euritas
European Association of Public IT Service Providers

EURITAS SUMMIT 2021 – Executive Summary

Ensuring Digital Sovereignty of European Governments

On 30th September 2021 Euritas – the European Association of Public IT Service Providers – hosted the third edition of the Euritas Summit in Brussels to discuss the challenges of digital sovereignty of European Governments. Representatives from public authorities (EU, national and regional), from public IT service providers, and digital experts gathered to discuss possible ways to reduce the dependence of many public administrations in Europe on software products from a small number of companies.

The Summit was opened with a keynote address of EU Commissioner for Budget and Administration Johannes Hahn who stated that after more than 20 years of voluntary cooperation regarding EU government interoperability, the Commission finally has to establish a mandatory framework to enable interoperability by design and default.

High-ranking speakers debated digital sovereignty in three panels, each with a different focus:

- European Cloud Strategies and Services
- Open Source as an Enabler for Digital Sovereignty
- Cyber Security

Cloud Strategies and Services

Pierre Chastanet, Head of Unit, Cloud & Software, DG CONNECT, European Commission
Ernst Stöckl-Puckall, Head of Unit Digitization and Industry 4.0, German Federal Ministry for Economic Affairs and Energy, Germany
Herald Jongen, Partner, Greenberg Traurig, the Netherlands
David Vannozzi, CEO of Cineca, Italy

The aim of this panel was to look at the current cloud market situation of public services and to discuss possible concepts to guarantee the safety of public administration’s data in the cloud and the necessary standards to guarantee that cloud services meet these demands.

Europe is fully aware of the market situation and is preparing actions

In the cloud market, the US and Chinese players are dominant: 75 % of public cloud services are operated by five major providers from these two countries. From the European point of view "the pie" is getting bigger, but "the slice" of European providers is getting smaller, which is a worrying trend.

In this market, European public administrations and private companies cannot find the services they want in terms of data protection and the ability to switch between providers.

The European Alliance for Industrial Data, Edge and Cloud will help public administration bodies that process sensitive categories of data in buying these services. Opportunities for European service providers are the growing SaaS market, edge computing, telecom network and cloud native, 5G, industrial IoT, B2B applications: The EU Commission will facilitate coordinated investments for cloud and edge computing.

While providers prefer to operate "one size fits all"-solutions, tailored solutions are required. 750 billion euros are being invested in digital development, and the EU member states have an interest to use cloud services. There is a clear need to combine intelligently both resources and interconnecting services. The EU Commission is currently working on a Cloud Rule Book to provide a procurement framework for trusted cloud services.

Gaia-X as part of the European cloud strategy

The proprietary age of cloud services is coming to an end, and we need a new system of trust and value for a flexible value chain. Gaia-X should be a data ecosystem with transparency and interoperability, defining standards for data exchange in specific data spaces. GAIA X (300 members) is meant to create open data space for European countries, as well as countries world-wide.

How to negotiate with large cloud suppliers

Negotiating with large cloud suppliers such as Microsoft, Amazon and Google who dictate services, prices, terms and conditions is difficult. Leverage can be found by consolidating negotiation power and focussing on specific items.

Some lessons learnt from negotiations and consulting the Dutch and the Austrian governments are:

- Always be and stay in control
    - control the agenda, control the locations
    - always be on guard – mind the 5 D’s (Delay, Deflect, Deny, Disinform, Divide)
- Let the supplier bring the right team

    decision makers, NO pure sales, a negotiator, NO dial in/video conference (COVID permitting)

Public IT service providers stay in control of their data

Public IT service providers can provide the secure management of data. Specifically in the healthcare sector, the control of technologies like Big Data and AI in European rule based environments is extremely important.

An example is the Leonardo project of Cineca in Italy. The core of the project is the aggregation of health data at a national level - from laboratory data to the genetic profile of individual patients -, applying the highest standards in terms of cybersecurity and real-time active protection for targeted public health interventions and precision medicine. The newly-created infrastructure allows the clustering of patients’ profiles and the identification of targeted therapeutic indications through secure cloud services, which are available to healthcare facilities throughout the country.

