DIGITALEUROPE

DIGITALEUROPE views on the Regulation on the Framework for the Free Flow of Non-Personal Data

Brussels, 8 December 2017

EXECUTIVE SUMMARY

DIGITALEUROPE, as the voice of Europe's digital technology industry, welcomes the general principle of free flow of data and reinforces the importance of banning national data localisation rules. This principle will provide legal certainty for companies, boost the European economy and herald new innovative technologies.

Recent studies show that data localisation reduces competition and increases storage costs with up to 120% for companies and consumers. If existing data localising measures are removed, GDP gains are estimated to up to 8 billion euros per year (up to 0.06% of GDP), which is on par with the gains of recent free trade agreements (FTAs) concluded by the EU.[1] This Regulation represent an opportunity not to be missed.

However, to maximise the benefits of cross border dataflows, the scope should not be narrowed. In our opinion, Member States should be able to localise non-personal data in only exceptional cases. Any limiting the scope and widening the exemptions will risk defeating the purpose of the Regulation.

DIGITALEUROPE believes any future actions by policy makers should take into consideration the following:

1. ARTICLE 2 – SCOPE

The general principle of free flow of data could be undermined by limiting the scope and widening the exemptions.

Public and private data

The Regulation proposed by the Commission covers non-personal data in general. DIGITALEUROPE support this scope and firmly believes this includes non-personal public data.

As public institutions adopt cloud, they lower the tax burden for their operations, bring more efficiencies to their internal work processes, and improve constituent interactions by offering e-governance solutions.
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:

1 ECIPE study: http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

- Running your storage facility might not give you 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 Government.
- Cloud services become less scalable and unable to respond to changes in demand.
- Member States could unnecessarily increase capital expenditures and decrease operational efficiencies including weakening cybersecurity options. Leading public servants to maintain their own infrastructure and services instead of dedicating time to create further value to customers/citizens.

Personal data versus non-personal data

The interplay between this regulation and the GDPR needs to be clarified, particularly with regards to mixed data sets. While we do agree with the GDPR taking precedence on the personal part of mixed datasets, it can place companies in a difficult situation where mixed datasets are technically and/or economically impossible to unbundle.

2. ARTICLE 3 - DEFINITIONS

The definition of "data localisation requirement" covers laws and administrative provisions of the Member States, but it is not clear if laws and other rules adopted by regional or local authorities are also covered. To avoid fragmentation when the regulation is implemented and enforced it should be clarified that this also includes laws and administrative provisions at regional and local level.when the regulation is implemented and enforced it should be clarified that this also includes laws and administrative provisions at regional and local level.

This is important in the context of public procurement rules. It would be welcomed if the text clarified that public procurement rules and practises are covered.

3. ARTICLE 4 - FREE MOVEMENT OF DATA ACROSS BORDERS WITHIN THE UNION

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 been defined in EU secondary legislation.

The public security exception should not be broadened, or lead to any uncertainty in interpretation as to which data localisation measures could be justified on public security grounds. We seek clarification in a recital with regards to the meaning of public security in line with the interpretation of the European Court of Justice.[2]

2 http://ec.europa.eu/transparency/regdoc/rep/2/2017/EN/SEC-2017-392-3-EN-MAIN-PART-1.PDF

Regarding the oversight mechanism, it is not clear if the Commission has the power to block a draft act which it considers to be unjustified. In the case of data localisation, a notification procedure should be extremely robust and give clear blocking powers to the Commission in order to be effective. DIGITALEUROPE fully supports transparency obligations on Member States regarding justified data localisation measures.

4. ARTICLE 5 - DATA AVAILABILITY FOR REGULATORY CONTROL BY COMPETENT AUTHORITIES

DIGITAL EUROPE supports to leave the 'competent' authorities' powers to access, inspect, control and audit. Public authorities should be able to carry out regulatory control as if the data was stored on their territory. It is important that the scope of this provision is not broadened beyond access for regulatory control and that such controls take place without prejudice to existing legal obligations. There is not a clear framework with regards to non-personal data cooperation mechanisms and this can create a conflict of law between territorial jurisdictions. Clarity is needed in order to avoid conflicts of law among different member states.

5. ARTICLE 6 - PORTING OF DATA

DIGITAL EUROPE supports the development of self-regulatory codes of conduct to facilitate the switching of providers and porting of data. As confirmed by the Regulatory Scrutiny Board there is not enough evidence to regulate in this field.[3] As the porting of data is agreed in business-to-business (B2B) contracts, regulating this area would interfere with contractual freedom.

The one-year deadline for all data service providers to effectively implement these codes of conduct is too short. More time will be needed to ensure all stakeholders are involved and to achieve a robust and future-proof result. Therefore, we suggest a more realistic timeframe.

CONCLUSION

DIGITALEUROPE supports the European Commission proposal. It is of the utmost importance that every effort is made to guarantee the free flow of data, which is a vital source of innovation, growth and jobs. Our members and national trade associations stand ready to discuss this topic with the co- legislators. We invite the European Commission, the Parliament and the Council of the EU to maintain their support for the principle of the free flow of data without limiting the scope or extending the exemptions.

For more information please contact:

Ray Pinto, DIGITALEUROPE Policy Director
+32.472.55.8402 or ray.pinto@digitaleurope.org

3 Only 35 respondents (26,9%) were dissatisfied or very dissatisfied with the current conditions for data portability.

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK