GISAD

Global Institute for
Structurerelevance,
Anonymityand
Decentralisationi.G.

GISAD statement on Interoperable digital public services – European Interoperability Framework evaluation & strategy

GISAD (Global Institute for Structure relevance, Anonymity and Decentralisation i. G.) is an institute in founding. From the perspective of the citizens of Europe, GISAD wants to develop a digital system (EU-D-S) that can compete with gatekeepers and a social credit system.

The aim of GISAD is to accompany the preparation of a holistic Marshall Plan, as requested by the President of the European Commission, Ursula von der Leyen. At the heart of the Marshall Plan is a digital concept adapted to civil rights and diversity. In the case of individual measures without an overall system of their own, there is a risk for Europe of losing system competition against other economic areas such as a centrally controlled China.

- GISAD's opinion is subject to the fact that it is part of a digital overall concept (multiple use of the same infrastructure at no extra cost).

GISAD has defined three objectives on which a Marshall Plan should focus:

1. The optimal processing and easy utilisation of digital data, while maintaining diversity and performance-adopted integration of all parties involved in the value creation.
2. The stigmatisation-free, lifelong digital involvement of all citizens with incentives for self-development.
3. Digitally guaranteeing the necessary state tasks to preserve the security of citizens, the economy and the state, while maintaining pre-digital democratic achievements.

Challenges:

In the various European countries there is a different speed of enforcement of eGovernment. These differences are related to general security concerns in digitalisation. Many citizens do not have so often to contact authorities for that digitalisation of public infrastructure can offer them a real advantage. The GDPR and other attempts by the EU to safeguard citizens' rights have often led to the opposite, because the aspect of the convenience of citizens has not been taken into account. For example, those who have to click through cookie policies until they have reached a citizen-friendly portal setting, prefer to waive their civil rights and accept all cookies.
If the EIF is to be successful, it must set standards and technologies where officials and citizens see an advantage for their convenience in the same way. Most cyber attacks are successful due to human failure. This failure is often due to the desire for convenience. It is more convenient to open every email than to consider whether you are allowed to open it. A communication infrastructure must be structured in such a way that it is an effort for every user to overcome IT security.

Proposal for a solution against the backdrop of an overall digitalisation strategy:

Every official is also a citizen. If he has already become acquainted with an infrastructure/technology as a citizen, he will be able to use this competence as an official. Such eGovernment services will be accepted by citizens who use infrastructure/technology that citizens use in their daily lives and therefore know well.

In the pre-digital world, it is natural for an official to carry his authority key and his apartment key with him on the same keychain. The principle of locking is the same. By using his key, he shows his legitimation. Nevertheless, the names of the key holder are not automatically communicated when unlocking. It is sufficient if the user can be identified in the event of unauthorised use of a key.

In order to achieve interoperability, the human side of the human-technology interface must be designed as equal as possible for everyone. Unnoticed by the user, completely different concepts can be stored in the cloud or decentralised behind the same interface.

Similar terminology in different EU languages should lead to the same standardised category. This will make it easier for EU citizens and public authorities to find together with the same concerns. In a second process, translation programs adapted to categories can remove language barriers.

Due to the increasing dominance of foreign monopolists in both hardware and platform development, an unregulated open source standard must be rejected. An EU-source standard is proposed, which should only be available to European-dominated companies.

