Mar 03, 2022

Dear Colleagues,

Government Relations Germany has published a comment piece in the German daily digital-policy newsletter “Tagesspiegel Background”. Please find the translated version below.

Best,
Jörg

Digital sovereignty in practice – a plea for a multi-cloud approach

For businesses and government agencies to operate with sovereignty in the digital space, certain requirements must be met, writes Jörg-Alexander Albrecht. Among other things, cloud diversity and complete portability of applications and content are needed. There is political tailwind through the Data Act, he adds.

Digital sovereignty, multi-cloud, interoperability – data policy discussions around these terms are always at risk to become debates between experts. Yet, these are simple principles that are directly useful for many users, whether private companies or public agencies.

Digital sovereignty is essentially about being able to act in a self-determined manner in the digital space. This requires choice, transparency and control over one's own data. VMware is already implementing these principles in the cloud. Our answer is a "cloud smart" approach that makes several cloud offerings interoperable with each other and thus provides a multi-cloud solution.

Connecting different clouds with each other

In this way, the right combination can be selected depending on requirements, be it a private cloud run on the company's own data center, one or more public clouds from international or local providers, or a mixture. Which cloud is most suitable depends on how sensitive the data is and what protection requirements are needed. In addition, the decisive factor is how much the cloud service should scale and how sustainable it should be. This approach is thus also in line with the planned multi-cloud strategy in public administration.

Sometimes digital sovereignty is equated with the broad use of Open-Source software. However, for a successful multi-cloud scenario, it is more crucial to implement open standards than to prescribe Open-Source. Open standards enable seamless data portability, reversibility, interoperability and the use of whichever solution is appropriate, be it open source or proprietary.

Behind the term interoperability is a principle that companies already take for granted. A simple example: companies may use different payroll systems, but the social security and tax data is reported and processed via a uniform interface.

Interoperability in the Data Act

This principle of interoperability implemented there could also be applied to many other cases with the European Data Act. At the very least, the Act should make it possible for companies to retrieve the data stored with providers and, if necessary, take it with them when they switch providers. The Data Act provides customers in the European Union with the right to change their provider while maintaining "functional equivalence".

Behind this unwieldy term lies nothing less than a uniform protocol that makes it possible, for example, to switch from one cloud service to another. This is not just about storing data, but

also about applications operated via the cloud structure. These are often the real reason for the so-called "lock-in" effects, i.e. harmful dependencies on a single provider without the possibility to switch easily.

This is very important, however, because companies and public authorities often have requirements to reduce dependency on individual providers, increase fail-safety and connect different systems with each other (think of the many specialized procedures in public administration that have to be connected as part of the implementation of the Online Access Act).

We are very pleased that this approach now enjoys political backing, as it democratizes the benefits of interoperability, strengthens customer rights, and thus improves market access.

Principles for digital sovereignty

Against this backdrop, the following five points are crucial if we are to achieve true interoperability and make cloud services permanently accessible to all.

1. **Full portability of data and applications**: This includes being able to migrate between public and various privately offered cloud services.

2. **Commitment to open standards**: If we already think about the handling of data from the consumer's point of view, we should also do the same for technological solutions to avoid dependence on individual solutions and lock-in effects.

3. **A better distribution of data and commitment to cloud diversity**: Applications will be less susceptible to serious failures if they (can) use different cloud services.

4. **Control over cloud data**: Especially for public data, local regulations, verifiable confidentiality measures and tightly controlled access are critical.

5. **Inclusion of local community data services and functions**: In addition to legally secure protection for sensitive data, local cloud providers make an important contribution to local value creation.