October 26th, 2022

Open letter to Mr. Thierry Breton on the necessity of creating new market opportunities for highly secure cloud solutions in Europe

Dear Mr. Commissioner, dear Mr. Breton,

Business users of digital technologies within the European Union obviously have to (and want to) comply with the security regulations in effect. Furthermore, a reinforcement of these regulations, along with an increasing appeal to European sovereignty from the member states of the European Union, is foreseeable. Of course, our members support such regulations, considering them as highly important for the protection of their organisations, and as a means to provide the necessary guarantees of data integrity to their customers and their employees.

In the current business reality European enterprises often don't find verifiably adequate solutions provided on the market, or they find solutions that claim to be compliant, but in fact they lack the trustworthiness needed. Some providers of digital technology presently claim that their solutions are compliant with EU security and privacy regulations, making use of the legal uncertainty surrounding international data transfer and processing issues, even if these claims are not fully demonstrated, or obviously incorrect.

As a result, organisations – both businesses and public administrations – have to resort to either of the following options, each carrying their own risks:

a) drive the development of dedicated solutions by themselves or in their community,
b) choose to take the risk of not being compliant,
c) buy solutions with the described residual risk of legal problems.

Choosing option a) will lead to the risk of high costs for maintaining a specialised solution with no guaranty of sufficient long term support throughout the life cycle. Additionally, the risk of running out of specialised resources remains. Setting off on such a path, does not guarantee a successful result.

Option b), choosing not to be compliant, is unacceptable, as it obviously bears legal risks of losing business secrets and private customer data, bringing reputational damage in case of becoming public. The minimum is the risk of fines and other penalties.

It is therefore option c), buying sub-optimal solutions, that is usually chosen or – frankly speaking - the only real option available. As the system will not be totally compliant, there is still a risk of fines.

In any case, the current situation frequently leads to digital systems and the data contained therein are less secure than required.

Especially when government or trade secrets are involved, this lack of security is certainly not acceptable.

This fact becomes even more important when the changing geopolitical landscape is taken into account. It is rapidly transforming from open trade, rule of law and common perspectives, towards antagonistic competition between regions, where threats, coercion and use of force is becoming common practise. With that obviously an increased risk of cyber espionage and sabotage and, subsequently, the increasing necessity of cybersecurity based on European values and requirements comes into play.

The Cyber Security Act of 2019 provides for a cybersecurity certification framework that should lead to certification schemes, requirements for products, services and processes and three levels of assurance. Certification schemes are being worked on, but at the moment no provider can deliver solutions that comply with a high level of assurance, at least not on a required scale. Such solutions are increasingly necessary, as the Network and Information Security Directive 2 will soon require more organisations to provide assurance of high levels of security.

In our experience, business users that demand high assurance levels from their providers are not taken seriously. Several Data Protection Impact Assessments into products and (Cloud-) services of some major suppliers over the past years have revealed serious issues, complicating or making GDPR-compliance very difficult, if not impossible for business users.

That's why our associations call for requirements to be fulfilled by "trusted cloud" offers in order to undoubtedly protect our (business) secrets and personal data. They notably call for a European certification scheme for cloud services (EUCS) to guarantee the highest level of immunity to non-European legislation with an extraterritorial scope for certain cloud service offerings on the European market.

In the current market situation providers will only take steps in the desired direction when there is an obligation written in law. The adoption at a European level is the only way to create a real European market for cloud services dedicated to sensitive data and trade secrets, which doesn't really exist today. All solutions that by design meet the requirements should be welcome in this new market.

We can see similar measures being taken on a national level (France and Germany are trying to establish solutions in co-operation with the non-EU market leaders). However, this leads to a further fragmentation of the European Single Market and it also leads to even less competition between providers in the cloud market, bearing the risk of high costs for the business and public administration users in the end.

Our communities of European business users of digital technologies call upon the European Commission to ensure that by mid-2024 the following steps are taken:

1. Requirements for cloud services that need a high level of assurance are available, and uniformly apply throughout the European Union,
2. All public administrations and providers of vital services are required to use cloud services that have a high level of assurance, dedicated for their sensitive data,
3. A grace-period for compliance with the legal requirements for security is granted for as long as no solutions with a trusted high level of assurance are freely available on the market within the European Union.

These steps would benefit:

- the integrity of the Digital Single Market,
- making available in the EU higher security levels in cloud technologies (Trusted Cloud) - especially for processing sensitive data,
- clearer specifications of requirements for providers to adhere to, so they can provide for compliant, secure and affordable solutions in the whole of Europe, and
- the possibility for businesses and public organisations to be compliant with the law, including NIS2 and GDPR.

We are of course available to provide the Commission with more elaborate insights into the experience we have in negotiating with providers or developing solutions that make our organizations compliant with security requirements.

We will send a copy of this letter to DG Connect, DG Trade, DG Grow and the Secretariat General of the European Commission, and publish it on our websites.

Yours sincerely,

C. Rapoport	**J.-C. Laroche**	**M. Koning**	**H.-J. Popp**
President	President	President	Vice-president
Beltug	Cigref	CIO Platform Nederland	VOICE e.V.

About our four associations
Beltug, Cigref, CIO Platform Nederland and VOICE are the Belgian, French, Dutch and German CIO-associations; the communities of Chief Information Officers (CIO's) and other senior leaders that are responsible for digital technologies and digital transformations within private or public organisations. Our members are European business users of digital technologies; they acquire, implement, and use digital technologies in practise. We do not represent IT-providers and consultants.