TRANSATLANTIC DIVERGENCE IN PRIVACY PROTECTION: Policy and economics in the regulation of data flows

The EU's position on data privacy has long been more conservative than other countries'. As the divergence grows so does the risk that restrictions on data flows will stifle cross-border trade and innovation in the EU.

The regulation of transfers of personal data

Since 1995, under the Data Protection Directive, the EU has allowed the transfer of personal data within the EU, but permitted the transfer of data out of the EU only to those other countries that provide - essentially – an equivalent level of protection. Only a small number of countries have been recognised as providing equivalent protection including Israel, New Zealand and Switzerland.[1] Importantly, the US is not among them.

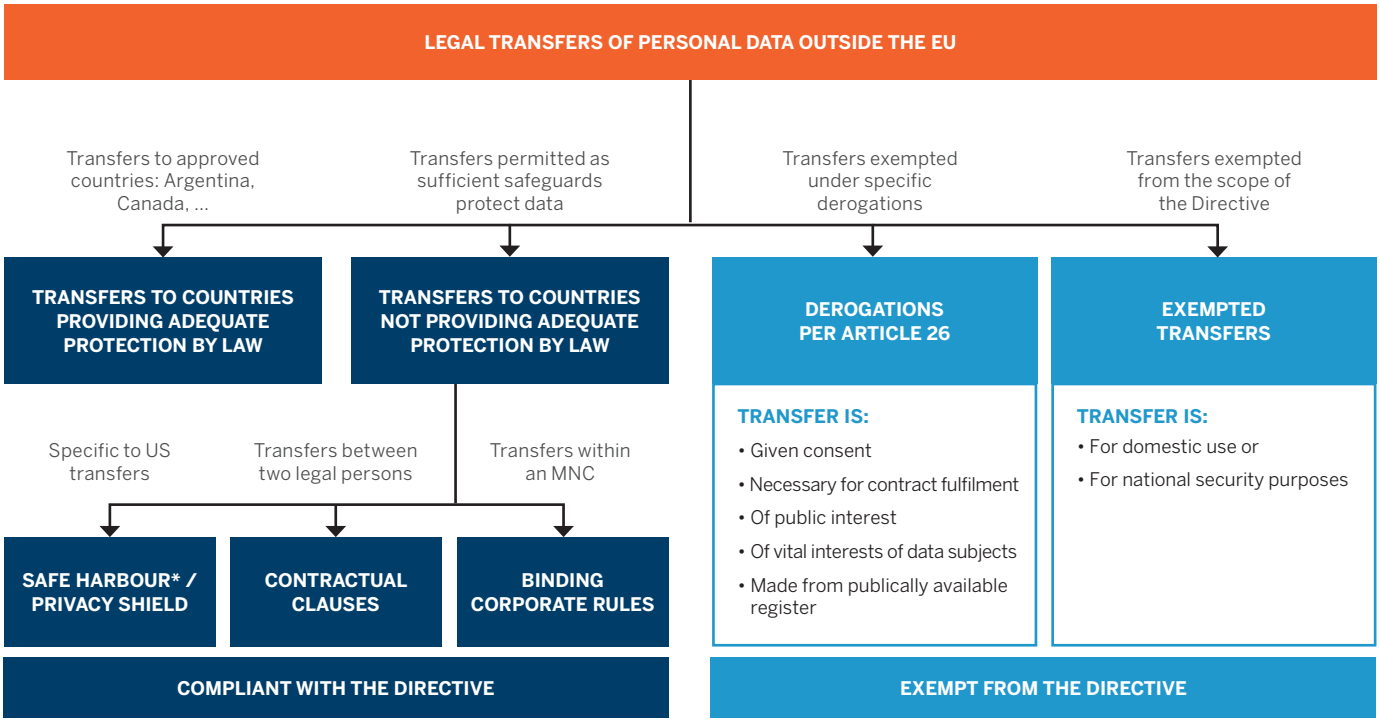
Transfers of personal data between the EU and the US were, however, covered by the Safe Harbour agreement, until October 2015, when the European Court of Justice ("ECJ") ruled that the agreement was inadequate – in particular in not providing, for EU citizens, the possibility of legal redress, in the event of any breaches in the US of the security arrangements covering their personal data.

