19 December 2017

CISPE Response to the public consultation on the draft Regulation proposal on a framework for the free flow of non-personal data in the EU

Introduction

CISPE would like to express its support for adopting such regulation which is very important for a truly integrated Digital Single Market. Removing restrictions to the flow of data across EU borders will greatly support spreading the benefits of the cloud to the European economy. In order to achieve that, it is necessary to adopt in parallel a harmonised level of data security across the EU.

CISPE also welcomes the measured approach in addressing data portability in the cloud and the encouragement in developing self-regulatory Union Codes of conduct, an area where CISPE has experience in[1]. When looking at the specificities of cloud computing, it is clear that customers embracing the cloud today are enjoying much more freedom and flexibility when choosing their underlying technology components than in the traditional IT environment and that the potential for "lock-in" is now significantly lower than it used. However, the envisaged dispositions do not seem to be operational in their current wording which lacks clarity.

Free flow of data principle

The cloud industry welcomes the general principle of free flow of data and reinforces the importance of banning national data localisation rules, which will provide legal certainty for cloud services providers and boost the European economy.

However, to maximise the benefits of cross border data flow, the final Regulation should limit cases when Member States will be able to localise non-personal data. That should happen only in very exceptional and pre-determined cases. While such cases have not yet been clearly identified (e.g. public safety or the definition of non-personal data), they should not be expansive such that they defeat the purpose of the Regulation.

1. Exceptions:

a) Public Security:

The Regulation states that grounds of 'public security' can constitute an exception to the rule of free flow of non-personal data. This term has not yet been defined in EU secondary legislation and therefore leaves room for a broad interpretation at national level.

The cloud industry suggests clarifying in a recital the meaning of public security in line with the following interpretation of the European Court of Justice:

- *'public security may not be invoked unless there is a genuine and sufficiently serious threat to a fundamental interest of society'*

[1] CISPE has developed the first sectorial data protection Code of conduct for Cloud infrastructure providers anticipating on the upcoming implementation of the GDPR.

Cloud Infrastructure Services Providers of Europe ('CISPE') ASBL
Rue Ernest Solvay 32, B – 1050 Brussels, Belgium EU Transparency Register: 041495920038-44
Website: www.cispe.cloud

b) Personal data vs non-personal data:

Non-personal data has not yet been defined in EU legislation. In certain cases, non-personal data has been defined as 'data other than personal' for instance while discussing the proposal for a Digital Content Directive. In this regard, the European Data Protection Supervisor (EDPS) provided a non-binding opinion on the notion of personal data:

'In the light of the broad definition of personal data under the GDPR, it is likely that almost all data provided by the consumer to the provider of the digital content will be considered as personal data'.

Therefore, since the definition of personal data is intentionally broad, consequently the scope of the free flow of data is limited and not clearly defined.

Additionally, under the GDPR, Member States may neither restrict nor prohibit the free movement of personal data within the Union for reasons connected with the protection of natural persons with regard to the processing of personal data. However, Members States can use any other derogations than data protection, for instance, fight against gambling addiction, patients' safety to localise data, which can also defeat the purpose of the free flow of data principle.

As it stands the draft Regulation's text does not recognise the complexity that arises of large volumes of data generated by machines and sensors that can include both personal and non-personal data. For example, smart building pilots today generate several million data points a day on energy, water and HVAC data where datasets often combine personal and non-personal data.

Understanding how consumers are using scarce resources such as water and energy is mission critical for scientists and engineers to develop sustainable solutions and efficient products. Trying to separate the two from these data sets create unnecessary burdens, often difficult or too costly, to unbundle such information.

In certain cases, non-personal data is bundled with personal data and it would not be technologically possible or economically reasonable to differentiate such data.

The cloud industry proposes to clarify the meaning of term "non-personal data" to avoid uncertainties in the implementation.

c) Public data

The proposed Regulation covers non-personal data in general. We believe that same principle should apply to non-personal public data. Otherwise, such an exception could again lead to uncertainties and arbitrary exceptions leading to overall fragmentation in the EU.

