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

GISAD statement on https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13336-United-Nations-Cybercrime-Convention-authorising-negotiations_en

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

The aim of GISAD is to support the creation of a holistic Marshall Plan, as called for by the President of the European Commission, Ursula von der Leyen. The core of the Marshall Plan must be a digital concept adapted to civil rights and diversity. If individual measures are taken without an overall system of their own, Europe runs the risk of losing the system competition to other economic areas such as a centrally controlled China.

- GISAD's opinion is subject to the proviso that it is to be as part of an overall digital concept understood (multiple use of the same infrastructure without additional costs).

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

1. The optimal refinement and simple exploitation of digital data, while maintaining diversity and performance-adopted involvement of all parties involved in the value creation.
2. The stigma-free, lifelong digital inclusion of all citizens with incentives for self-development.
3. The digital guarantee of the necessary state tasks to maintain security for citizens, the economy and the state, while preserving pre-digital democratic achievements.

Challenges:

GISAD welcomes the EU's participation in the United Nations negotiations on cybercrime. These offer a unique opportunity to position itself as a third digital power alongside the US and China. In addition to existing negotiation approaches, the way should be paved for the EU D-S, with the aim of ensuring by design the highest possible standard according to the state of the art in the interest of citizen sovereignty, democracy and diversity. The goal should be that all internet platforms and operators that enable cybercrime on the basis of inferior concepts have to pay for the damages according to the polluter pays principle. This must also apply to states that build backdoors into software or enable the installation of backdoors.

The tax revenues generated by this should be used as provisions for the guarantees necessary for the cooperatives. The cooperatives are open to any business. If the EU manages to make this standard the standard of the United Nations in the future, it will thereby enable the EU-D-S to expand democracy, prosperity and human rights worldwide.

Minimum standards, which are implemented in the EU-D-S:

- Every citizen must have the right to reach other citizens or institutions via a secure infrastructure. For this purpose, according to the current state of technology, every citizen must be provided free of charge with his or her own hardware (comparable to a USB plug) on which the keys for files stored in the cloud and currently 1000 IP addresses for concealing identity are stored.
- The fact that the real power of disposal over the data lies with the author means that backdoors and copyright infringements can be largely ruled out.
- Communication in the EU-D-S is encrypted, usually anonymous, with IP addresses being used like today's telephone numbers for telephone calls, video conferences, e-mail and messages. Anonymity can only be lifted in individual cases with regard to the participants in the conversation if everyone agrees. It is forbidden under penalty of law to publicly lift anonymity.
- Automatically, authorised participation must be verifiable within the EU D-S.
- The trust station associated with a citizen's place of origin can be uniquely identified via each IP address used, similar to a car license plate.
- Each participant of the EU-D-S must be uniquely identifiable via a trust station on a case-by-case basis and according to a court order, without personal data being stored on the internet for this purpose.
- The possibility of securing extensive forensic data via the trust station after a court order must be ensured. In doing so, the trust station represents the data owner in a function comparable to that of a lawyer.
- Data protection provisions are accepted once at the beginning of membership in the EU-D-S and also apply to information from third-party providers displayed in the EU-D-S, as long as a citizen does not actively request a different use of his or her data in individual cases. It must be possible to revoke this consent at any time.
- The non-personalisable data may be exploited without limitation by all companies organised in the EU-D-S cooperatives.
- Every citizen must have the freedom to choose between search algorithms. Real freedom of choice only exists if the user does not store his preferences and, if required, passwords in a third-party browser or platform, but in his own user profile on his own hardware.