The ECJ's investigation was initially triggered by a complaint made by Maximillian Schrems, an Austrian student. Mr Schrems claimed, following the Snowden revelations, that the EU-US Safe Harbour agreement could not provide adequate protection to EU citizens for any personal data transferred to the US. Following success at the ECJ, Mr Schrems has subsequently requested the Irish, Belgian and German data protection authorities ("DPAs") to investigate the other legal bases under which the transfers of personal data between the EU and the US are permitted.

The other legal bases are known as Contractual Clauses and Binding Corporate Rules - the latter applies, for example, to transfers of personal data within multi-national corporate entities. The concern is that these bases may also be found to be legally inadequate. If so, the economic consequences – for any company that transfers personal data across the Atlantic or indeed to any non-equivalent country, and for society more widely - could be far reaching.

1 For the full list, see the European Commission's website, ec.europa.eu/justice/data-protection/international-transfers/adequacy

The legal mechanisms by which the transfer of personal data outside the EU is permitted



Note: * Safe Harbour was declared invalid by the ECJ on 6 October 2015 and has been replaced by the Privacy Shield.

Under the Safe Harbour agreement companies could self-certify with 7 principles (including notice, choice and security) which had been jointly developed by the EC and the US Department of Commerce to safeguard the personal data of EU citizens. Between 2000 and 2016 more than 5,000 companies from over 100 different industries self-certified under the agreement.

Organisations also used Custom or Standard Contractual Clauses ("CCCs" or "SCCs") in a binding contract between the transferor and the transferee covering the responsibilities and rights of each and providing a legal remedy if those rights were breached. The EC has drafted SCCs which it deems sufficient to protect personal data. Although there is no central registry of companies using SCCs it is widely understood that thousands of companies rely on this mechanism.[2]

Finally, Binding Corporate Rules ("BCRs") are rules incorporated into the governing documents of multi-national corporations ("MNCs") allowing them to transfer personal data between subsidiaries in any country. The process to confirm a BCR is lengthy, and imposes strict conditions on companies, such as the need for the entire group to undertake comprehensive data protection audits.[3] As such, BCRs are only an option for the largest and most sophisticated companies (examples being. in finance ABN AMRO, in pharmaceuticals Astra Zeneca, or in heavy industry, Airbus.

Impacts are driven by the nature of transfers

A variety of types of organisations transfer personal data between the EU and the US. These include businesses, non-profits, educational institutions, public authorities, professional societies and charities. The majority of available evidence concerning the use of personal data relates to for-profit businesses since they disclose this information on the Safe Harbour list[4] or on their own websites.

The four key types of business activities which involve personal data transfers between the EU and the US are:

1. **Provision of services to consumers (business to consumer)**

   At its simplest, US based businesses utilise personal data - such as name, address and payment details - to deliver goods and services to EU consumers. They also analyse personal data in order to tailor and improve their services.

   For some US businesses, the analysis of personal data is a core service offering. For example, 23&Me is a personal genomics company which analyses customers' saliva samples to provide information on their inherited conditions, drug responses, genetic risk factors and traits. These types of offerings are increasing with the rise in connected devices (for example, wearable fitness bands).

2 Financial Times (25 May 2016), Ireland warns on Big Tech's data rules
3 Strategic Risk (1 January 2015), Is your business ready for the Data Protection Regulation?
4 safeharbor.export.gov/list.aspx

At the end of the spectrum, online platforms including social networking sites and internet service providers offer the opportunity to EU and US based consumers to store and exchange personal data.

2. **Provision of services to businesses (business to business)**

   EU companies may outsource functions to US based service providers: e.g. marketing and advertising, human resource activities and IT support. For all these activities they may need to disclose personal data associated with their customers or employees. Increasingly, businesses rely on cloud computing services which provide storage for, and often also analysis of, their data.

   Amazon Web Services ("AWS") is one of the largest providers of cloud computing services. AWS protects personal data by allowing customers to choose from its datacentres located in different regions. AWS will not move the data outside of the chosen region.

