls.se



## Legal background

### The Schrems II Judgement

- The CJEU invalidated Privacy Shield
- Still permissible to rely on SCC, however, supplementary measures required
- *No adequacy decision* to rely on for transfers to the U.S.
- *Significant due diligence* (TIA) burden upon data exporters
- Affects all third country transfers

### Deciding to use a cloud service

- SOU 2021:1 proposes a new secrecy provision
- SKR advice
- Swedish DPA encourages health provider to investigate a cloud solution further indicating that it is still possible to use cloud services under strict compliance adherence as long as the providers is under the same confidentiality regulation and no foreign infringing law applies.

### Health data and outsourcing of processing

- The Swedish Authority for Privacy Protection finds outsourcing of support of cloud services used for healthcare problematic because of the confidentiality requirement

### U.S. owned IT solution and cloud services

- the Swedish Tax Authority and other public authorities have declined the use of Teams
- eSam investigation
- Stockholm stad and Microsoft Teams
- Doctolib: sufficient encryption allows for processing of health related data in the cloud
- The Dutch authority regarding Microsoft Cloud service: "If government organisations ... implement all recommended measures, there are no known high risks for the data processing"

### General assessment of cloud services

- The EDPB and other national DPA will assess the use of cloud services by public authorities. IMY has shared a long list of questions and the answers to these questions will be the basis for future measures.



## Common problem

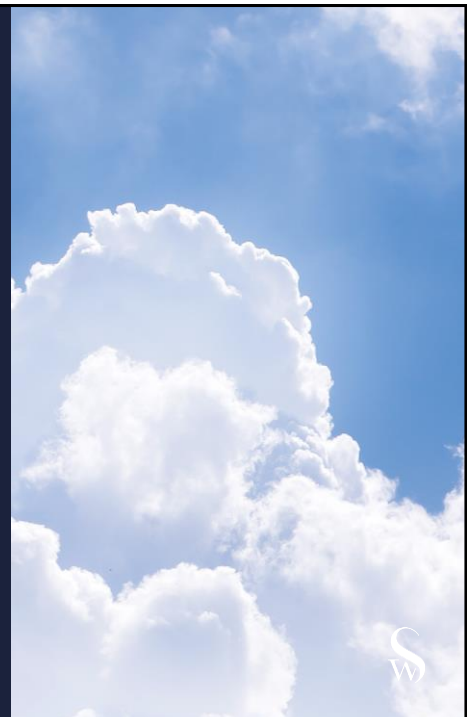
- Can we use a cloud service for processing of health data?
- Does it matter if the cloud service is owned by a foreign company:
  - (i) that stores data outside the EU?
  - (ii) that stores data inside the EU?



## This is what we know

### “Can we process health data in the cloud?”

1. There is no legal restriction on cloud use as is
2. Uncertainties regarding
  - terms and conditions and
  - if large cloud providers transfer personal data
3. Because of this, the rules on third country transfers are still relevant.
4. This means: There is an obvious risk that many uses of cloud services within the health sector are non-compliant.



## Practical considerations

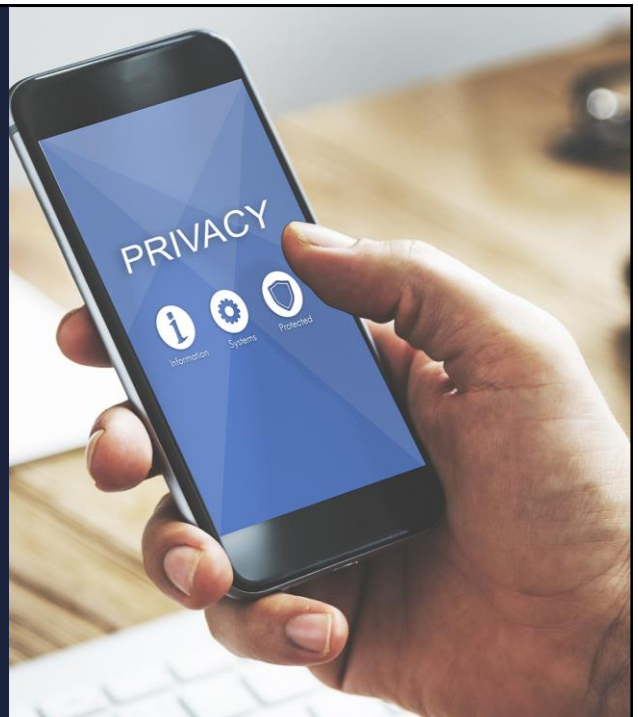
### If you want to use a foreign IT solution

- know where and how your/your customer's data is stored and processed
- know if your/your customer's data is sensitive
- be aware of your customer's requirements, some customers will not tolerate certain foreign IT solutions
- make a thorough assessment of local laws and implementations in the third country
- find out if the foreign IT solution is certified and what measures the provider has taken towards compliance
- make a risk assessment regarding non-compliance and consider the effects on your business
- be aware that systems and tools are being challenged by authorities



## Final reflections

1. It is currently not prohibited to use cloud services for processing of health data.
2. The uncertainties in relation to third country transfers and legal use of cloud services are unsatisfactory
3. Understand that the legal landscape can change quickly; we expect continuous developments on third country transfers.
  - Highly political; ongoing and intense discussions between the EU and the U.S. – Privacy Shield 3.0?
  - Increasing regulations of the digital landscape; stay updated!



**Thank you!**



**SETTERWALLS**

