

# THE HAGUE FORUM FOR CLOUD CONTRACTING

August 29, 2019

Ministry of Justice and Security / Strategic Vendor Management in co-operation with the European Data Protection Supervisor

European institutions gather to keep control over data processing when in the cloud.

**Over a hundred representatives of public institutions from all over Europe gathered in The Hague on August 29 for the first European Software and Cloud Suppliers Customers Council to discuss plans to keep control over their digital infrastructures from hyperscale cloud providers like Amazon, Google and Microsoft. The aim of the Council is to collectively create standard terms and conditions that need to be accepted by the hyperscale providers in collaborative procurements of cloud and software services.**

Representatives of a wide range of scientific, international and governmental institutes from across the EU discussed ways to keep control over data processing by cloud and software providers. The conference was organized by Strategic Vendor Management of the Dutch Ministry of Justice and Security in collaboration with the European Data Protection Supervisor



Strategic Vendor Management successfully negotiated earlier this year new contractual clauses with Microsoft to make sure using Windows and Office will not violate privacy legislation.

A study commissioned by the ministry found that Microsoft Office 365 was in fact in violation of the GDPR. Secretary-General Mr. Siebe Riedstra opened the conference, explaining that renegotiating contracts is the first step in rebuilding the relationship with the suppliers of hyperscale cloud and software services like Amazon, Google and Microsoft:

"Keeping up with changes in supplier's terms and conditions as well as with the continuous changes in their product costs millions of Euros per year. This can only be changed by collectively imposing our own terms and conditions

The 2018 Office 365 Data Protection Impact Assessment (DPIA), which builds on a similar 2017 study into Microsoft Windows 10 by the Dutch Data Protection Authority, found that Microsoft Office 365 ProPlus for enterprise users, even in the version that is installed locally, will in numerous ways transmit personal data to Microsoft servers, without the system administrators having any way to prevent or review these transmissions. Microsoft used to reserve the right to change the data they collected for diagnostic purposes and other telemetry – and also to use those data for its own purposes. This was no longer acceptable for the ministry.

Based on the DPIA study, the ministry negotiated significant changes, both in the way Office 365 ProPlus and Windows will handle data, as well as in the contract with Microsoft. Strategic Vendor Manager Microsoft for the Dutch government, Mr Paul van den Berg – who initiated the conference:

"We turned it all around on Microsoft, to say: in case you receive data from us, it can only be for one of three purposes: provide the service we bought and use; keeping it secure; and keeping it up to

In order to become compliant with GDPR requirements, enterprise users of Microsoft Office 365 ProPlus have to adopt these same technical measures, that have since been made available by Microsoft to all enterprise users. They also need to negotiate their own changes in the contracts. But that turns out to be hard to do for many organizations, which lack the leverage of the

collective Dutch government. Getting the necessary contractual amendments will only be possible for most customers if they generate collective bargaining power.



Some European Institutions have already found cloud providers unwilling to change their terms and conditions, even when confronted with the results of the Dutch studies. Acting European Data Protection Supervisor (EDPS), Mr. Wojciech Wiewiórowski, however, points out that first it is the data controller that is required to be compliant. While Microsoft claims to be a processor for much of the processing it does, it is the controller's responsibility to use only processors meeting the requirements of the applicable data protection law. It is therefore up to the institutions to organize the way they keep control, according to Mr. Wiewiórowski:

"The solution implemented by the Dutch government shows what can be done by a well-equipped, skillful and knowledgeable institution – and on a scale that cannot be done by individual, smaller organizations. I am grateful to the Dutch for making the results of their study and their negotiations public, so others can benefit."

Two factors keep being mentioned by speakers as essential ingredients for staying in control over data processing, especially in the cloud. The first factor is that enough leverage needs to be generated to successfully make fundamental changes to the way terms and conditions are being negotiated. If enough institutions collaborate on procurement and contract management, change will be possible, says Mr. Wiewiórowski:

"If I didn't believe we can find the people and the institutions to make a real change, I wouldn't be here."

A show of hands in the room shows that the majority of participants are eager to join in the effort.

The second factor that will determine the success is in developing standardized frameworks for creating contracts and controlling their execution, based on the tools created by GDPR. If the institutions are to be in control over the way software processes personal data, they need a common understanding of the way to use DPIAs and audit powers – and that requires sharing of information among the institutions. The Dutch DPIA study therefore looked beyond the reality as described in the official documentation, to the actual transmissions that could be detected coming out of the software.

A holistic approach to controlling data processing requires looking at organizational and contractual, as well as technical aspects. This is underlined by the presentations of Mr. Maximilian Winkler of the German Federal Office for Information Security, who investigated the inner workings of the telemetry infrastructure of Windows 10, and Mr. Anders Steijaert of SURF, a cooperative association for IT services for Dutch educational institutions, who explained some of the challenges when leveraging collective bargaining power with hyperscale providers.



Building a comprehensive strategy to achieve success at the table is required. Attention to detail and being in control of the negotiations and the drafting were key ingredients in the negotiations with Microsoft, says Mr. Herald Jongen, one of the negotiators present:

"We had to make sure that Microsoft understood we both had an interest in the outcome of the negotiations. They are not the enemy. We only wanted to exercise our responsibilities to keep control over the data they process for us."

The energy in the room to change the way the institutions depend on suppliers is strong. Where for years it had been impossible to imagine a future where the suppliers don't keep a stranglehold on the conditions under which they supply their services, after this meeting, most participants seem to agree that collective action is inevitable.

The alternative seems almost too dystopian to contemplate. In the end the conference will be a test of the resilience of GDPR and even more may depend on it, as Mr. Robert Riemann of the EDPS states:

"In order to maintain sovereignty, public authorities must protect critical supply chains and have exit strategies when using Software-as-a-Service."

This is even more clear when considering the rise of artificial intelligence, algorithms and the internet of things. One speaker points out that if those gain wide adoption, that would compound the problem with compliancy with GDPR and other standards and make it harder to change contracts.

In the end the conference agrees the desired changes simply have to happen, and have to happen soon. Since regaining control and compliancy with GDPR is only possible through improved contracts, there simply is no alternative. It is suggested that the EDPS may move things forward by issuing Guidance, an idea which is enthusiastically received by many participants. The conference will reconvene in the spring of 2020 and will continue under the name **The Hague forum for Cloud contracting**.

The hyperscale providers will have no choice but to accept that GDPR changes the way control is executed in the cloud. And that prospect is clearly a welcome prospect for those attending the conference.



KLAER  
COMIC  
HOUSE

**All EU member states, EU institutions, European governmental partnerships and European governmental organizations or governmental alliances that purchase cloud services, are cordially invited to participate in the 'The Hague forum for cloud contracting'.**

**For more information contact:  
Ministry of Justice and Security  
Strategic Vendor Management**

**Email: [SLMMicrosoft@minjenv.nl](mailto:SLMMicrosoft@minjenv.nl)**