3. **Internal transfer of personal data within an MNC**

   MNCs often centralise certain support functions such as payroll, employee performance assessment, customer analytics, IT support, etc. If the support is carried out from the US and the MNC has offices in the EU, then this will almost certainly involve the transfer of personal data from the EU to the US.

4. **Compliance with governmental, legislative and regulatory bodies**

   Companies may also need to transfer the personal data of their employees, customers, suppliers and other business contacts to US authorities to comply with governmental, legislative and regulatory requirements. It is not always clear whether these types of transfer are exempted from the scope of the Data Protection Directive.

The scale of potential economic impacts

A complete removal of the legal protection otherwise available for transatlantic transfers of personal data could cause significant disruptions in EU-US business relationships. The Data Protection Directive, which uses generic and broad definitions, creates a great deal of ambiguity as to which activities fall under its scope. The EC itself notes that "*there is currently no strong mechanism to ensure a harmonised interpretation of the Directive*".[5]

In this environment it is likely that more rather than fewer parties will feel exposed. Some entities may conclude that the benefits of continued data transfers outweigh the potential legal costs of non-compliance. Some, however, may conclude that it is necessary to avoid any transfers involving personal data of EU citizens between the EU and the US (by localising all data processing activities). Data localisation would be a costly solution, requiring the replication of relevant functions and services within the EU in order to avoid sending any personal data abroad. Some companies, especially SMEs, will lack the necessary legal and financial resources, and may therefore exit (or not enter) the EU market.

Reduction in US exports to the EU

Very few studies have sought to quantify the economic consequences of data localisation. It is reasonable to expect that the direct consequence of these actions would be a reduction in US exports to the EU, both of goods and services. The EU and the US are each other's main trading partners: in 2014, the EU exported to the US over €500 billion in goods and services, and imported, from the US, some €400 billion.[6]

The European Centre for International Political Economy ("ECIPE") estimated that a requirement for US exporters to acquire data processing capacities inside the EU would reduce US services exports to the EU by 17-24%.[7]

Reduction in EU exports to the US

This, in turn, would lead to lower choice and higher prices for EU consumers, and higher input costs for EU businesses (data processing within the EU could be 25-35% costlier than in the US).[8]

If firms start facing higher costs, their ability to produce at competitive prices could be affected. ECIPE estimated that, in the absence of legal protection to EU-US personal data transfers, exports of services from the EU to the US could decrease by 5-7%, and exports of goods could decrease by 7-9%.[9]

Productivity, innovation and growth

Productivity, innovation and growth would also be affected. The global economy is increasingly data-driven and any restriction on data flows could impact the way firms are able to innovate and grow.

According to the OECD "*more connected countries learn from the global productivity frontier more effectively and get a resultant boost in their own productivity growth*".[10]

