euritas
European Association of Public IT Service Providers

WE MAKE **IT** POSSIBLE. **TOGETHER.**

EURITAS POSITION PAPER DIGITAL SOVEREIGNTY

Version 1.0

19.05.2020

TABLE OF CONTENTS

1. Introduction

EURITAS is a European network of public ICT service providers which aims at creating better ICT services for public administrations, businesses and citizens in European society.
This position paper of EURITAS is about our understanding of Digital Sovereignty, which is the common baseline of all our ICT efforts.

In Europe, where things are becoming 'digital by default', we must ensure that digital government services match public needs and expectations. Digital services should be human centric, secure and trustworthy, as well as being widely accessible and comprehensible for everyone. The Tallinn Ministerial Declaration on eGovernment[1], adopted in 2017, remains in force as common guidance for EU member states and EU institutions. The need for digital services has become dramatically clear in light of the severe and global crisis we face due to coronavirus. It is this crisis that demonstrates the absolute need for resilience in our countries – resilience not only in the health sector or the economy but also in the ability to work for the public, as a public service and public administration which monitors and controls behaviour and protects the lives of citizens. From this perspective, digital sovereignty is an essential part of becoming more resilient in response to present and future crises.

The European Commission has published the strategies "Europe fit for the digital age[2]"and "Shaping Europe's Digital Future[3]", which prove that digitalisation in Europe has top priority for the Commission. This European approach aims at giving citizens, businesses and governments control over the digital transformation. Euritas considers digital sovereignty as crucial for realising this vision. This paper proposes guiding principles for preserving the digital sovereignty of public administrations and citizens and highlights the fields in which Euritas is actively working to achieve this goal.

[1] ec.europa.eu/newsroom/document.cfm?doc_id=47559

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[3] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

2. Euritas Guiding Principles on Digital Sovereignty

EURITAS understanding of Digital Sovereignty:

EURITAS understands Digital Sovereignty as being the possibility of the public administration and the citizens whose data it stores and processes to act independently in the digital realm in a self-determined manner. To preserve the possibility of self-determination, it is necessary for the public administration and also its ICT service providers to keep full control over citizens' data, so they can ensure their availability and security.

Public ICT service providers have the responsibility to secure the Digital Sovereignty of the public administration and thereby of the citizens.

Ownership and control over data and digital identities:

Public administrations and their ICT service providers have to guarantee that citizens' data will not be transferred or processed without their knowledge or consent. Besides the necessity to comply with the General Data Protection Regulation (GDPR), this is also an important factor for preserving citizens' trust in the public institutions that store and process their data. Furthermore, the concept of Self Sovereign Identity (SSI) promises citizens full sovereignty over their own data with safe and user-friendly use of data points by various parties, also across borders. Public administrations must ensure the integrity of SSI when they act as providers as well as when they grant access to services.

Access to own data must be secured:

The availability of ICT infrastructures and data has become crucial for a functioning public administration capable of providing to citizens and enterprises. With the system of global free trade under threat, storing data outside the EU has become a risk for public administration, because access to cloud services could be cut off to pressure the EU and its member states, e.g. in trade disputes.

Independence from monopolistic vendors:

Many public administrations have become heavily reliant on a small number of large software suppliers who have gained monopolistic market positions. This often means that public administrations find themselves in lock-in situations, lacking the alternatives and leverage needed to negotiate with vendors.

The aim of the EURITAS members is to reduce dependence on monopolistic vendors and find or create alternatives, preferably open-source solutions.

Co-operation and cross border interoperability:

Digital government should serve citizens and businesses alike and support their freedom of movement within the EU. In line with the once-only principle, data should be reused in a responsible way. When citizens expect personalised and comprehensible digital services, traditional boundaries between government, private organisations and civil society may become more hybrid in nature. At the same time, privacy must be guaranteed. When it comes to interacting with public and private organisations, citizens and businesses must be in control over who they share their data with.