Removing public data from the scope risks incentivising public authorities to (i) insource their data storage and processing or (ii) not to outsource it at all. This could have the following consequences:

- Running storage facility might not provide access to the latest innovation-enabling technology.
- Hindering innovation as it does not allow SMEs to create a cloud ecosystem to offer services and products for the public authorities in the Member States.
- Cloud services will become less scalable and unable to respond to changes in demand.

Cloud Infrastructure Services Providers of Europe ('CISPE') ASBL
Rue Ernest Solvay 32, B – 1050 Brussels, Belgium EU Transparency Register: **041495920038-44**
Website: www.cispe.cloud

- Member States could unnecessarily increase capital expenditures and decrease operational efficiencies including weakening cybersecurity options.

The cloud industry suggests leaving public data in the scope of the Regulation.

2. On cloud lock-in/data portability

Customers are not locked in with the state of the art commercial cloud. Serious cloud providers offer a wide variety of different operating systems and programming languages from third parties to work with, giving their customers a great selection and making it easy to port whatever they have built on their infrastructure back in-house or onto another cloud platform.

Customers can choose from many different operating systems, which includes Windows, Ubuntu, CentOS, Debain and a number of other Linux variations. Serious cloud providers also offer their services with pay as you go pricing and no long-term commitments meaning if customers so choose they can move away from their infrastructure and stop paying whenever they like.

Each migration of data needs to be evaluated on a case-by-case basis since it depends on several factors such as the type of data, the connectivity to the cloud, the type of storage etc. For instance, migration is a shared responsibility with customers; and their interaction and resources play a key role when determining the timing of such migration.

The cloud industry welcomes the development of a self-regulatory code of conduct, which may entail model contract terms concerning data portability. Nevertheless, the one-year deadline for all data service providers to effectively implement these codes of conduct seems particularly short, considering the time that is usually needed for the drafting and approvals from data protection authorities.

The cloud industry suggests increasing the time to develop a code of conduct up to 2 years since it is a complex task.

3. Data availability for competent authorities (law enforcement access to data)

Users of data processing services (including Cloud Infrastructure Service Providers) cannot refuse to provide data access to national competent authorities on the grounds that the data is stored is another Member State, or because of contractual or technical reasons.

For instance, if the competent authorities in Italy are unable to access the data located in Germany (e.g. because the provider refuses), Italian authorities can request the assistance of the competent authorities in Germany. Competent authorities of EU Member States would have a legal obligation to help each other.

The cloud industry suggests introducing further clarification for the Regulation not apply to users "established in the Union" if the data is stored/processed outside the Union.

Additionally, there is not a clear framework with regards to non-personal data cooperation mechanisms and this can create a conflict of law where laws of one jurisdiction conflict with the laws of another. Clarity is needed in order to avoid conflicts of law.

Cloud Infrastructure Services Providers of Europe ('CISPE') ASBL
Rue Ernest Solvay 32, B – 1050 Brussels, Belgium EU Transparency Register: **041495920038-44**
Website: www.cispe.cloud

Conclusion

We trust that CISPE suggestions will be taken into consideration to ensure a proportionate approach to the free flow of non-personal data in Europe. CISPE stands ready to constructively engage with all stakeholders involved in this crucial piece of EU legislation.

About CISPE

CISPE brings together 22 Cloud infrastructure providers operating data centres in more that 15 European countries and including: Aruba (IT), GIGAS (ES) AWS (US), Daticum (BG), Dada (IT), Hetzner Online (DE), Ikoula (FR), Leaseweb (NL), OVH (FR), UpCloud (FI), SolidHost (NL), Seeweb (IT), Adenis (FR), IOM Cloud (UK), Lomaco (FR), eLogic (IT), Neurones (FR), Netalia (IT), IDS (FR), Outscale (FR), Serverplan (IT), Hot Potatoes (NL).

***

Cloud Infrastructure Services Providers of Europe ('CISPE') ASBL
Rue Ernest Solvay 32, B – 1050 Brussels, Belgium EU Transparency Register: **041495920038-44**
Website: www.cispe.cloud