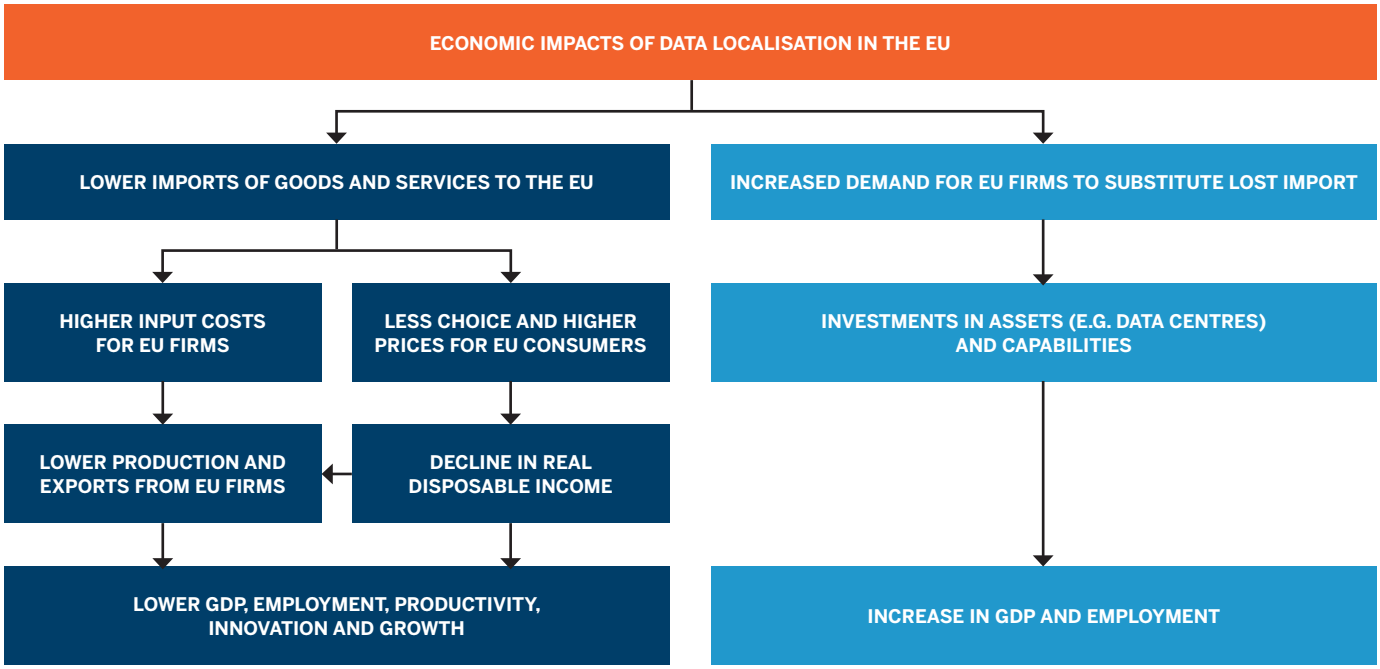
Benefits from protection of privacy

Data localisation would also, of course, have some economic benefits (besides the expected benefits of stronger protection of personal data). Part of the demand for the goods and services that are currently supplied from the US - and rely on the transfer of personal data on EU citizens - would shift to EU businesses. On balance, however, it is likely that the impact would be overwhelmingly negative, at least in the short term.

5 http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

6 ec.europa.eu/trade/policy/countries-and-regions/countries/united-states
7 ECIPE, 2013, the Economic Importance of Getting Data Protection right
8 Ibid
9 Ibid
10 OECD, 2016, Economic and social benefits of internet openness

Economic impact of data localisation on the EU economy



Conclusion

If the result of increasing EU regulation over the transfer of personal data were increasing data localisation, the impact would be unambiguously adverse, and likely to be significantly so. The question that arises is whether the benefits of increased privacy for EU citizens are likely to outweigh these economic costs. This is partly a question of the value that Europeans attach to privacy (including, for example, to the "*right to be forgotten*").

The relative weight of each effect is unclear: the European Commission ("EC") appears to attribute, to some extent, the low share of cross-border e-commerce – within the EU - to EU citizens' lack of trust in online services. The EC expects that stronger data protection rules will build Europeans' confidence in e-commerce, thereby unlocking "*€415 billion additional growth and hundreds of thousands of new jobs*".[11]

According to Eurostat, however, online shopping is popular in the EU.[12] But 54% of online trade comes from US-based online services; and just 4% from EU cross-border sales.[13] It may be the case that cross-border e-commerce within the EU is hindered, rather than helped, by regional and national rules and regulations; and it is their complexity, rather than privacy concerns, that constrains online cross-border trade within the EU.

If so, the apparent strengthening in the regulation of data transfers by the EU is likely to have unambiguously adverse economic consequences, and not just in the short term. The five largest companies by market capitalisation in the world (Apple, Alphabet, Microsoft, Amazon and Facebook) are now data-driven, and they are all US-based. The possibility of an EU company joining their ranks may be receding.

11 EC, 2015, Stronger data protection rules for Europe

12 Eurostat, E-commerce statistics
13 EC,DSM Factsheet

FTI CONSULTING™

Dora Grunwald
Managing Director
+ 44 20 3727 1217
dora.grunwald@fticonsulting.com

EXPERTS WITH IMPACT