3. Current Fields of Action for EURITAS

In order to comply with the guiding principles on Digital Sovereignty, Euritas considers the following fields of action as necessary to focus on:

> Negotiations over terms and conditions with existing external cloud suppliers. In order to gain more leverage together with other European public institutions, Euritas members engage in

- Fostering knowledge exchange with other European public institutions (e.g. in The Hague Forum)

- Exchange between national institutions about negotiations with software suppliers

As an example, see the analysis of Microsoft cloud services and related GDPR issues in the annex to this document.

> EURITAS members cooperate in searching, designing and implementing alternative software solutions and services together to break vendor lock-in and also strengthen their position against big software suppliers:

- Open-source desktop solutions, which can be run "on-premises" and in own cloud infrastructures

- Cloud solutions, which can be run within own datacentres

- Exchange with other European institutions about the development of alternative platforms for public administration

> Handling and maintenance of self-sovereign digital identities by public ICT providers

- Provision of secure and reliable SSI

- Enable citizens to manage their own digital identities, including determining which data they want to share

4. Conclusion

The EURITAS community is ready to develop and realise the goals laid out here and is offering a discourse with all relevant stakeholders on initial questions such as:

> What is your understanding of Digital Sovereignty?
> Are you already "digitally sovereign" enough?
> What are your guiding principles, action fields and conclusions for coping with Digital Sovereignty?
> What have you achieved so far to act with Digital Sovereignty?

EURITAS members are developing and implementing solutions towards strengthening digital sovereignty. We are ready to discuss ideas and cooperate with EU institutions, representatives and digital stakeholders, national contact points and policy makers within European countries and other public ICT service providers or external suppliers in order to implement them.

To conclude the statements made thus far: EURITAS is committed to shaping the digital sovereign ecosystem within Europe. If you are interested in a cooperation with EURITAS, please contact us.

EURITAS Headoffice Vienna
M: euritas@brz.gv.at
Web: www.euritas.eu
Twitter: @EuritasEU
Linkedin: https://www.linkedin.com/company/euritas

Annex: Microsoft GDPR Issues

In order to use Microsoft products GDPR-compliant, at least the following changes to the "Provisions for online services" in the version of January 1, 2020 and "Appendix to the data protection provisions for Microsoft online services" must be agreed and the following technical measures taken:

Disclosure of customer data

The disclosure of customer and support data to subsidiaries (especially the United States) must be restricted to absolutely necessary cases and the disclosure to law enforcement agencies must be restricted to cases that require the law of the European Union or a member state.

International data transfer (Art 28 Para 3 lit a GDPR, Art 44ff GDPR)

All data transfer outside the European Union must be Privacy Shield certified. Microsoft must take precautions in the event that the Privacy Shield adequacy decision is removed.

Processing customer data for own purposes

Customer data may not be processed by Microsoft for its own purposes (i.e. as the person responsible for data protection), but only in the position and scope of the processor.

Audit rights (Art 28 para 3 lit h GDPR)

Microsoft must grant the inspection rights provided for in the GDPR.

Right to object to the use of sub-processors (Art 28 Para 2 GDPR)

The customer is to be granted a right of objection or a right to object to the use of new sub-processors without the termination of the customer contract.

Support with a data protection impact assessment (Art 28 Para 3 lit f GDPR)

Microsoft must disclose all of the information available that can assist in the preparation of a data protection impact assessment.

Support for applications from data subjects (Art 28 Para 3 lit e GDPR)

Microsoft must provide information about all personal data stored by it and correct or delete it when requested.

Generic description of data processing (Art 28 Para 3 GDPR)

Details on data processing (in particular the type of personal data) must be specified in the order processor agreement.

Implementation of technical and organizational measures (Art 28 Para 3 lit c GDPR)

The use of personal data from Microsoft must not only be minimized contractually, but also as far as technically and organizationally possible. The following measures are particularly necessary:

> Deactivating the "Customer Experience Improvement Program"

> Preventing the use of "Controller Connected Experiences"

> Blocking telemetry traffic or setting the telemetry level to "neither"

> Introduction of encryption methods that protect the data from access by Microsoft