The infrastructure uses the supercomputing (150 nodes for a power of 5 petaflops) and cloud (with a power of 20 petabytes distributed over 1,500 hard drives) capabilities of Leonardo’s Davinci-1 HPC and Dompé's Exscalate molecular library.

Open Source as an Enabler of Digital Transformation

Gawain MacMillan, Chief Architect and Programme Management, Dataport, Germany
Thomas Gageik, Director for “Digital Business Solutions”, DG Informatics, European Commission
Leonardo Favario, Open Source Project Leader, Digital Transformation Team of the Italian Government

The introduction of open source software in public administration can potentially be a painful process, but it can enable public administrations to stay in control of their citizens’ data.

Open source software is an opportunity for public administrations

Public administrations can use Open Source software as a means of reducing their dependence on non-digital-sovereign vendors, which will increase citizens’ trust in the management of their personal data, regarding security and privacy concerns.
Open source does not mean that the cost of running open source software is free. Open source requires an active service & support model with partners and suppliers.

When negotiating with suppliers, it is important to show them that there are alternatives, and this affects the overall product and operational costs. Being independent and self-determined will help accelerate innovation in the European economy. The pandemic has shown us how important it is to react quickly to new situations and to retain control of GDPR-compliant alternative solutions for diverse domains (e.g. education)

Dataport has built an open source web-based collaboration platform called Phoenix. It combines best-of-breed open source software in the areas of groupware, file-sharing, document-editing, messaging and audio/video for a complete communication and collaboration suite. Dataport has bundled these applications to fit the requirements of public administrations. Phoenix is constantly improving thanks to a trusted and active network, with the participation of manufacturers of open source products and diverse open source communities.

Introducing open source software requires overcoming barriers

The European Commission is going through an evolution in the IT organization, the latest Open Source Strategy 2020-2023 is based on the transition from being an open source user to be an open source contributor.

The transition represents a major change process, because it has to deal with barriers:

- Individual barriers: The Commission has to convince IT professionals in the agencies to move to an open source approach, which takes time.
- Cultural barriers: In the Open Source Strategy, a way to implement the use of open source is to make all source code that the Commission develops internally open by default and to convince people to embrace an "open source life style".
- Legal Barriers: Every contribution to the open source community has to pass through the decision of the college commissioners, which makes it a very long process. The goal is to remove these bureaucratic steps and freely share software as open source with the community.

Public administration need support for a successful transition

The Italian strategy of using open source software is based on three main pillars:

- Legal Context: In 2005 Italy launched the new approach for the reuse of software, under which public administration bodies were obliged to share their software with other administrations upon request. In 2016 the concept was adapted, now obliging public administration bodies to actively publish software, which they newly built or acquired, under an open source license.
- The Guidelines: In order to overcome the lack of broad knowledge and experience with open source, guidelines were released. These contain information on what open sources is, how open source software can be used, and which issues have to be considered when publishing open source software as well as how to deal with them.
- The Developers Italian Catalogue: The national government needed to deliver concrete actions and tools to local public administrations. A marketplace where needs and offers can meet, was the first tool to be established. Thus a catalogue of open source software released and used by public administrations in Italy was implemented. The catalogue currently contains approx. 240 open source solutions, which have already been re-used 2400 times.

In conclusion, the three pillars have to be taken in consideration when public administrations deal with open source software.

Cyber Security

Leonardo De Vizio, Policy Officer, DG Connect, European Commission
Philipp Amann, Head of Strategy, European Cybercrime Center, Europol
Cristian Hesselman, Director of SIDN Labs, The Netherlands
Hannu Naumanen, Chief Security Officer, Valtori Government ICT Centre, Finland

Digital independence requires both interoperability and data security. Initiatives among interoperability should lead to the mandatory use of an interoperability framework by design and default. Benefiting from interoperability can only succeed if cybersecurity can be ensured.