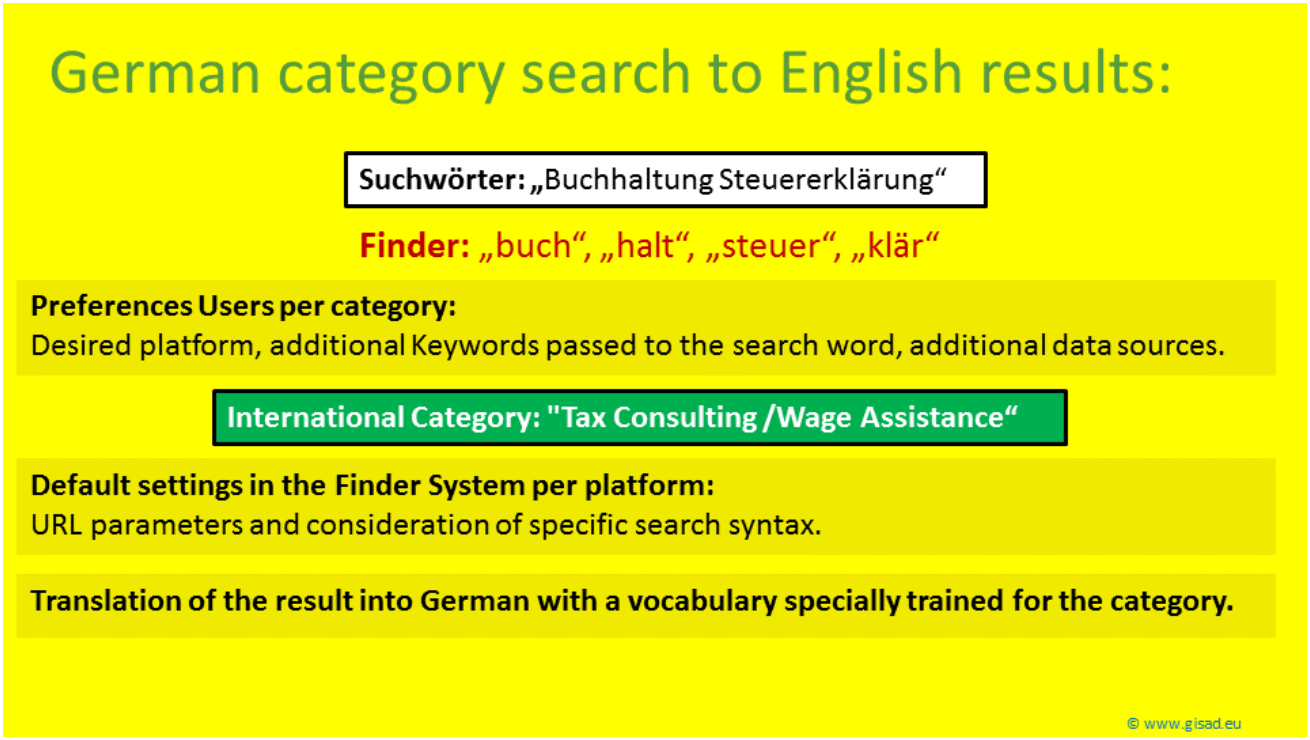
Requirements for an EU-D-S system:

Every EU citizen must be provided with a small hardware as an extension to his devices, which he/she uses permanently in his digitalised everyday life. The same hardware and functionalities are then also used for professional activities in a company or authority.

An EU-D-S is called for:

- In which an IP address can be uniquely assigned to the person responsible for an information, a product, a service or a machine.
- Consisting of regional trust stations located in the residence of an EU citizen, with state recognition corresponding to a notary.
- By awarding a unique public IP subnetwork to each trust station.
- With the publication to each EU citizen by a trust station of 1,000 randomly generated IP addresses from the IP subnet.
- With the obligation of the trust station to assign the IP addresses given to the EU citizen only to the personal data that their storage location is physically separated from the Internet (no network connection).
- With the right of the trust station, without the direct knowledge of the EU citizen concerned, to negotiate with a judge in a concrete investigation which data (related to a category, period, accumulated in a given geographical area) must be issued.
- With the obligation of the Trust Station to inform the affected EU citizen of the issue after a reasonable period of time and to restore WAN anonymity (WAN means WIDE AREA NETWORK) by issuing new IP addresses.
- In which the storage of personal data over the Internet in relation to the civil rights infrastructure is prevented technically and legally.
- In which the physical authority over keys and identities and the content created over it lies with the individual citizen.
- In which security is guaranteed by the provision of hardware created exclusively in Europe (USB stick as an extension of any device).
- In which all metadata, symmetric keys and identities for the data used are stored in such a way that the authority over the data lies with the individual citizen.

- Which an automatic option to create update (e.g. when loading a device) that ensures the availability of metadata for each EU citizen and ensures forensic digital evidence in the event of a house search.



- Standardisation Committee for Categories.
- Search system for finding the appropriate category for a search entry.
- Categories Optimised translation system between EU languages.

Further information on the EU-D-S can be found at:

https: //youtu.be/qd9xGbRbvWY?t=24 ,

https: // youtu.be/2oWLsVhkD0w?t=25 ,

http: // gisad.eu/statements/ .

..