ECIPE EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY
BULLETIN

ECIPE Bulletin No. 5/2015

The Bundes Cloud: Germany on the Edge to Discriminate Against Foreign Suppliers of Digital Services

by Matthias Bauer (matthias.bauer@ecipe.org) and Hosuk Lee-Makiyama (hosuk.lee-makiyama@ecipe.org) - respectively, *Senior Economist* and *Director* at ECIPE

Germany is increasingly accused of being engaged in a digital protectionism, and commandeering the rest of Europe into policies aimed at 'information sovereignty' and counter the threat of the data-driven 'Industrie 4.0'. While the politically important German telecom and publishing sector openly argue for a 'data Schengen' that would effectively push US competition out of Germany or Europe, the government has been more cautious, preferring to talk in ambiguous terms – not least because German exporters face such barriers overseas.

Adam Smith said that the road to certainty passes through the valley of ambiguity – Germany's stance on cross-border data flows is no exception. The federal government has just adopted a set of guidelines aiming to increase the 'flexibility and security' of its government-run IT systems. Germany's 200 or so different government agencies run 1,300 data services centres, causing functional overlap and economic inefficiencies. The new proposal, drafted by Germany's interior ministry, advocates the consolidation of government-run IT systems and IT services centres.

So far, this is in good order. Efficiency and order – sound like good governance that we come to expect. However, the proposal is accompanied by a far-reaching move towards data localisation: for external cloud and software services to be purchased by Germany's public authorities the government's new guidelines (Resolution 2015/5 of the federal governments IT Council) stipulate that *sensitive* information (including government secrets and infrastructure information) have to be stored on servers *within* Germany. In addition, all suppliers of cloud and software services must guarantee that such information will not become subject to any disclosure obligation in foreign jurisdictions such as the United States.

The last nail in the coffin

At first sight, such requirements may sound reasonable in the post-Snowden environment; NSA was after all listening into the Chancellor's phone calls. Also, a serious attack on the IT systems of the Bundestag caused parliamentarians to question government agencies' cyber security competences.

But such notions are built on a very common misconception that data security is a function of where the data is physically located. In contrary, centralising data in one country increases both the potential risk, but also the scale of the damage that hackers can cause. This is why the native tech industry in Europe advocates against such localisation policies. Data is not more secure because its IP address is in Germany, as it is accessible from any location in any case. It is simply the old saying about laying all the eggs in one basket.

But what is aimed at just public institutions will inarguably spill over to the private markets as well. Government employees use same type of business software to draft their documents as common folks; government payroll and planning run on enterprise applications used in private businesses. Excluding certain vendors from government purchases will affect the profitability of these firms, and whether they continue to

be present on the German market at all. The new proposal is an effective message to major vendors of software, storage and processing services: either to head for Germany or – *bitte* – leave.

It probably goes without saying but the issue is not necessarily about imposing security requirements or imposing German law on federal data. The problem is *how* it is being done.

Firstly, many countries (including the United States), determine where government data can be placed on a case-by-case basis. Unlike what is aimed for by Germany, government data is usually heavily decentralised, which allows for proportionate measures taken by each authority and each case. Not all data held by public authorities is indispensable to Germany's national security, which brings the danger of arbitrariness on the part of the government and discrimination of foreign suppliers. If the German government centralises its servers, and thereby extends the localisation requirement through bundling sensitive information with other data, it may find itself in violation of its WTO commitments.

Secondly, Germany imposes its law unilaterally on its data, i.e. independent from foreign jurisdictions and international law. Rather than tackling the issue directly with the culprit – the US government that unfairly exercises jurisdiction over its tech firms – the new German proposal is designed to make sure that German and US industry will be caught in the middle. You can only abide by one law, not both. Germany only cemented the precedence for, say, US, Chinese or Russian governments, to claim jurisdiction against German tech firms on more arbitrary grounds. To continue with old proverbs: Germany did not cast the first stone, but it most likely hammered the last nail in the coffin.

Rather than fighting fire with fire by prosecuting business, Germany should exercise its moral higher ground to force other governments into a system built on mutual legal assistance – where governments are held accountable for their laws, not firms who try to abide by them. But it seems as the imperative of *look*ing tough took priority over *being* effective.

In the long term

Many private firms increasingly or exclusively rely on cloud-based storage and data processing. According to a recent Eurostat survey, 19 per cent of European firms used cloud computing in 2014, primarily for email hosting and storage services. 46 per cent of those companies used advanced cloud services including financial and accounting software applications, customer relationship management and other business applications.

In general, a government-imposed limitation of vendor choices artificially restricts competition, incurs higher cost and prevents innovative business models from gaining ground and scale. Accordingly, data localisation destroys well-functioning digital business models, increases the risk of successful attacks due to data concentration, and undermines the international competitiveness of digital and traditional exporters – all of which is at the detriment of the German economy.