Free Flow of Data is at the essence of a true European Digital Single Market

Digitalisation can be at the heart of Europe

The undersigned organisations strongly believe the EU should complete the Digital Single Market (DSM) in a timely manner by ensuring the **free movement of data** so as to take full advantage of the digital transformation and compete effectively worldwide. The data economy is paving the way for the ongoing digital transformation. Its evolution can significantly improve lives, create growth and jobs, and benefit society overall.

Data has the potential to be worth EUR 566 billion by 2020 (European Commission). If harnessed appropriately, this economic lever will fuel growth in Europe. Europe needs to adopt an innovation-friendly approach to data to empower the digitalisation process and offer robust solutions for data use. Policy makers should carefully assess if and where action is needed. The European legislative framework for data must allow companies to compete globally, foster the creation of new business models and ensure a level playing field, with legal certainty and stability.

Companies in Europe are already facing various data localisation restrictions (see examples at annex), which may be likely to increase in the future in absence of EU action. In addition, there are many other indirect, non-legislative barriers that stifle free movement of data further (for example localisation requirements in public procurement). The European Business community believes that **the EU should put forward legislation to remove and prevent unjustified restrictions to the free flow of data**, as announced in the 2015 DSM Strategy. The ability to transfer data across borders is crucial for companies, both within the Single Market and beyond. Companies need to be able to efficiently transfer data across borders in order to respond to customers' need, deliver goods and services, process payments or provide technical support.

Imposing direct or indirect restrictions on the location of data limiting the possibility of data flowing across borders without objective and justified reasons would undermine the ability of companies to define their business models and stifle Europe's competitiveness and growth.

We strongly recommend avoiding any forced data localisation requirements on a national, European or global scale. These requirements in most cases find no valid justification, as under a true DSM there is little justification to deem data safer or better accessible by default if stored in a specific Member State, as the physical location where the data is stored does not seem to have much relevance anymore.

Any forced data localisation requirements should be subject to EU scrutiny and should only be kept if proportionate and in line with EU legislation and single market principles. **The EU should introduce a legal instrument that removes existing national data localisation requirements and prevents the creation of new ones.**

As regards data ownership, access and liability, we believe that these issues are – for the time being - adequately addressed by existing legislation. Current rules and practices allow adapting to the needs of the parties and provide the appropriate setting to share data based on contractual terms, allowing innovation. The current framework is fit to address liability issues in the field of IoT and **no new liability rules for data-related services and products are needed**.

List of examples of current data localisation requirements in Europe[i]

MS	Act/Practice	Description
UK	Companies Act 2006 - Art. 388	*According to the Companies Act 2006, "if accounting records are kept at a place outside the UK, accounts and returns (...) must be sent to, and kept at, a place in the UK, and must at all times be open to such inspection".*
UK	NHS information governance rules	*In the UK, there are no legal prohibitions on exporting NHS patient data outside the country. However, the NHS and associated institutions are bound by strong legal, ethical and regulatory obligations of confidentiality. The location outside the UK of the data recipient is considered a risk factor by the NHS information governance rules and therefore might result in data localisation.*
SW	Local storage requirement	*The Financial Services Authority requires 'immediate' access to data in its market supervision which, according to business, the supervisory body interprets as been given physical access to servers. Accordingly, Swedish financial services providers are de facto required to maintain all their records inside Swedish jurisdiction.*
SW	Local storage requirement	*In relation to specific government authorities, there are certain provisions which might require the data processed by the authority to be held within SW or within the authority. This might affect the supply of cloud computing to public authorities.*
SW	Swedish Accounting Act (BokfÃringslag (1999:1078))	*In SW, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in SW for a period of 7 years.*
LUX	Circ. CSSF 12/552 as amended by Circs. CSSF 13/563 and 14/597	*According to Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.*
DK	Consolidated Act No. 528/2000 as changed by Act No. 201/2001 (Executive Order on Security)	*Since 2011, the Danish DPA has ruled in several cases against processing of local authorities' data in third countries without using standard contractual clauses. This is the result of a strict interpretation of the European Directive 95/46/EC. Therefore, services such as Dropbox, Google Apps and Microsoft's Office 365 cannot be used by local authorities unless they have signed an agreement with the processor based on standard contractual clauses.*
SI	Slovenian Personal Data Protection Act	*In Slovenia, transfers of personal data to non-EEA and non-whitelist countries require the approval of the Commissioner. The approval is issued if the Commissioner establishes that a sufficient level of protection is ensured for the transferring of personal data respectively for the data subjects to which this data relates.*
RO	Data protection Law	*In Romania, any outbound transfer of personal data requires prior notification to the National DPA. Moreover, any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.*
RO	Law no. 124/2015, approval of GVT Emergency Ordinance no. 92/2014 regulating fiscal measures	*In Romania, the game server must store all data related to remote gambling services provision, including records and identification of players, stakes placed and winnings. Information must be stored using data storage equipment situated in Romania.*
PT	Data protection law	*In Portugal, all transfer of data outside the EU must be notified and authorized by the relevant Commission, except when directed to whitelisted countries or when using model contract. In 2015 the Portuguese DPA also issued specific guidelines on Intra-Group Agreements ("IGA") involving personal data transfers to non-EEA countries. The DPA considers that such transfers depend on its prior authorisation for the purposes of assessing if IGAs contain sufficient guarantees that the personal data transferred continues to benefit from the same level of protection as in the EEA countries.*
PL	Polish Gambling Act	*According to the Polish Gambling Act, any entity organizing gambling activities is obliged to archive in real time all data exchanged between such entity and the users in an archive device located in Poland.* *Another restriction is the requirement that the equipment (servers) for processing and storing information and data regarding the bets and their participants must be installed and kept on the territory of a member state of the EU or EFTA.*
NL	Public Records Act	*Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records.*

