Vismas use of cloud vendors - clarifications in light of the Schrems II verdict and the CLOUD act

Dear Customer,

In the aftermath of the Schrems II verdict from the European Court, Visma has received multiple questions from customers regarding which measures Visma has taken in light of the verdict, and questions related to Visma's use of subcontractors from the US in general. This document is made to clarify misunderstandings about using US vendors as subcontractors.

What is new after Shrems II?

In the Schrems II judgment, the European Court of Justice provides additional requirements for the transfer of personal data to countries outside the EU/EEA (third countries). This means that it is no longer sufficient to merely use a valid transfer basis such as the European Commission's standard provisions (EU SCC) or binding corporate rules (BCR). If one wants to transfer or process data in the US or any other third country, one must establish "additional measures". It is still unclear what this means in practise.

Visma's use of US vendors - hosting data in the EU

All of Vismas strategic cloud hosting providers (AWS, Azure, Google and Salesforce) host data on data centers within the EU/EEA. This means that customer data, including backups of customer data, from Visma cloud services and products, are processed within the EU/EEA only. Visma controls access to customer data in AWS, Azure, Google and Salesforce. The cloud hosting provider's personnel are not granted access to customer data. Visma does not transfer customer data outside the EU/EEA, nor does Visma instruct our cloud hosting providers to do so.

The risk regarding using US vendors - CLOUD act

Another topic Visma receives questions on is the CLOUD Act. Vendors like Google, Amazon, Microsoft and Salesforce are all based in the US and thereby are subject to US law, hereunder the CLOUD Act.

The CLOUD Act does *not* grant US law enforcement agencies free access to data stored in the cloud, inside or outside the US. American law enforcement agencies can compel service providers to provide data only by meeting the rigorous legal standards for a warrant issued by a US court. US law sets a high bar for obtaining a warrant, requiring that an independent judge conclude that the law enforcement has reasonable grounds to request the information, that the information requested directly relates to a crime under US law, and that the request is clear, accurate, and proportional. These are international legal principles and not a specific US vendor

risk: any authority from any country in the world is free to file a request for access to data to a cloud vendor, including norwegian tax authorities or the swedish police.

Our strategic cloud hosting providers have a strong commercial interest in not disclosing data to any authorities. Cloud providers' business, including their aim to further increase market shares within the public sector, rely on trust from customers that their data is kept strictly confidential.

Thus, Visma's cloud hosting providers have included contractual commitments to challenge government requests for data if they were to receive a court order.

In any case, Visma controls access to customer data. The vendor's personnel are not granted access to customer data. This means that if a Visma vendor receives a court order, and their challenge of it is not successful, they have to notify Visma and ask for Vismas approval to access data. In such cases, Visma would fight the request and notify the affected customers. Visma has not received any such requests.

Visma Trust center

At https://www.visma.com/trust-centre/ our customers can find information concerning the different services Visma delivers and how these services fulfil the obligations under the GDPR.