Developing the legal framework and implementing strategy

Building better resilience of strategic sectors becomes more important as digital transformation shapes the future of public administration. Intensification of cybersecurity attacks on essential public services (including the use of the IoT) has led to an extended scope of version 2.0 of the directive on security of network and information systems (NIS). The EU Cyber Security Strategy for the Digital Decade was formed during the pandemic, an example of new issues being raised by a change in the environment. There are several initiatives within the EU Commission implementing the key areas:

1. Resilience, Technological Sovereignty and Leadership
2. Operational Capacity to Prevent, Deter and Respond
3. Advancing a Global and Open Cyberspace.

Ability to implement national cybersecurity strategies on operational level should be based on the principle of comprehensive security, which includes also personal and facility security. Setting the goals and targets in an implementation plan must be set to the correct destination. Digital security guidelines should stretch out cooperation, resources, leadership, identifying competence needs as well as strengthening education and research. One must be prepared, practice and participate. There is also a need to be humble, expect the unexpected and take care of identity - trust but verify.

Raising awareness and educating more experts is vital

There is a growing number of security issues requiring resilience, sovereignty and leadership. The geopolitical tensions increase pressure on supply chains. This makes increasing the awareness of cyber threats and improving cybersecurity culture in the rapidly changing environment crucial. The latent lack of cybersecurity experts in the EU area has been noticed, and identifying the needs and identifying relevant university courses as well as collaboration with the academia and the industry has begun. Bringing in young professionals to the individual public administrations to learn is an option already adapted.

Helping the victims

Public administrations have a need to secure their own organisational environment, but there is also a need to help the victims of cybersecurity attacks. An example of collaboration and sharing is the work conducted at Europol. The Joint Cybercrime Action Taskforce comprises members from 19 law enforcement agencies and public-private partnerships or advisory groups (communication providers, financial services, internet security). Europol also has its own innovation lab. The agency has brought together 180 partners and 120 decryption tools. Six million victims already have been helped in 37 languages.

Collaboration increases cybersecurity resilience

One example of security threats is the misuse of administrator tools to spread ransomware to private as well as governmental server farms, which is a growing threat. Another example of high-impact cybersecurity threats are DDoS attacks, the number of which has increased over the last couple of years. DDoS mitigation services (for example scrubbing) are getting more and more important.

The battle against DDoS attacks can be divided into three areas: sharing DDoS measurements, large scale collaborative drills and sharing expertise. Sharing of DDoS intelligence and expertise across organizations lowers response time and learning provides increased insight, increases control, and builds up a joint pool of expertise. Key innovations are bridging multidisciplinary gap of deployment and potentially open source design. Public administrations have a need for "DDoS early warning systems" and relevant communities just like earthquake warning systems. An EU-wide anti-DDoS coalition to produce malware information sharing platforms could be deployed either regionally or across a sector. At the moment the vast majority of the DDoS mitigation services are not produced in the EU area.

As the society increasingly depends on online services, disruptions reduce digital autonomy. Sharing information is not something to be scared of. There is a need to find new ways to promote greater cooperation and coordination to ensure cybersecurity of the developing digital infrastructure within the EU. In addition to covering the basics and implementing best practices, public administrations have a need to cooperate with the private sector.

Closing Panel

Markus Richter, Federal Government Commissioner for Information Technology, Germany
Luis Barreira de Sousa, Digital and Cyber Ambassador, Portugal
Sasa Bilic, Vice-President of Euritas, CEO of APIS IT, Croatia
Markus Kaiser, President of Euritas, CEO of Austrian Federal Computing Center

The closing panel highlighted the following findings of the Summit:

- Digital sovereignty in Europe is important for citizens, governments and the economy alike.
- Digital sovereignty not only means more secure data for citizens, but also more high skilled jobs.
- Fair competition and the reduction of lock-in effects are positive for the economy as more options are created.
- More interoperability between member states is necessary, the needed resources and capabilities are available.
- Regarding European digital solutions one-size-fits-all is the wrong approach, but too many different solutions are not the answer either.
- Europe has to control cloud providers, not the other way around.
- Safety regulations and standards have to be implemented for digital services.
- Collaboration is more important than ever, a more structured approach toward this is needed.