IT	Presidential Decree No. 633 of 1972	*Article 39 of the Presidential Decree no. 633 of 1972 states state electric archives related to accounting data for VAT declarations might be kept in a foreign country only if some kind of convention has been concluded between Italy and the receiving country governing the exchange of information in the field of direct taxation. Therefore, such limitation does not apply intra-EU.*
GR	National law 3917/2011	*In Greece, the Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later annulled by the European Court of Justice) by requiring that retained data on traffic and localisation stay within the premises of the Hellenic territory. The Law is still in force.*
DE	German Telecommunications Act, as amended in December 2015	*In October 2015 Germany adopted a new data retention law (entering into force in 2017), replacing the previous law implementing the Data Retention Directive that was declared invalid by the EUCJ In 2014. The new law provides that telecoms providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either 4 or 10 weeks. The data is to be stored in servers located within Germany (Â§113b).*
DE	German Commercial Code – Sect. 257 No. 1, 4 - (Handelsgesetzbuch Â§ 257)	*According to the German Commercial Code, accounting documents and business letters must be stored in Germany.*
DE	Tax Code - Section 146(2) (Abgabenordnung)	*Under the Tax Code, all persons and companies liable to pay taxes that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.*
DE	VAT Act - Section 14b (Umsatzsteuergesetz, UStG)	*The Act on Value Added Tax states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electric storage, they may be stored within the territory of the EU if full online access and the possibility of download are guaranteed. In this case, the entity is obliged to notify the competent tax authority in writing of the location of the electronically stored invoices, and the tax authority may access and download the data.*
DE	Ban to transfer	*There is no European prohibition of data transfer, neither has any EU Member State implemented a national prohibition of data transfer. However, the data protection authority (DPA) at the German federal state of Schleswig Holstein has declared in a position paper that all data protection instruments for the transfer of data to the US after the EUCJ Schrems v Facebook judgment are going to be illegal. The DPA it has not taken any action in this regard, but has threatened to do so.*
FR	Decree 2012-436 amending Electronic Comms Code	*Through a decree amending the Code of Electronic Communications, France has included a territorial restriction requiring that the systems for interception of electronic communications must be established in France.*
FR	Ministerial circular on cloud computing 5 April 2016[ii]	*On public procurement states that it is illegal to use a non-"sovereign" cloud for data produced by public (national and local) administration: all data from public administrations have to be considered as archives and therefore stored and processed in France.*
FIN	Accounting Act (1336/1997)	*The Accounting Act requires that a copy of the accounting records in kept within Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed.*
BG	Gambling Act	*In Bulgaria, an applicant for a gaming license must assure that all data related to operations in Bulgaria is stored on a server located in the territory of Bulgaria. Moreover, the applicant has to assure that the communication equipment and the central computer system of the organizer are located within the EEA or in Switzerland.*

*** * ***

[i] The Digital Trade Estimates (DTE) database, European Centre for International Political Economy (ECIPE)
[ii] http://circulaires.legifrance.gouv.fr