GISAD

Global Institute for
Structure relevance,
Anonymity and
Decentralisation i.G.

## GISAD statement on Civil, defence and space industries (action plan on synergies)

### Preliminary remarks:

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 the 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 statement is subject to the restriction that it is part of a digital overall concept (multiple use of the same infrastructure at no extra cost).

### Challenges:

If we want to achieve synergies between the space/defence industry and civil society, the basis for this is a unique digital judicial area. In times of Home Office and in a future of colonisation of space, it is no longer expected that citizens will remain in one location throughout their lives. Citizens want and must be clearly achievable in the digital space. Digital systems are increasingly competing for this purpose. These centrally managed digital systems often escape the European judicial area. Physical residence becomes less important than the digital system that a citizen chooses as his digital home. The collection of personal profiles takes place today at the expense of privacy and civil rights through digital systems from the USA and China. Cybersecurity is becoming increasingly important to the view of Europe’s defence. Today, almost all the information available to the EU about its own citizens is also available to foreign services. The reason is the lack of protection of digital communication. The greatest danger always comes from the weakest link in a communication chain. That’s the citizen right now. Every politician, every soldier and every employee is also citizen. North Korean ruler Kim Jong-un once said: “We are stronger in cyberwar than you. We have good hackers and our people are not on the Internet, so we are not vulnerable.”

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

Every EU citizen needs an embassy in the EU-D-S, regardless of his permanent place of residence. It is subject to the laws and access of the European representative office he has elected. Ideally, the European representative office is a European notary or lawyer (trust station) who makes the personal data not stored on the Internet available in individual cases and upon judicial disposal.

**Shared use for space, defence and security industries and civil society**

With the provision of accurate satellite navigation data, many new applications are possible. If we want to preserve citizens' rights, navigation data may only be linked to personal data if absolutely necessary. Security also will be seriously compromised if it is possible to personalise movement profiles, as a fitness app from US soldiers in Iraq and Syria has shown.

In the following, I show some examples of applications that would be possible after the introduction of an EU-D-S.

- **Anonymous friend-enemy recognition**

In the purely military solutions, friend-enemy detection (IFF) is installed in aircraft, vehicles, and ships, as well as weapons. Such systems only work for soldiers. Civilians are not protected by this. In the context of satellite navigation, it is possible to display the locations of civilians. Smartphone owners with applications that transmit navigation data via radio can be assigned to military target areas. A safe friend-enemy detection is not possible, and can only be assumed indirectly by the language used and other characteristics. An evaluation of larger groups of people takes too long for a current battle situation. In the EU-D-S, 1000 IP addresses per person are issued by a trust station. These 1000 IP addresses are used alternately for all online transactions to prevent profiling. However, it is possible for anyone to identify the trust station that issued the IP address via the public part of the IP address and to validate a single IP address via an automatic response. Even if the enemy would falsify a single IP address, it is unlikely that he will be able to falsify several valid IP addresses. In addition, a plausibility check can be installed. For example, if the same IP address was used at the same time in a distant place, it is very securely forged. If several EU citizens are displayed at one destination via the EU-D-S, there is a high likelihood that the information is correct. It is appropriate to include also friends as non-EU citizens in the EU-D-S in order to protect them. The exclusion of citizens of a country can simply be caused by the fact that the IP addresses of the respective trust stations are no longer accepted by the EU-D-S.

- **Sector-specific anonymous emergency assistance**

If you leave GPS coordinates for each trust station, for example, an Italian in Amsterdam can start an emergency call with his GPS data behind the category “Auto Repairs”. The EU-D-S identifies the trust stations based in Amsterdam. These send the request automatically to the clients listed in the category. Offers of Dutch auto repair workshops from nearby are displayed to the Italian. He makes contact and it is up to him to cancel his anonymity.

- **Automatic collection of car sharing data**

In accordance with the GDPR, effective consent from the user would have to be obtained for every use of the vehicle's movement profiles. At present, this is usually not done because it could deter potential customers. With the EU-D-S, it is possible to cancel anonymity only if it was deemed necessary by a judge on the basis of a violation of the law. When renting and paying, the user uses any of the 1000 IP addresses assigned to him. The assignment is only known to the Trust Station. The customer remains anonymous. The user profile cannot be assigned to him personally. The acceptance problems with sharing are falling away. This also applies to sharing opportunities in other industries.

- **Real control over one's own data**

Weincreasingly store our data with service providers in the cloud. Cloud services are good at providing the integrity and availability of data. As regards confidentiality, they do not provide sufficient protection when passwords and keys are exchanged openly over the Internet. Furthermore, the authority of an owner over his data is not guaranteed. Many providers operate outside the European judicial area. We trust that these areas of justice will remain stable. In fact, there are many ways to deprive the owner of the authority over his data. Service providers can be handled or sold to foreign companies and the data can be deleted. Even when the owner of a company has changed, we must also trust that no employee of a service provider will remove the central security mechanisms.

In an EU-D-S, the metadata with the keys for data storage and communication are individually stored in a decentralised way for each user. The data encrypted on the basis of the same metadata can be stored at several service providers in any location. If a service provider missing, the availability is still ensured by a second commissioned service provider. The availability of metadata is also decentralised via a decentralised automatic backup system. For the space, defence and security industries, this creates a European unique selling point with a high level of security for European citizens and businesses.

- **Hardware production based on the dual-use principle**

The EU-D-S costs around EUR30 per citizen. The hardware accounts for more than half of the costs. In order to ensure a high level of safety, all subcomponents must be developed of companies in a majority European ownership. 448 million people live in Europe (source Eurostat for 2020).If we expect 400 million participants in the EU-D-S (excluding children under the age of 8), there will be an investment of around EUR 6 billion. The investment requirement does not arise at once, as an expansion in several stages by a wide variety of providers makes sense. These investments can also be quickly refinanced by the multitude of new applications. It makes sense to consistently develop specifications for such a large volume, how the components used for this purpose can be used as diverse as possible.

**Conditions for the EU-D-S**

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 release to every EU citizen through 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 given.
- 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 EU-D-S 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.
- With provide an automatic update option (e.g. when loading a device) that ensures the availability of metadata for each EU citizen and guarantees forensic digital evidence in the event of a house search.
- By standardising around 1000 categories worldwide for all industries.
- Through a search entry into the search of different platforms per category in up to 2500 languages.

**For further information:**

Http: //gisad.eu/statements/

Https: //youtu.be/doPXxmX7fec?t=233

Https: //youtu.be/XZS1YGTULIw?t=57

Https: //youtu.be/s1occJG5SOw?t=29